Redbooks
ibm.com/redbooks

SAP HANA on IBM Power Systems Backup and Recovery Solutions

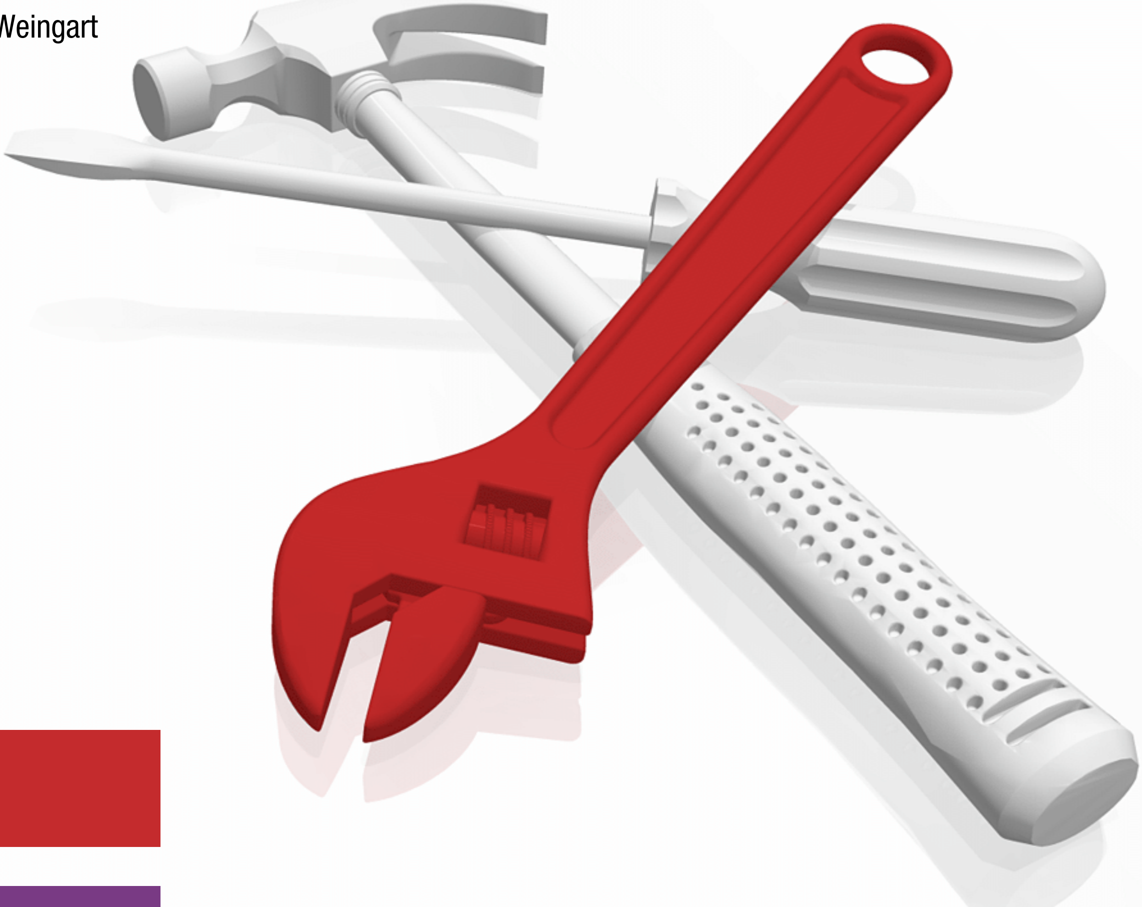
Dino Quintero

Rosane Goldstein

Adriana Melges Quintanilha Weingart

Pia Nymann

Andrei Socoliuc



Cloud

Power Systems

In partnership with
IBM Academy of Technology

IBM

Redpaper

IBM Redbooks

SAP HANA on IBM Power Systems Backup and Recovery Solutions

May 2021

REDP-5618-00

Note: Before using this information and the product it supports, read the information in "Notices" on page vii.

First Edition (May 2021)

This edition applies to:

- SAP High-performance Analytic Appliance (HANA) 2.0 SPS 05.
- SAP HANA Database (HDB) 2.0 SPS 04.
- SAP HANA Cockpit 2.0 SP 12.
- Red Hat Enterprise Linux 7.8 Little Endian (LE) on an IBM POWER9 logical partition (LPAR).
- SAP HANA Studio 2.3.53 that is installed on an external Windows workstation.
- IBM FlashSystem 9110 with IBM Spectrum Virtualize V8.3.1.2.
- IBM Spectrum Protect V8.1.10 on an IBM POWER9 LPAR with IBM AIX 7.2.
- IBM Data Protection for SAP HANA V8.1.11 that is deployed on an SAP HANA LPAR.
- IBM Spectrum Copy Data Management V2.2.12 that is deployed on a VMware 6.5 environment.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®
Aspera®
Db2®
FASP®
FlashCopy®
Guardium®
IBM®
IBM Cloud®
IBM FlashSystem®
IBM Garage™
IBM Security™
IBM Spectrum®
POWER®
POWER8®
POWER9™
PowerHA®
PowerVM®
QRadar®
Redbooks®
Redbooks (logo) ®
Storwize®
SystemMirror®
Tivoli®
XIV®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redpaper publication provides guidance about a backup and recovery solution for SAP High-performance Analytic Appliance (HANA) running on IBM Power Systems. This publication provides case studies and how-to procedures that show backup and recovery scenarios.

This publication provides information about how to protect data in an SAP HANA environment by using IBM Spectrum® Protect and IBM Spectrum Copy Data Manager. This publication focuses on the data protection solution, which is described through several scenarios.

The information in this publication is distributed on an *as-is* basis without any warranty that is either expressed or implied. Support assistance for the use of this material is limited to situations where IBM Spectrum Scale or IBM Spectrum Protect are supported and entitled, and where the issues are specific to a blueprint implementation.

The goal of the publication is to describe the best aspects and options for backup, snapshots, and restore of SAP HANA Multitenant Database Container (MDC) single and multi-tenant installations on IBM Power Systems by using theoretical knowledge, hands-on exercises, and documenting the findings through sample scenarios.

This document provides resources about the following processes:

- Describing how to determine the best option, including SAP Landscape aspects to back up, snapshot, and restore of SAP HANA MDC single and multi-tenant installations based on IBM Spectrum Computing Suite, Red Hat Linux Relax and Recover (ReAR), and other products.
- Documenting key aspects, such as recovery time objective (RTO) and recovery point objective (RPO), backup impact (load, duration, scheduling), quantitative savings (for example, data deduplication), integration and catalog currency, and tips and tricks that are not covered in the product documentation.
- Using IBM Cloud® Object Storage and documenting how to use IBM Spectrum Protect to back up to the cloud. SAP HANA 2.0 SPS 05 has this feature that is built in natively. IBM Spectrum Protect for Enterprise Resource Planning (ERP) has this feature too.
- Documenting Linux ReaR to cover operating system (OS) backup because ReAR is used by most backup products, such as IBM Spectrum Protect and Symantec Endpoint Protection (SEP) to back up OSs.

This publication targets technical readers including IT specialists, systems architects, brand specialists, sales teams, and anyone looking for a guide about how to implement the best options for SAP HANA backup and recovery on IBM Power Systems. Moreover, this publication provides documentation to transfer the how-to-skills to the technical teams and solution guidance to the sales team. This publication complements the documentation that is available at IBM Knowledge Center, and it aligns with the educational materials that are provided by IBM Garage™ for Systems Technical Education and Training.

Authors

This paper was produced in close collaboration with the IBM SAP International Competence Center (ISICC) in Walldorf, SAP Headquarters in Germany and IBM Redbooks®.

ISICC | IBM SAP International
Competence
Center

Dino Quintero is an IT Management Consultant and an IBM Level 3 Senior Certified IT Specialist with IBM Redbooks in Poughkeepsie, New York. He has 24 years of experience with IBM Power Systems technologies and solutions. Dino shares his technical computing passion and expertise by leading teams developing technical content in the areas of enterprise continuous availability, enterprise systems management, high-performance computing, cloud computing, artificial intelligence (AI) (including machine and deep learning), and cognitive solutions. He also is a Certified Open Group Distinguished IT Specialist. Dino holds a Master of Computing Information Systems degree and a Bachelor of Science degree in Computer Science from Marist College.

Rosane Goldstein is Storage Consultant at IBM Systems Lab Services in São Paulo, Brazil. She has been working at IBM since 1999, and she has more than 15 years of experience with IBM Spectrum Protect (formerly IBM Tivoli® Storage Manager). She provides technical pre-sales support, proof of concepts, and workshops for customers in Latin America and Brazil, and she also provides design, planning, and implementation services for IBM Spectrum Protect and IBM Spectrum Protect Plus. She has authored other Redbooks and is a regular speaker at IBM technical conferences.

Adriana Melges Quintanilha Weingart is a certified IBM Thought Leader / The Open Group Distinguished Technical Specialist working as Infrastructure Architect for SAP solutions on IBM Cloud, where she reviews exceptions and proposes viable alternatives to solution architects and customers as part of the Boarding Solutions team. She has more than 22 years of experience in IT/SAP, and has been with IBM for 15 years. She supported global, Latin America, and Brazilian customers in the banking and consumer products industries an SAP and Middleware subject matter expert (SME) by working close with the customer, partners, and other IBM teams. Adriana is a member of the IBM Academy of Technology and IBM Technology Leadership Council in Brazil, has authored other Redbooks, and participates as a speaker at IBM and non-IBM technical conferences.

Pia Nymann is an IBM Certified Senior IT Specialist working at Systems Lab Services in Denmark, which is part of IBM Systems Group. She has more than 20 years of experience in the IT industry and has several years of IBM Spectrum Protect (formerly IBM Tivoli Storage Manager) software experience, which includes designing and implementing backup and recovery solutions on various platforms and applications. She used her skills during that time by supporting and educating many clients about data protection. Pia has worked with various areas of the storage management discipline, including IBM Spectrum Control, IBM Spectrum Scale, storage analysis, and service management. She is an author of *IBM Tivoli Storage Manager as a Data Protection Solution*, SG24-8134.

Andrei Socoliuc is a Certified IT Specialist in Systems and Infrastructure working at IBM Global Technologies Services at IBM Romania. He has 20 years of experience in IT infrastructure, and also has experience working with IBM Spectrum Protect and designing and implementing backup and recovery solutions. He is a coauthor of several IBM Redbooks publications on IBM PowerHA® SystemMirror® and IBM Spectrum Scale.

Thanks to the following people for their contributions to this project:

Wade Wallace
IBM Redbooks, Austin Center

Katharina Probst, Thomas Prause, Graham Hardy, Thomas Gerisch, Axel Westphal
IBM Germany

Kavish Ghogale
IBM India

Natasha Walker, Pepe Lam, Arun Viswanathan
IBM US

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

To complete the tasks that this publication describes, you must understand IBM Spectrum Copy Data Manager and IBM Spectrum Protect architecture, concepts, and configuration.

This chapter contains the following topics:

- 1.1, “Executive summary” on page 2
- 1.2, “Backup and restore scenarios” on page 3
- 1.3, “Abbreviations and terminology” on page 4

In the executive summary, the key elements of the publication are described briefly.

1.1 Executive summary

Data protection is insurance to protect against data loss. You must balance recoverability and investment in the data protection strategy to support optimally the business, as shown in Figure 1-1.

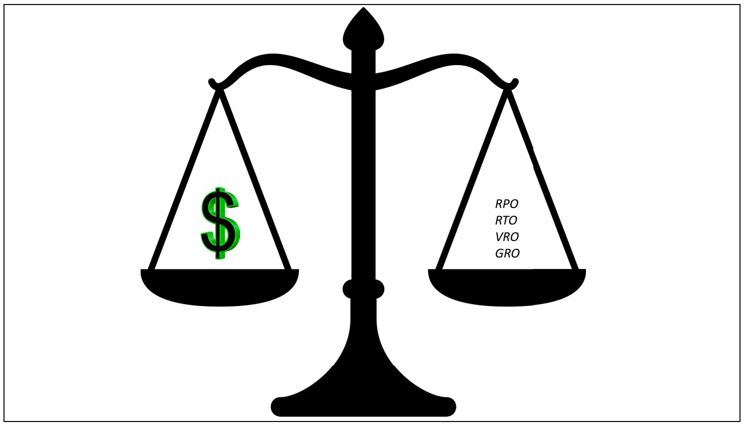


Figure 1-1 Data protection strategy balance

There are four key objectives for a good and resilient data protection solution for SAP High-performance Analytic Appliance (HANA) and other types of data sources:

- Recovery time objective (RTO) and recovery point objective (RPO) make up the core strategy of how quickly a service that is based on data can be brought back if there is failure and with how much data loss. By combining IBM Spectrum Protect and IBM Spectrum Data Copy Manager, the data loss can be minimized and the time to recover can be shortened.
- Version retention objective (VRO) and geographic redundancy objective (GRO) cover how many copies of data back in time can be restored and from how many dispersed locations. In some situations, going back in time to find historical data can be relevant, but it is not necessary that the data is quickly accessible. Cheaper storage media can lower the total cost of ownership (TCO) of the data protection solution. Using replication with IBM Spectrum Protect and IBM Spectrum Data Copy Manager and making data instantly accessible can minimize multiple copies and the physical foot print.

A sample scenario is to reduce the RPO by using the SAP HANA Backint integrated solution, which covers full, differential, and incremental backups in a space-efficient way by including the option to increase the GRO by using IBM Cloud Object Storage.

These four important pillars determine how cyber resilient the solution is. Going through different scenarios, this publication shows how to use data protection tools that are based on IBM Spectrum Protect and IBM Spectrum Data Copy Manager to fulfill the data protection requirements for SAP HANA.

Figure 1-2 on page 3 shows a schematic representation of the terms RPO and RTO. Also, the agreed values of RPO and RTO are *not* fulfilled.

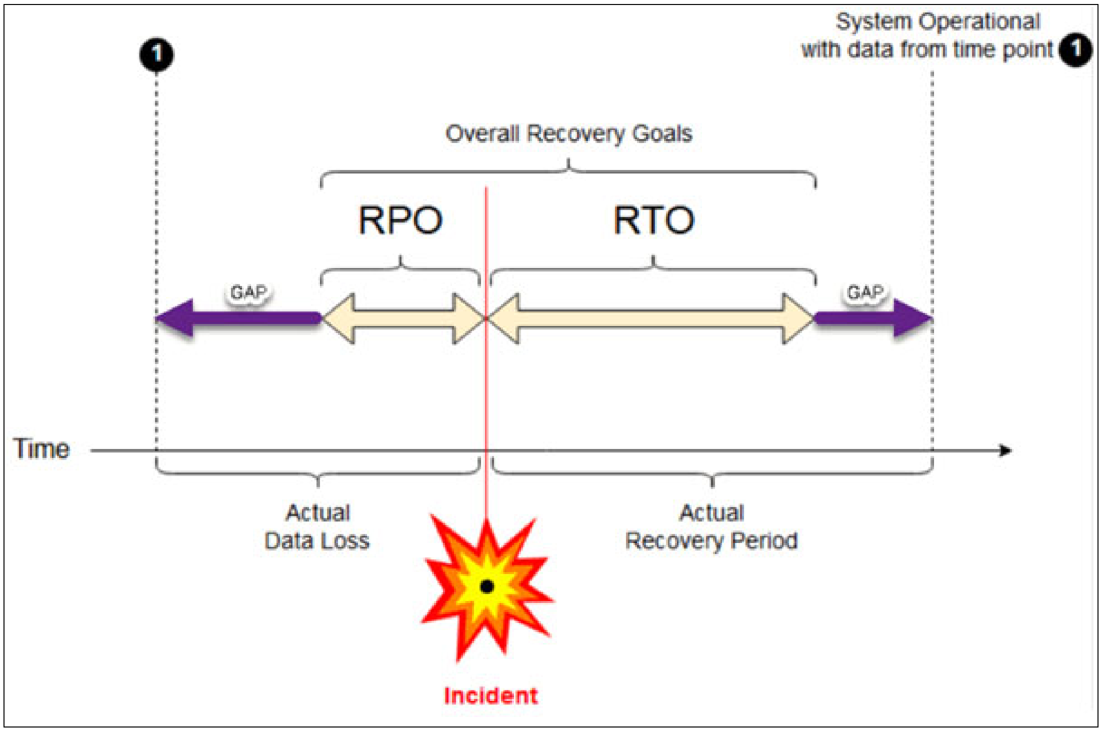


Figure 1-2 Overall recovery goals: RPO and RTO[1]

More refined toolsets are required to remove the gaps to recover the service and meet these objectives. This publication provides strategies and solutions that are based on the IBM technical solution design to address the gaps in RTO and RPO.

There are aspects describe in this publication to protect the backed-up data against ransomware attacks through incident detection, and to be able to store the data securely.

All these requirements and operational functions must be fulfilled at the lowest possible cost. Data reduction capabilities like incremental backups, deduplication, and compression also are part of the solution design, which what makes a modern data protection solution for SAP HANA and the infrastructure around it.

1.2 Backup and restore scenarios

This publication investigates different backup and restore scenarios and approaches that are based on what is possible with SAP HANA. The backup catalog of SAP HANA is the source to record the different copies of the database. Backint and snapshot solve different requirements (RTO, RPO, VRO, and GRO) and can be used separately or in combination.

The scenarios this paper focuses on are:

- Backup and restore by using Backint with full, differential, and incremental backups, including logs to IBM Spectrum Protect.
- Backup and restore by using snapshot through IBM Spectrum Copy Data Management with and without IBM Spectrum Protect.

[1] Disaster recovery: https://en.wikipedia.org/wiki/Disaster_recovery

1.3 Abbreviations and terminology

This section provides terms that are used throughout this publication. For abbreviations and acronyms, see "Abbreviations and acronyms" on page 131.

RPO An expression of how much data back in time is allowed to be lost after a disaster or loss-causing event strikes. A low RPO strives for smaller backup windows, which can be difficult with large databases that require periodic full backup copies.

RTO The window that you have to recover a service from a failure. These windows become shorter as data access becomes more important. Near-instant recovery is the objective for data-serving critical applications.

VRO Able to go back in time to earlier recovery points that include historical data that might have been removed from the current production data.

GRO Makes sure that the data copies are on geographically dispersed storage on different media (types) in different places to prevent data loss in case of disasters or media failure.

IBM Spectrum Protect Can either refer to the server or the client.

Service-level agreement (SLA) Also referred to as a data retention policy.

Chunk/extent Subfiles that are used to eliminate duplicated data streams of objects. Only one instance is stored for each common chunk/extent.

Restore An act that involves the restoration of all files that are required to recover your database to a consistent state (like copying all backup files from a secondary location such as tape or storage to your stage area).

Recovery Process to apply all transactions that are recorded in your archive logs by rolling forward the database to a point-in-time (PiT) or until the last transaction recorded is applied, thus recovering your database to a specific PiT.

Backup Process to make a copy of data to a different storage repository than a production disk for retention versioning.

Snapshot and IBM FlashCopy® A data set recovery point at a specific time.
IBM Spectrum Virtualize uses the term FlashCopy for this type of recovery point of a set of volumes.

2

Architecture decision aspects

When planning a backup solution for an SAP High-performance Analytic Appliance (HANA) system, you should understand the system configuration, the backup possibilities and architectural aspects of each element, and then select the best fit for the system and business needs.

This chapter introduces some architectural aspects of the components of a backup solution that are addressed and clarified throughout this publication.

This chapter contains the following topics:

- 2.1, “SAP HANA architecture” on page 6
- 2.2, “Requirements for a data protection solution for SAP HANA” on page 11
- 2.3, “IBM Spectrum Protect architecture” on page 11
- 2.4, “Protecting an SAP HANA database with IBM Spectrum Copy Data Management” on page 15
- 2.5, “Retention policies and placement of backup copies” on page 29
- 2.6, “Cyber resiliency aspects of an SAP HANA solution” on page 36
- 2.7, “Other tools to use for backup and recovery of SAP HANA” on page 43

2.1 SAP HANA architecture

SAP HANA is a column-oriented in-memory relational database system that was developed by SAP and released in 2011.

This database model and its compression factor allow fast data processing and smaller space that is allocated in memory.

SAP HANA is an excellent tool for real-time analytics. Often, it requires no extra data-warehouse systems and regular ETL processing because data can be consolidated and recalculated for specific reports inside the OLTP system that is powered by HANA.

SAP HANA is composed of several components. Its database is developed in C and runs on SUSE Linux Enterprise Server or Red Hat Enterprise Linux on the IBM POWER® platform.

Tip: For SAP HANA supported operating systems (OSs) on the Power platform, see SAP Note 2235581. An SAP ID is required for access to the SAP Support Portal.

SAP HANA has several components, as shown in the Figure 2-1.

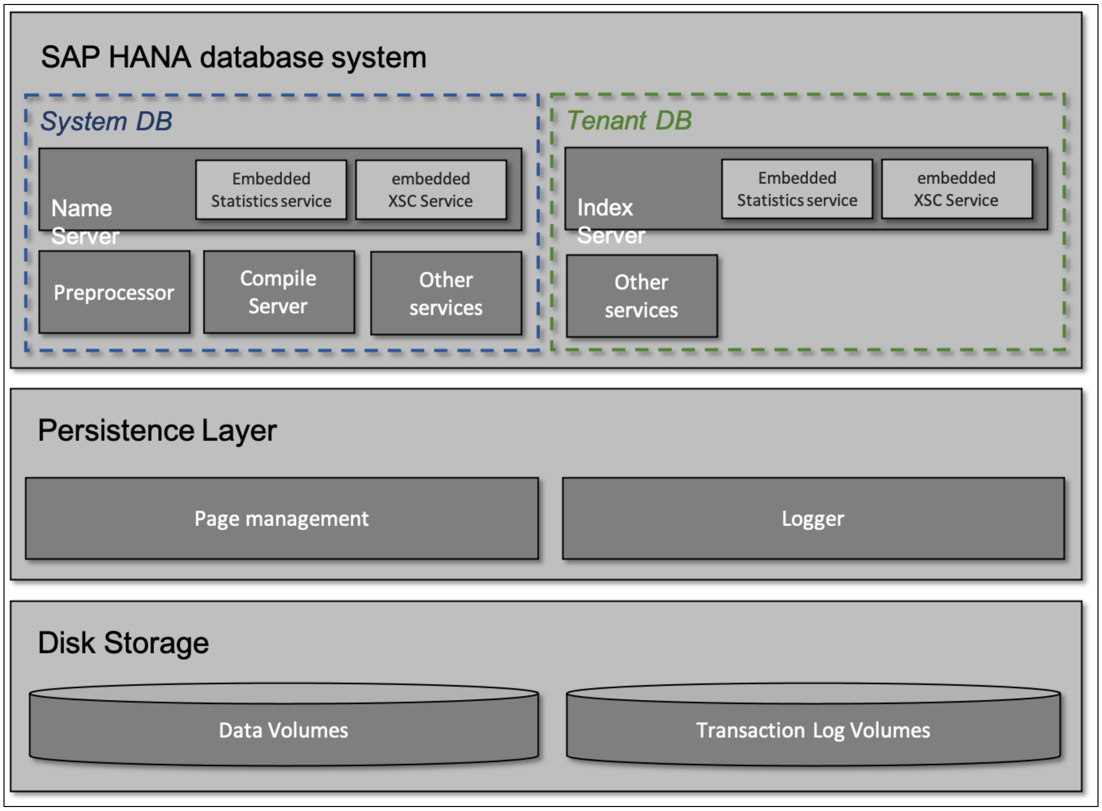


Figure 2-1 SAP HANA architecture

2.1.1 Multitenant Database Container

Since Version 2.0 SPS 01, all SAP HANA installations have the Multitenant Database Container (MDC) architecture.

MDC is an operating concept and technical deployment approach that allows multiple but isolated databases in one SAP HANA system, as shown in Figure 2-2. It has the following components:

- One system database that is used for centralized system administration.
- One or more tenant databases (containers).

Each database has its own separated components (database users and objects, repository, catalog, traces and logs, and persistence and backup).

In an MDC architecture, all tenant databases are placed in `/hana/data` and cannot be distinguished from each other, which can affect backup and recovery definitions and procedures.

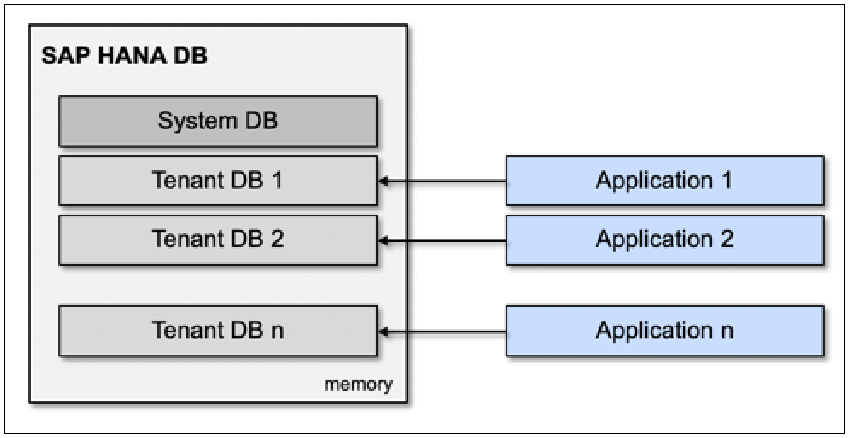


Figure 2-2 SAP HANA MDC architecture

Note: Before SAP HANA 2.0 SPS 01, other operational modes (or architectures) were available for SAP HANA databases:

- Single Application on One SAP HANA System (SCOS)
- Multiple Components on One Database / Multiple Applications on One SAP HANA System (MCOD)
- Multiple Components in One System / Multiple SAP HANA Systems on One Host (MCOS)

Currently, all SAP HANA installations use the MDC architecture.

For more information about SAP HANA MDC, see SAP HANA Administration Guide or SAP Note 2101244.

2.1.2 In-memory persistence and savepoints

One important aspect of an in-memory database is how to protect its data if there is a memory failure.

SAP HANA persists in-memory data to persistent storage media and flushes all changed data from memory to data volumes. All SAP HANA operations are saved periodically to disk by using savepoints in data and redo log files.

In a savepoint operation, the SAP HANA database flushes all changed data that is in memory to the data volumes. So, the data that belongs to each savepoint has a consistent state of the data on disk until the next savepoint is completed.

Note: The redo log entries are written to the log volumes for all changes in the persistent data.

Figure 2-3 illustrates SAP HANA persistence and the related volumes / file systems that are used to store the flushed data.

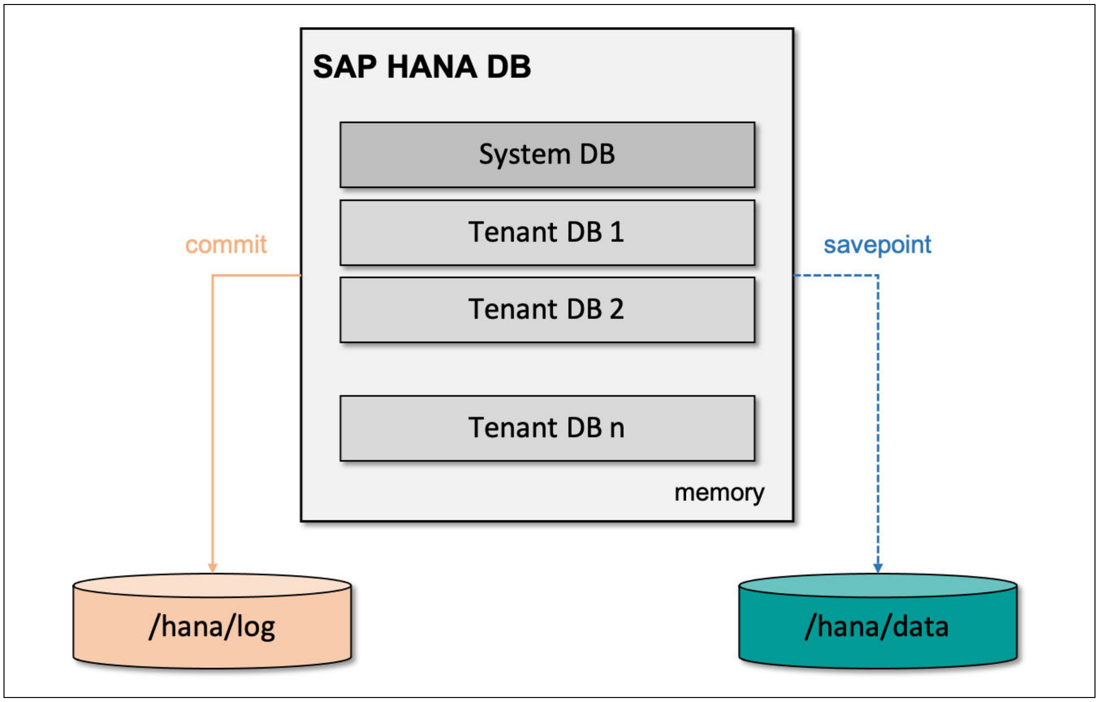


Figure 2-3 SAP HANA in-memory persistence

New savepoints normally overwrite older savepoints, but it is possible to freeze a savepoint for future use. In this case, the savepoint is called a *snapshot*.

Snapshots can be replicated in the form of full data backups to be used to restore a database to a specific point. To ensure a minimal loss of data in these cases, extra, smaller, and periodic log backups are necessary. These scenarios and possibilities are addressed in Chapter 5, “Backup, restore, and recovery scenarios for SAP HANA” on page 73.

Although the logs are written for any change in data after each operation (commit), that is, synchronously, the savepoint to flush the data from memory to disk happens asynchronously at a frequency that is defined in the `persistence` section of the `global.ini` profile (the default is every 5 minutes). Besides this automatic trigger, savepoints can be triggered by many other operations, such as a database shutdown, restart, and data backup. You can also do a savepoint by running a command manually.

Figure 2-4 represents how savepoints and logs saves happen over time. It also shows an extra savepoint that is triggered as a snapshot.

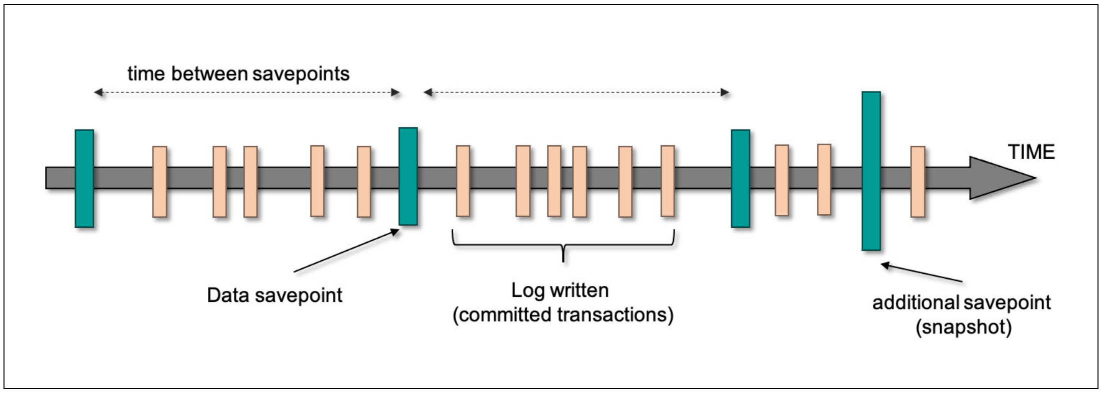


Figure 2-4 SAP HANA savepoints and logs saves

Data savepoints have a significant recovery point objective (RPO), and adding the logs to the data adds to the costs and infrastructure requirements. Although this solution works, consider other more flexible solutions to speed up the backup, and reduce the time, space, and impact to the whole system and architecture. This publication presents other solutions in the next chapters that can work as possible alternatives for backing up the SAP HANA system.

2.1.3 SAP HANA System Replication

The SAP HANA system has a mechanism to ensure its high availability through the continuous replication of data from a primary to a secondary system, which enables resuming productive operations with minimal downtime. This mechanism is called SAP HANA System Replication (SAP HSR). Figure 2-5 presents a high-level scheme of the SAP HSR solution.

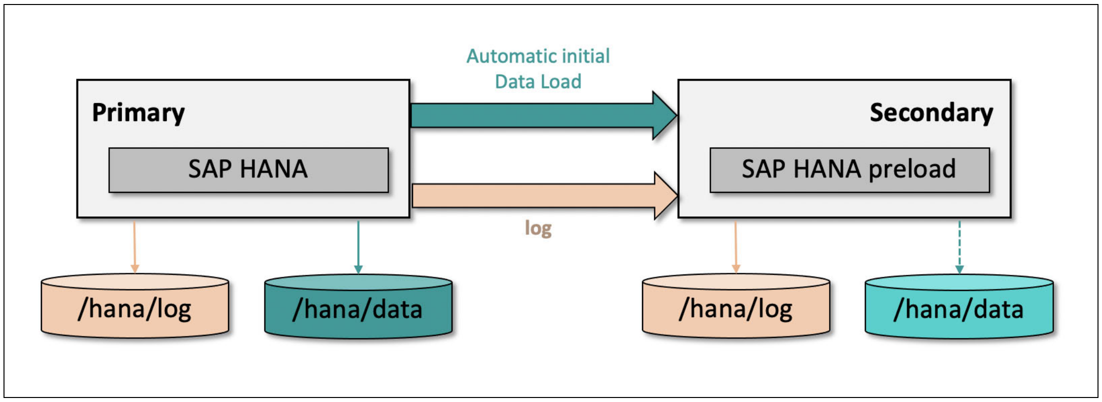


Figure 2-5 SAP HANA System Replication

SAP HSR allows rapid failover (including the in-memory data) if there is a disaster that affects the whole system. If the system has a system database and many tenant databases, then the replication and takeover happen for the entire system because a takeover for a single tenant database is not possible.

If a new tenant database is created in a running SAP HANA system, it must be backed up to participate in the replication.

System replication does not eliminate the need for backup or vice-versa. They work together: System replication ensures data redundancy, and backups can recover to any point. During a takeover, a backup is essential if the redundancy mechanisms of system replication fail.

Here are some considerations about the SAP HSR configuration:

- Both primary and secondary systems must have the same configuration, which includes the number of active hosts, and the names of the hosts and failover groups.
- Primary and secondary systems must be in separate hosts because replication between two systems on the same host is not possible.
- The secondary system must have the same SAP System ID (SID) and instance number as the primary system.

2.1.4 SAP HSR and SAP backup

When working with SAP HSR, you must consider when and how to perform backups.

Only the primary site runs backups, and for system replication, the primary site must be configured for backup or the secondary site does not register.

To configure system replication, you must create an initial full data backup or storage snapshot. In addition, you must consider some important details about backup in this setup:

- Data and log backups can be written only on the primary system. After the takeover happens and completes, the secondary system becomes the new primary system, and only then can it write data and log backups.
- After a takeover, the new primary system must have the backups scheduled and configured properly, and the original primary system must not continue writing backups to the same destination. If backups from different systems and sources are mixed, it is not possible to recover the database.
- After a takeover, it is necessary to perform a full data backup (data backup or storage snapshot). Until it completes, no delta backups can happen in the new primary system.

Note: For more information and details about how to configure the HANA System Replication in an SAP HANA System, see the following resources:

- *SAP HANA System Replication Guide*
- SAP Note 2165547

Although having system replication configured and working can ensure data redundancy, backups allow a recovery to any point. During a takeover, a backup is essential as system replication as redundancy mechanisms fall away.

2.2 Requirements for a data protection solution for SAP HANA

When selecting a data protection solution for SAP HANA, there are functional and non-functional requirements to consider. The following list is not mandatory and exhaustive, but can be used as a start:

- Use a certified solution.
- Use the Backint application programming interface (API) in combination with snapshots.
- For your backup strategy use full, differential, and incremental backups.
- Use the backup state report from the IBM Spectrum Protect server (operation center) and from the SAP HANA Studio.
- Backups and restores can be started from SAP HANA Studio or SAP HANA Cockpit.
- Automate backups by using a script in a cron job, IBM Spectrum Protect scheduler, or other methods.
- An automated backup of SAP HANA logs is triggered by SAP HANA.
- Use a simple installation and a configuration installation script.
- Support scale-out or scale-out cluster as multiple nodes.
- Support multitenancy (multiple separate SAP HANA instances on one host).
- Have extra copies.

2.3 IBM Spectrum Protect architecture

SAP introduced a new version of the SAP HANA API interface for Backint 1.5 in SAP HANA SPS 05. IBM Spectrum Protect is certified as third-party software for SAP HANA database backup by using the Backint interface for this version of SAP HANA and earlier.

Figure 2-6 shows the components that are needed to perform SAP HANA database backups by using IBM Spectrum Protect.

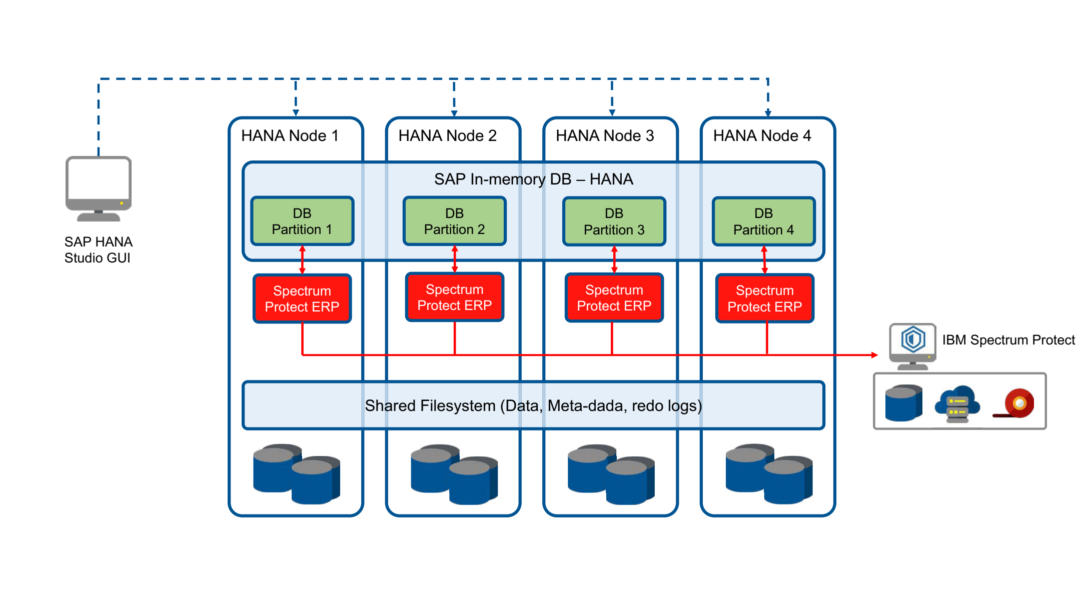


Figure 2-6 SAP HANA and IBM Spectrum Protect components

2.3.1 Overview of SAP HANA integration with IBM Spectrum Protect

SAP HANA offers functions to protect the database and ensure that it can be recovered. You can easily use SAP HANA tools (SAP HANA Cockpit, SAP HANA Studio, and SQL command-line statements) to perform backups locally.

Data Protection for SAP HANA operates as a link between SAP HANA and IBM Spectrum Protect and offers a production-oriented solution with the following characteristics:

- It moves backup data off the SAP HANA system to protect it from both logical and physical errors.
- It does not need to use local disk space as a target backup.
- With redo log backup, you can recover to any point.
- Data can be restored to other systems (even geographically separated ones).
- Online backups offer 24x7 application availability because no downtime is required for backups.
- Integration with a certified API (Backint) offers automated and consistent backups and restores.
- Backups are maintained inside the backup catalog.

2.3.2 The Backint interface

SAP HANA uses the Backint interface to communicate with Data Protection for SAP HANA and IBM Spectrum Protect. The Backint interface processes the request for backup, restore, and inquiry, and run them by using Data Protection for SAP HANA.

Hdbbackint is the Backint agent that uses the Backint parameters that are stored in the `initSID.utl` file that contains information about how to run the backup and restore process. A process that is called proLE connects to the `initSID.utl` file to get the configuration and ensures that the correct backup IDs are assigned. Hdbbackint sends the data to be backed up to the IBM Spectrum Protect API, which in turn backs it up to the IBM Spectrum Protect server, as shown in Figure 2-7.

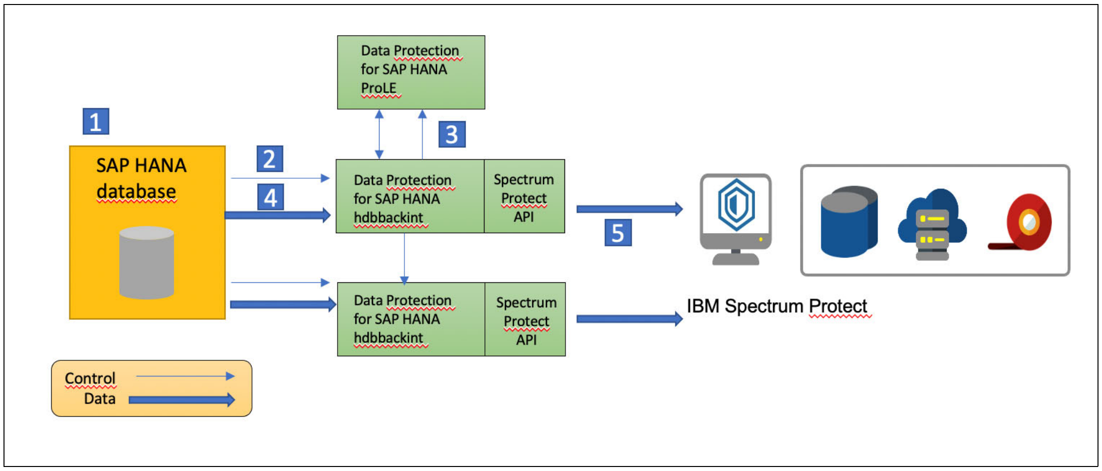

Data Protection for SAP HANA ProLE
1
SAP HANA database
2
4
3
Data Protection for SAP HANA hdbbackint
Spectrum Protect API
5
Data Protection for SAP HANA hdbbackint
Spectrum Protect API
IBM Spectrum Protect
Control
Data

Figure 2-7 Interactions between SAP HANA and IBM Spectrum Protect through the backing interface

In Figure 2-7 on page 12, backup operations proceed in the following order:

1. A backup operation starts by using SAP HANA Studio or through the **`hdbsql`** command-line interface (CLI).
2. A number of SAP HANA hdbbackint processes are started.
3. The hdbbackint processes connect to the ProLE to get the configuration information from `InitSID.utl`.
4. SAP HANA sends data to the hdbbackint processes.
5. Hdbbackint sends the data to the IBM Spectrum Protect server through the IBM Spectrum Protect API.

All the database and redo log backup information is stored by SAP HANA in the backup catalog. The backup history can be viewed in the SAP HANA Studio in the **Backup** tab or by querying the database view `M_BACKUP_CATALOG`. For more information about hdbbackint, see *SAP HANA Administration Guide*.

The configuration of the hdbbackint process is stored in the `initSID.utl` profile file. This file contains information that describes how to run backup and restore operations, and it can be customized for your SAP HANA environment.

The hdbbackint process requires that the Data Protection for SAP HANA ProLE process is running. The ProLE process coordinates multiple hdbbackint instances in a full database backup. The process ensures that all backup objects that belong to the same full database backup are assigned to the same backup ID. The full database backup is handled as a single entity even though it consists of many single objects.

2.3.3 IBM Spectrum Protect server

When setting up the IBM Spectrum Protect server for use with IBM Spectrum Protect for Enterprise Resource Planning (ERP), the following considerations help optimize performance. Consider these items when setting up the IBM Spectrum Protect server. Data Protection for SAP uses the IBM Spectrum Protect archive function for all backup activities.

- Dedicated backup server for multiple clients
- CPU power
- Storage hierarchy

> **Tip:** For the necessary hardware and software requirements and setup instructions, see IBM Spectrum Protect Blueprints and Sizing.

Figure 2-8 shows the IBM Spectrum Protect components and storage pool types and how they provide data reduction capabilities for backing up SAP HANA.

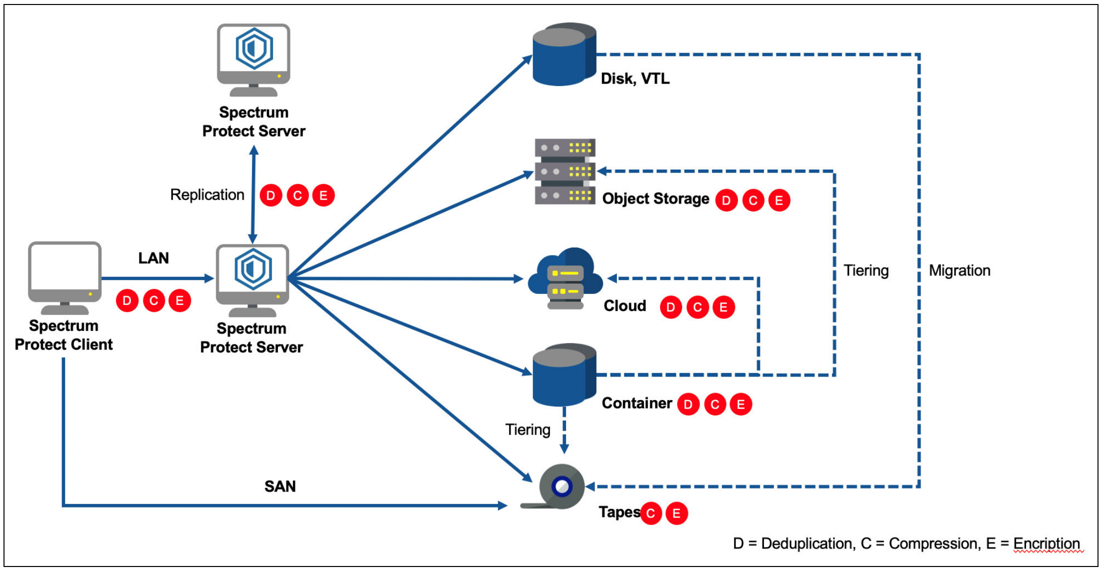


Figure 2-8 IBM Spectrum Protect server components

2.3.4 IBM Spectrum Protect for Enterprise Resource Planning

IBM Spectrum Protect for ERP provides application integration to protect SAP environments that use IBM Db2®, Oracle, or SAP HANA as a data back end.

The requirements for Data Protection for SAP HANA are available in hardware and software technotes for each release. To review the hardware and software requirements technote for your version, see Hardware and Software Requirements: Version 8.1 IBM Spectrum Protect for Enterprise Resource Planning.

Note: From the page, follow the link to the technote for your release or update level.

IBM Spectrum Protect for ERP is installed on all nodes of the solution, and it acts as an interface between the SAP HANA environment and the IBM Spectrum Protect Server.

Data Protection for SAP HANA retrieves data directly from SAP HANA through named pipes and sends this data to the IBM Spectrum Protect server without storing that data on a local disk. The backup is physically separated from the SAP HANA node to provide better geographical distance, which is also true for the restore operation.

Backups and restores are started from and controlled from SAP HANA Studio or SAP HANA Cockpit interfaces.

2.4 Protecting an SAP HANA database with IBM Spectrum Copy Data Management

This section provides an overview on the SAP HANA data snapshot feature and the IBM Spectrum Copy Data Management software that is used for supporting the backup snapshot by using the hardware snapshot function of modern storage subsystems like IBM Spectrum Virtualize and generating copies for various use cases, including backup, recovery, and cloning. IBM Spectrum Protect Snapshot can also offer extra support for snapshot backups on IBM POWER environments running SAP HANA when using the Custom Application Agent. For more information about IBM Spectrum Protect Snapshot for Custom Applications, see Tivoli Storage FlashCopy Manager.

2.4.1 Overview on SAP HANA data snapshot

Data snapshots offer an extra option to protect the SAP HANA data area and recover an SAP HANA database. The data snapshot capability of SAP HANA offers the following advantages:

- Minimal impact on database performance. Data snapshots are created in the storage system and do not consume database resources.
- Fast recovery time. The operation is assisted by the storage snapshot services, which takes place in a short period compared to the recovery of the data backup where the backup data is transferred as a block level from the recovery media (file or Backint) to the target recovery system.

When generating a data snapshot, the following steps occur:

1. An internal database snapshot is created that reflects a consistent state of the data area on the file system. A `backup_ID` is associated with the internal snapshot in the backup catalog with the state `PREPARED`.
2. The data snapshot is created with the support of the storage services. The snapshot contains the data area. During data snapshot recovery, only the data area is restored from the snapshot, but it is possible to apply more logs from the log recovery area.
3. Confirm or abandon the data snapshot. This operation updates the backup catalog with a success or fail status of the snapshot backup operation and releases the internal database snapshot to create optionally further data snapshots or data backups. If an internal database snapshot exists, then no new data snapshots or data backups can be created until the release of the current internal snapshot.

Data snapshots are updated in the backup catalog with the tag `SNAPSHOT`, so they are uniquely identified among the other backup solutions (Backint or file). They participate in backup generations like the full (complete) data backups. Also, according to SAP HANA documentation, even if the internal database snapshot is used for SAP HSR, that does not conflict with the data snapshot. There is no relationship between these two types of internal database snapshots.

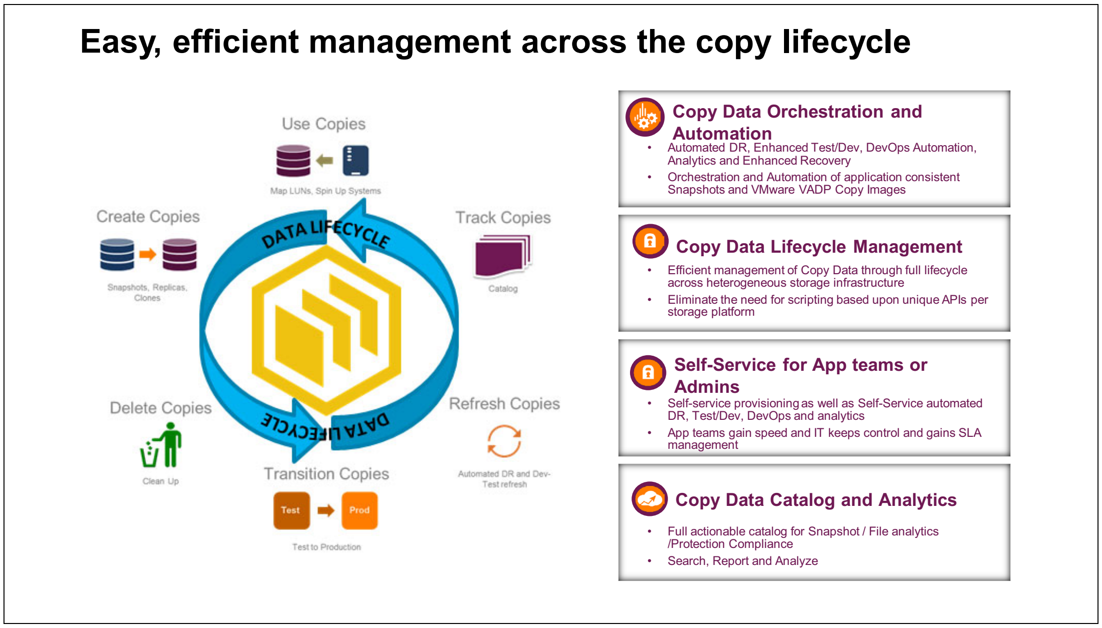
> **Note:** Starting with SAP HANA 2.0 SPS 04, creating a database snapshot is supported for the system database and all tenant databases. You cannot restore a single tenant database from a data snapshot, so recovery is performed for the system and all tenant databases. Previous versions of SAP HANA 2.0 support only single tenant databases for the data snapshot operation.

Currently, the data snapshot operation is supported by native SQL statements. For more information, see Create a Data Snapshot (Native SQL).

2.4.2 IBM Spectrum Copy Data Management

IBM Spectrum Copy Data Management delivers “in-place” copy data management to various enterprise storage arrays from multiple vendors, such as IBM, EMC, HPE Nimble Storage, NetApp, and Pure Storage, allowing the IT team to use its existing infrastructure and data in a manner that is efficient, automated, scalable, and easy to use. IBM Spectrum Copy Data Management offers a complete automation process that makes data copies available to users when and where they need them. It avoids creating unnecessary copies or leaving unused copies on the storage.

Figure 2-9 presents an overview of the major functions of IBM Spectrum Copy Data Management.



Easy, efficient management across the copy lifecycle

Copy Data Orchestration and Automation

- Automated DR, Enhanced Test/Dev, DevOps Automation, Analytics and Enhanced Recovery
- Orchestration and Automation of application consistent Snapshots and VMware VADP Copy Images

Copy Data Lifecycle Management

- Efficient management of Copy Data through full lifecycle across heterogeneous storage infrastructure
- Eliminate the need for scripting based upon unique APIs per storage platform

Self-Service for App teams or Admins

- Self-service provisioning as well as Self-Service automated DR, Test/Dev, DevOps and analytics
- App teams gain speed and IT keeps control and gains SLA management

Copy Data Catalog and Analytics

- Full actionable catalog for Snapshot / File analytics /Protection Compliance
- Search, Report and Analyze

Figure 2-9 Complete copy automation with IBM Spectrum Copy Data Management

The solution catalogs copy data from across local, off-site, or hybrid cloud infrastructures. It identifies duplicates and compares copy requests to existing copies. This process ensures that the minimum number of copies is created to service the various business needs. Copy processes and workflow are automated to ensure consistency and reduce complexity.

IBM Spectrum Copy Data Management is deployed as an agentless virtual machine (VM) in a VMware environment as an Open Virtualization Format (OVF) template, which enables a fast deployment. The data consumers can use the web interface to the self-service portal to create and manage the data copies as needed.

IBM Spectrum Copy Data Management workflow

A typical IBM Spectrum Copy Data Management workflow includes the following operations:

- Access the IBM Spectrum Copy Data Management interface by using the web browser:

  ```
  https://<CDM_hostname>:8443/portal/
  ```

  `<CDM_hostname>` is the hostname or IP address of the VM where IBM Spectrum Copy Data Management is deployed.

- Register a provider. The operation adds a provider in the IBM Spectrum Copy Data Management inventory. A provider can be an application service such as an SAP HANA database; a storage device such as IBM Spectrum Virtualize; a VMware ESX resource; or a cloud provider. Consult the product documentation for the latest IBM Spectrum Copy Data Management version for a complete list of providers.
- Create an inventory job definition. An inventory job definition provides the framework to collect and catalog information about objects on a registered provider.
- Run a job. The inventory job is run to collect information about the register provider and store it in the IBM Spectrum Copy Data Management database.
- Generate reports. This operation provides information about the cataloged nodes and the data and resources on them.
- Define the service-level agreement (SLA) policies. SLA policies allow storage and virtualization administrators to create customized templates for the key processes that are involved in creation and use of backup jobs. Copy types, destinations, parameters, frequency, and retention policies are configured in the SLA policies, which can be reused in the backup jobs.
- Run a backup. This job generates copies of data based on the selected SLA policy. The job can be scheduled for a specific date and time with a frequency that is defined in the SLA policy. The job advanced parameters allow integration of data copy generation on the target device with pre-scripts and post-scripts applicable at job-level and snapshot-level operations.
- Run a restore. Leverages IBM Spectrum Copy Data Management technology for testing, cloning, and recovering the copy of the data. The restore job provides various processing options regarding the mount points for the data copy, failure, and cleanup options, pre-scripts and post-scripts on the job execution, storage-specific options for the data copies, notifications on the job result on mail, and well scheduling options.

2.4.3 SAP HANA backup and recovery with IBM Spectrum Copy Data Management

This section details the SAP HANA backup and recovery features that are based on IBM Spectrum Copy Data Management.

SAP HANA and IBM Spectrum Copy Data Management overview

Figure 2-10 provides an overview of the infrastructure that is used for SAP HANA on IBM Power Systems and IBM Spectrum Copy Data Management.

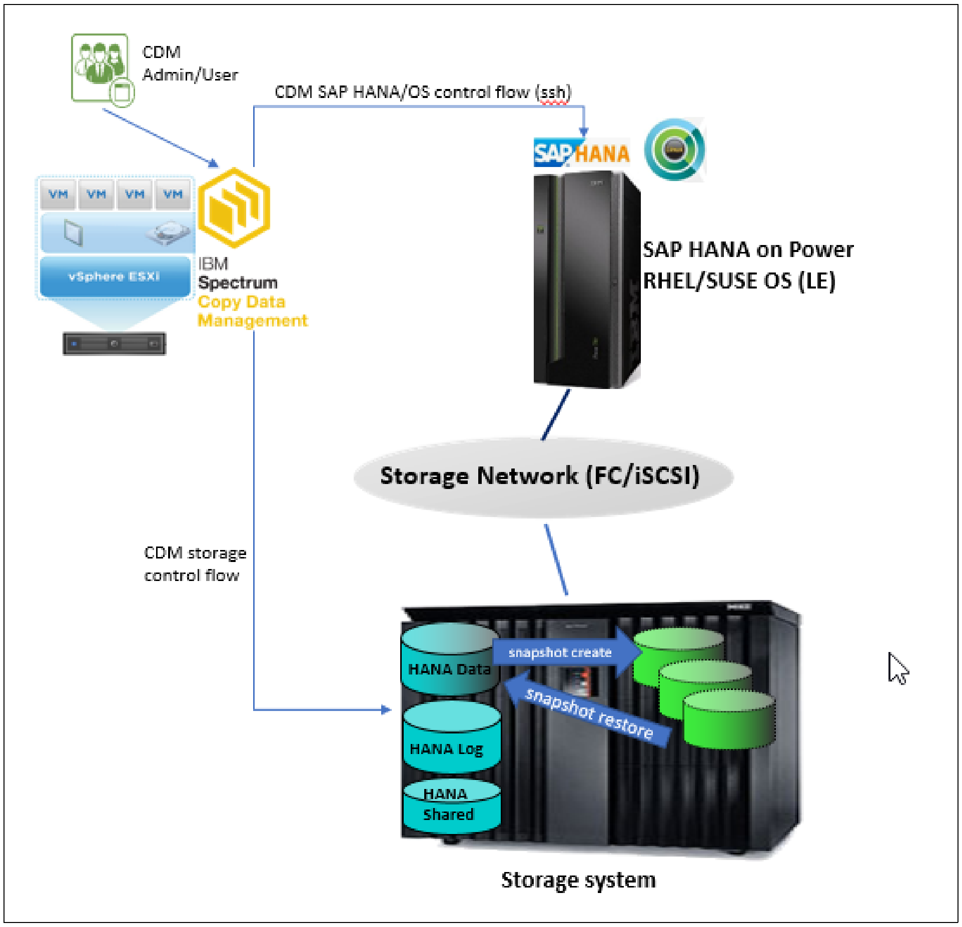


Figure 2-10 SAP HANA and IBM Spectrum Copy Data Management infrastructure overview

IBM Spectrum Copy Data Management runs in a VM on a VMware environment, enabling a fast deployment of the software in the target environment. For the updated list of supported versions of VMware, see IBM Spectrum Copy Data Management 2.2.11.

The users can access the IBM Spectrum Copy Data Management server by using a web browser interface for performing the copy data management operations by accessing the following URL:

```
https://<CDM_hostname>:8443/portal/
```

IBM Spectrum Copy Data Management integration with SAP HANA requires connectivity with the SAP HANA database server by using SSH, an OS user (for example, an IBM Spectrum Copy Data Management agent user) who is predefined on the system with root privileges who uses `sudo`, and a database user who accesses the SAP HANA database by using the local SAP HANA client. This communication is used for discovery and inventory services for the OS and SAP HANA resources, and coordination of the storage snapshot operations with the SAP HANA database. During the backup job, an internal database snapshot is generated in SAP HANA 2.4.1, “Overview on SAP HANA data snapshot” on page 15) to ensure a consistent state of the database data area on disk. During the restore phase, IBM Spectrum Copy Data Management performs the OSs tasks that are required to mount the storage snapshot for SAP HANA database recovery.

IBM Spectrum Copy Data Management also requires connectivity with a storage system on the management interface to perform the storage snapshot-related operations. IBM storage providers use port 22 to communicate with IBM Spectrum Copy Data Management. When performing the storage snapshot, IBM Spectrum Copy Data Management determines the disks that are associated with the database data area for this operation. You must maintain the proper database storage layout to separate the data and log disks, and maintain log backups, which can be applied during database snapshot recovery.

Notes:

- When a backup is performed on a multitenant environment (MDC), the system database along with the tenant database are part of the same snapshot operation. The restore also takes place for both. A tenant database cannot be restored independently from a snapshot.
- In IBM Spectrum Copy Data Management V2.2.11, SAP HANA transaction logs can be backed up and restored. When selected, IBM Spectrum Copy Data Management backs up the database logs to an indicated location, and then it protects the underlying disks of the log backups. With this feature, you can perform point-in-time (PiT) restores of SAP HANA databases.

Supported configurations for IBM Spectrum Copy Data Management

The following versions of SAP HANA are supported by IBM Spectrum Copy Data Management V2.2.11 on IBM Power Systems running Little Endian (LE) OSs (in physical or VMs):

- SAP HANA 2.0 SPS 02
- SAP HANA 2.0 SPS 03
- SAP HANA 2.0 SPS 04

Notes:

- IBM Spectrum Copy Data Management V2.1.11 supports only one tenant in MDC setups in addition to the system database.
- SAP HANA 1.0 on IBM Power Systems uses Linux Big Endian (BE) edition and is not supported by IBM Spectrum Copy Data Management. For specific cases, you can also consider the IBM Spectrum Protect Snapshot with Custom Application capability. For more information, see Tivoli Storage FlashCopy Manager.

The following OSs are supported by IBM Spectrum Copy Data Management software with SAP HANA 2.0 on IBM Power Systems:

- Red Hat Enterprise Linux 7.0+
- SUSE Linux Enterprise Server 12+

The following extra considerations apply for determining the appropriate version and minimum update level that is required for the OS:

- Verify the *IBM Spectrum Copy Data Management User's Guide* for the current release on supported SAP HANA and OSs versions at IBM Spectrum Copy Data Management documentation.
- Consult SAP Note 2235581 - SAP HANA: Supported Operating Systems on sections that are related to IBM Power Systems servers at SAP Notes.
- For supported distributions and minimum versions on IBM POWER8® and IBM POWER9™ servers, see Supported Linux distributions and virtualization options for POWER8 and POWER9 Linux on Power Systems.

Here are the supported IBM Storage Systems with IBM Spectrum Copy Data Management V2.2.11 and SAP HANA on IBM Power Systems:

- IBM Storage Systems running IBM Spectrum Virtualize Software V7.3 and later or V8.1.2 and later releases, including IBM SAN Volume Controller, IBM Storwize®, and IBM FlashSystem® V9000 and 9100 series.
- IBM Storage Systems running IBM Spectrum Accelerate V11.5.3 and later, including IBM FlashSystem A9000/A9000R and IBM XIV® Storage Systems.

IBM Spectrum Copy Data Management supported storage connectivity for an SAP HANA server with a storage subsystem is Fibre Channel (FC) or iSCSI. Virtual Fibre Channel (N_Port ID Virtualization (NPIV)) on IBM Power Systems servers that use IBM PowerVM® is also supported.

IBM Spectrum Copy Data Management configuration for SAP HANA

This section focuses on the major configuration activities and options that are required for IBM Spectrum Copy Data Management with SAP HANA and IBM Storage. This section supplements the *IBM Spectrum Copy Data Management User's Guide*, which can be found at IBM Spectrum Copy Data Management documentation.

Prerequisites

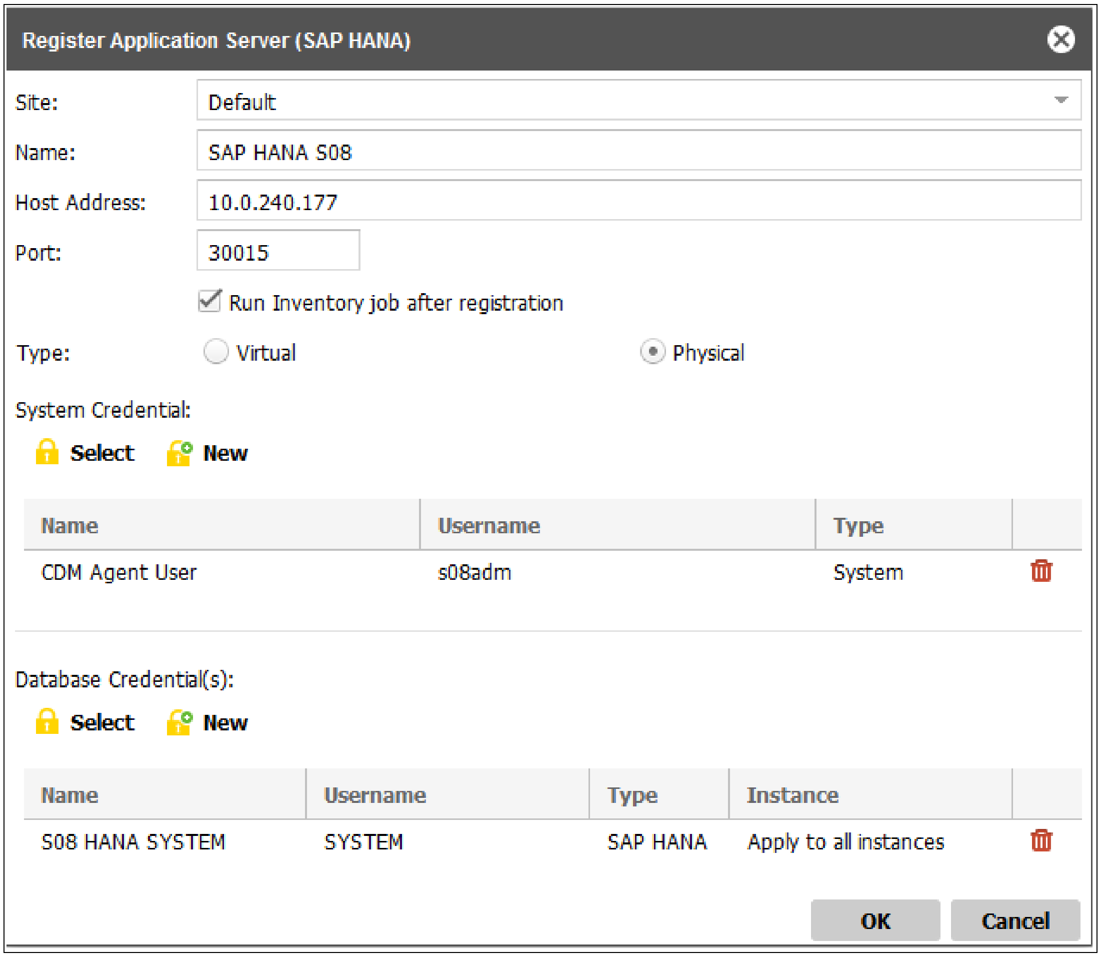
Ensure that all prerequisites are in place before registering the SAP HANA instance with IBM Spectrum Copy Data Management and running the inventory job on the server. They include the following components:

- The software packages that are required to be installed on the SAP HANA system: **`bash`**, **`sudo`** (minimum of version 1.7.6p2), and Python Version 2.6.x or 2.7.x and extra packages that are specific to Red Hat Enterprise Linux or SUSE Linux Enterprise Server versions according to the *IBM Spectrum Copy Data Management User's Guide*.
- SAP HANA client (hdbclient) must be installed. For SAP HANA SPS 04, the hdbcli module must also be installed.
- OS user (Agent User) is required by IBM Spectrum Copy Data Management to perform OS activities during backup, restore, and inventory jobs. This user must have root privileges to use **`sudo`** without being asked for a password, and attribute **`!requiretty`** must be set in the `sudoers` file. Users can be registered with IBM Spectrum Copy Data Management based on user/password credentials or by using key-based authentication.
- For the connectivity between the IBM Spectrum Copy Data Management server and SAP HANA database, the SSH service must be running on port 22 on the SAP HANA server, and any firewalls must be configured to allow IBM Spectrum Copy Data Management to connect to the server by using SSH. The SFTP subsystem for SSH must also be enabled.
- xfsprogs (minimum of Version 4.2.0) for database and file restores from XFS file systems.

For more information about your operating environment, see the SAP HANA Requirements section in the *IBM Spectrum Copy Data Management User's Guide* at IBM Spectrum Copy Data Management documentation.

Registering the SAP HANA provider

To access the registration menu for SAP HANA, go to the web interface, select the **Configure** tab, select **Sites & Providers** → **Application Servers**, right-click, and select **Register**. A window opens and shows the available application server types. Select **SAP HANA**, as shown in Figure 2-11.



Register Application Server (SAP HANA)

Site: Default

Name: SAP HANA S08

Host Address: 10.0.240.177

Port: 30015

☑ Run Inventory job after registration

Type: ○ Virtual ● Physical

System Credential:

Name	Username	Type
CDM Agent User	s08adm	System

Database Credential(s):

Name	Username	Type	Instance
S08 HANA SYSTEM	SYSTEM	SAP HANA	Apply to all instances

Figure 2-11 SAP HANA provider registration in IBM Spectrum Copy Data Management

The following parameters are required:

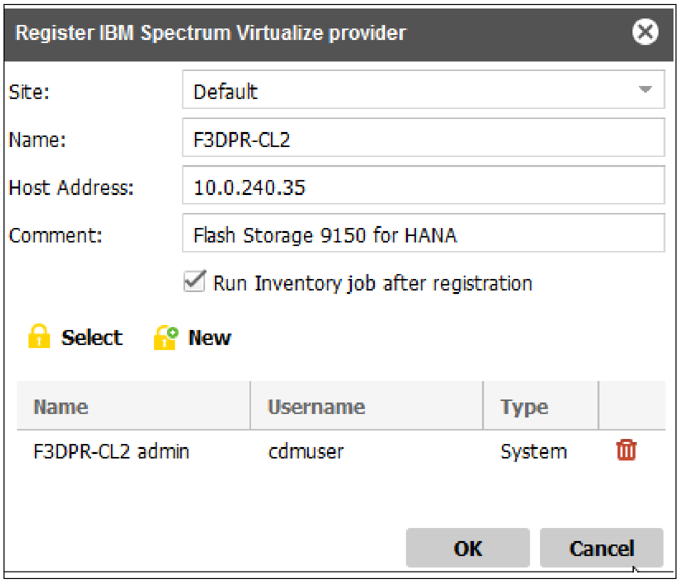
- Site: Defines a grouping of providers based on their location. You must select from the defined sites or use the **Default** one.
- Name: Provide a name for the SAP HANA provider in IBM Spectrum Copy Data Management.
- Host address: Provide the DNS name or IP address of the SAP HANA database server.
- Port: The format for the port number is 3<instance number>15. For example, if the instance number is 00, then the port number that is used is 30015.

- The system credentials are the OS user credentials that are required to access the system. These credentials are used to log in to the system and perform the OS-specific operations during inventory, backup, or restore operations.
- The database credentials are used for querying the database and performing the copy operations. The user must have sufficient privileges to access the database.

By default, the inventory job is checked in the registration window, so it is automatically started after the registration process.

Registering the storage provider

A similar process is required for registering the storage system that is used by the SAP HANA database (Figure 2-12) with IBM Spectrum Copy Data Management.



Register IBM Spectrum Virtualize provider

Site: Default

Name: F3DPR-CL2

Host Address: 10.0.240.35

Comment: Flash Storage 9150 for HANA

☑ Run Inventory job after registration

Name	Username	Type
F3DPR-CL2 admin	cdmuser	System

Figure 2-12 Registering an IBM Spectrum Virtualize provider

Important: For the registration process and the IBM Spectrum Copy Data Management jobs operating environment, always consider the time alignment between IBM Spectrum Copy Data Management, the storage device, and SAP HANA. Use the respective component operating guide for setting up the appropriate date, time, and time zone.

Defining the SLA policy

Before defining a backup job for SAP HANA, an SLA policy must be defined. Copy types, destinations, and parameters are configured in SLA policies, which can be reused in backup jobs. Initially, when defining a SLA policy you must select the storage provider, and extra copy type options depend on the storage provider that is selected, as shown in the selection window for IBM Spectrum Copy Data Management 2.2.11 in Figure 2-13.

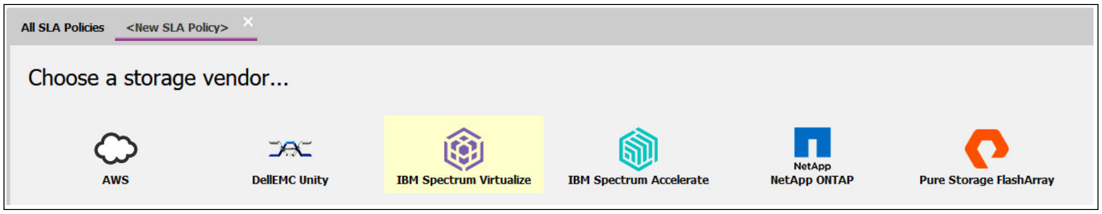
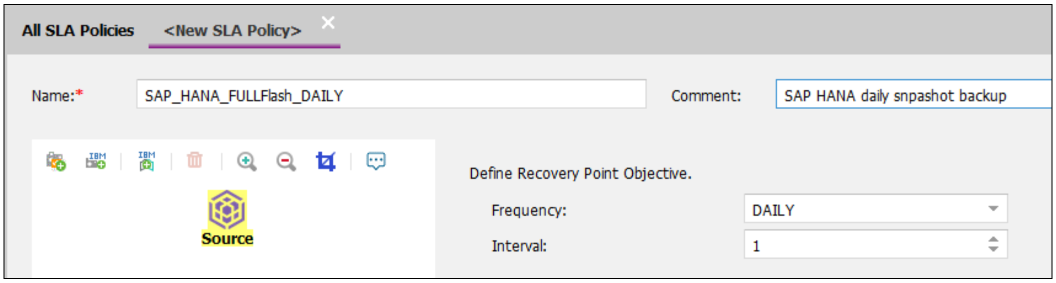


Figure 2-13 Selecting the storage vendor

The following configuration examples refer to a typical snapshot backup environment for SAP HANA that uses an IBM Spectrum Virtualize storage provider and local IBM FlashCopy.

Within an SLA policy, the following parameters are required:

- RPO: Figure 2-14 shows the following details:
  - Frequency of the data copy operation: Starting MINUTE, HOURLY, WEEKLY, or MONTHLY.
  - Interval number: The frequency determines how often the data copy operation takes place.



Name:* SAP_HANA_FULLFlash_DAILY

Comment: SAP HANA daily snpashot backup

Define Recovery Point Objective.

Frequency: DAILY

Interval: 1

Figure 2-14 SLA policy: Establishing the RPO for the copy operation

- Add a copy type for the source data. Right-click the **Source** object to see extra options, as shown in Figure 2-15. Depending on the storage provider, various options are available for local snapshot or remote copy of data to other storage (replication). The following options are available for IBM Spectrum Virtualize:
  - Add FlashCopy: Local snapshot on the IBM Spectrum Virtualize device.
  - Add Global Mirror with Change Volume: Data copy that uses remote replication. The replication type of Global Mirror with Change Volume is specific for the IBM Spectrum Virtualize family. For more information about supported copy services features on IBM Spectrum Virtualize, see Metro Mirror and Global Mirror.
  - VM Replication: Applies to a VMware environment.

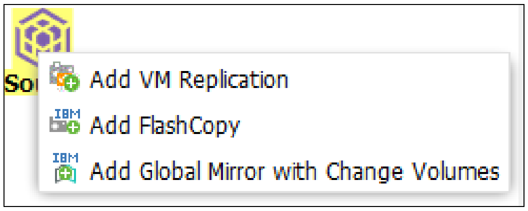
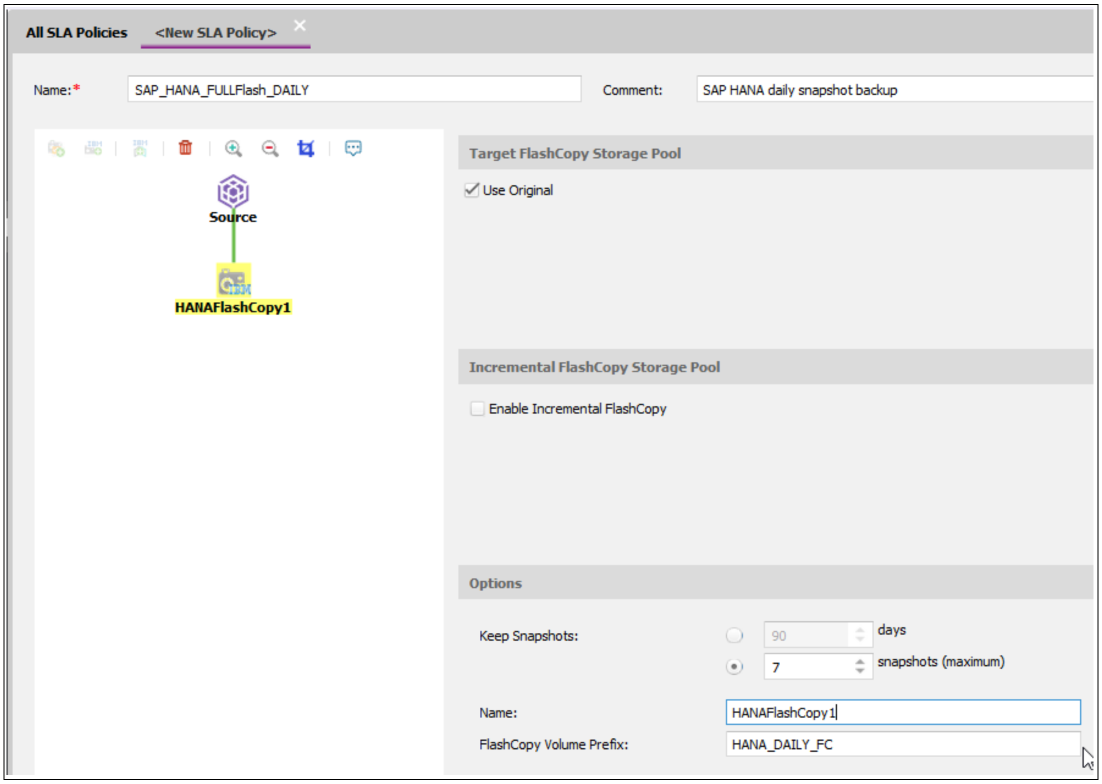


Figure 2-15 Selecting the copy type for the source data

- There are extra options for the copy type that is selected in the previous bullet. For FlashCopy operations, there are options for selecting the target storage pool or using the same source volumes (**Use original**) or for using the full volume FlashCopy or incremental FlashCopy type.
- Retention options: Retention can be set by duration (number of days) or a number of versions. For more information, see 2.5.2, “SAP HANA backup retention policies” on page 31.

Figure 2-16 shows a set of options for an SLA policy with regular (full) FlashCopy that uses the original pool for the target FlashCopy volumes and a retention policy with a maximum of seven copies to be kept on the storage system.



Name:* SAP_HANA_FULLFlash_DAILY

Comment: SAP HANA daily snapshot backup

Target FlashCopy Storage Pool

☑ Use Original

Incremental FlashCopy Storage Pool

☐ Enable Incremental FlashCopy

Options

Keep Snapshots: ○ 90 days

● 7 snapshots (maximum)

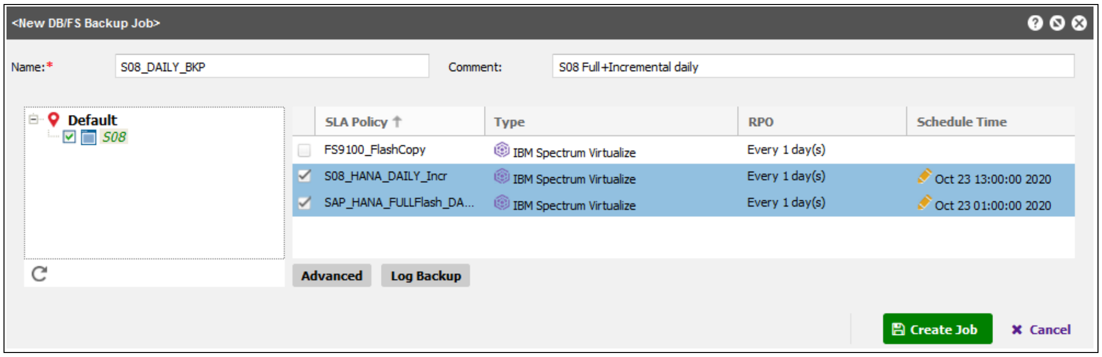
Name: HANAFlashCopy1

FlashCopy Volume Prefix: HANA_DAILY_FC

Figure 2-16 SLA policy settings for FlashCopy and retention policies

Defining an SAP HANA backup job

A backup job for SAP HANA can be defined to run the snapshot backup of the database at a scheduled time. During the new job definition, the IBM Spectrum Copy Data Management SAP HANA application instance is associated with the SLA available policies. More than one SLA policy can be applied for a job, as shown in Figure 2-17, where two types of snapshots are taken daily at 12 hours interval: one regular FlashCopy and one incremental.



Name:* S08_DAILY_BKP

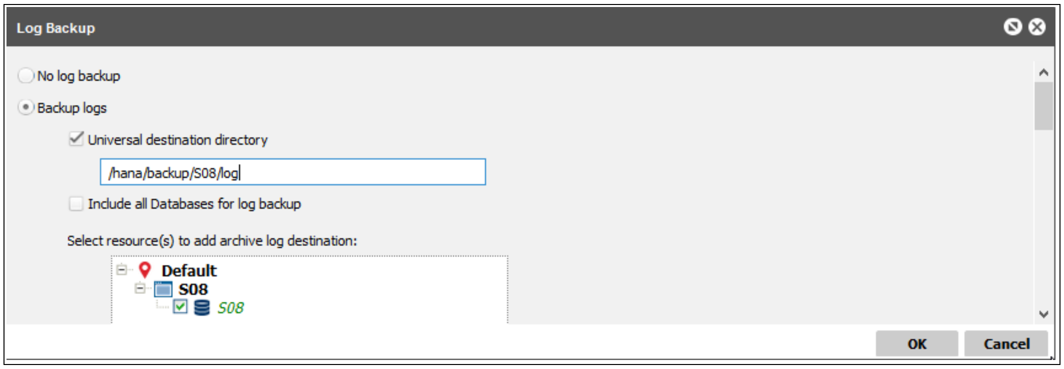
Comment: S08 Full+Incremental daily

	SLA Policy	Type	RPO	Schedule Time
☐	FS9100_FlashCopy	IBM Spectrum Virtualize	Every 1 day(s)	
☑	S08_HANA_DAILY_Incr	IBM Spectrum Virtualize	Every 1 day(s)	Oct 23 13:00:00 2020
☑	SAP_HANA_FULLFlash_DA...	IBM Spectrum Virtualize	Every 1 day(s)	Oct 23 01:00:00 2020

Figure 2-17 Defining a backup job for SAP HANA snapshot backup

Starting with IBM Spectrum Copy Data Management V2.2.11, log backup is also supported. When log backup is enabled in an IBM Spectrum Copy Data Management backup job and a new location is specified, the configuration of SAP HANA is changed during the job first run. The `global.ini` file is updated for SYSTEMDB and the tenant database with the new locations of the backup log and backup catalog. The log backup can be configured from the previous menu (see Figure 2-17 on page 24). When configuring the log backup with an IBM Spectrum Copy Data Management backup job, the following parameters are specified:

- Universal destination directory: You can specify an existing directory for the log backup or not. The current values for the target locations of the SAP HANA log backup and catalog backup are used. The catalog subfolder must exist, and it needs appropriate permissions from SAP HANA database instance owner. For more information, see the “Prerequisites” section for SAP HANA backup in the *IBM Spectrum Copy Data Management User’s Guide*, found at IBM Spectrum Copy Data Management documentation. The **Universal destination directory** can be applied to multiple SAP HANA instances running on multiple servers.
- Include and exclude options: Select the **Include all Databases for log backup** checkbox, which enables the exclusion option so that you can specify whether any databases should be excluded. If you do not check the box, you can specify the resources to be included, as shown in Figure 2-18.



Log Backup

○ No log backup

● Backup logs

☑ Universal destination directory

/hana/backup/S08/log

□ Include all Databases for log backup

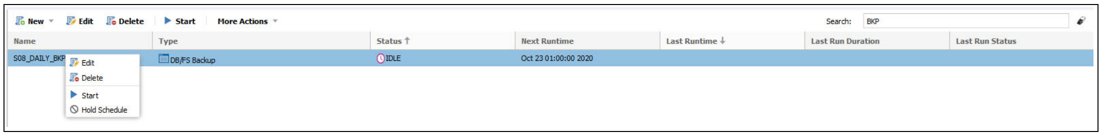
Select resource(s) to add archive log destination:

- Default
  - S08
    - ☑ S08

Figure 2-18 IBM Spectrum Copy Data Management log backup

More options may be accessed from the backup job main window (Figure 2-17 on page 24) by clicking **Advanced**. You can provide pre-scripts and post-scripts at job and snapshot levels, and also notifications to a mail server for the job run result.

The jobs that are defined for backup and their runs can be monitored from the **Jobs** tab, as shown in Figure 2-19. An IBM Spectrum Copy Data Management job can be manually started (for example, when taking a manual, on-demand backup) or it can be removed from the current scheduling cycle by applying the **Hold Schedule** action.



Search: BKP

Name	Type	Status ↑	Next Runtime	Last Runtime ↓	Last Run Duration	Last Run Status
S08_DAILY_BKP	DB/FS Backup	IDLE	Oct 23 01:00:00 2020			

Figure 2-19 IBM Spectrum Copy Data Management jobs and available actions for a job

> **Note:** Running the backup job requires the SAP HANA instance and the tenant database is protected by the snapshot backup to be started (active), or the IBM Spectrum Copy Data Management job fails.

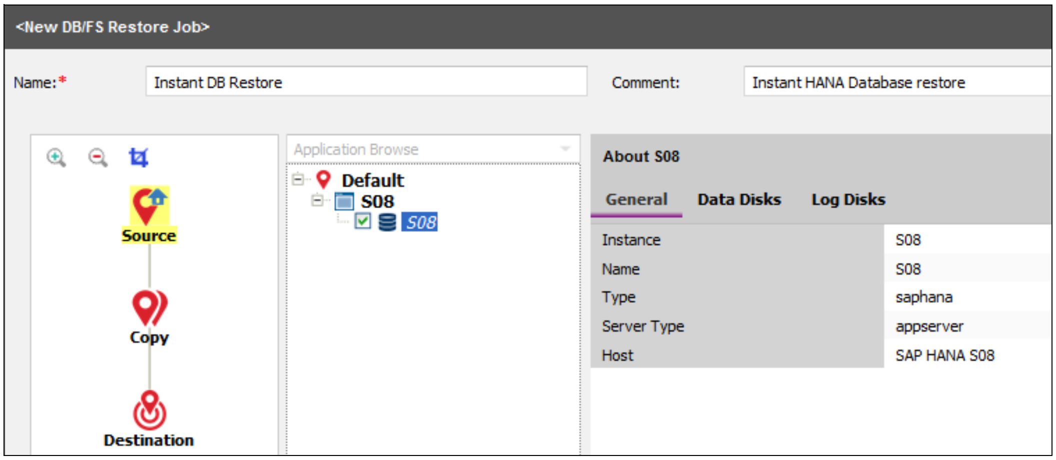
Defining a restore job

To restore the SAP HANA database, you must define an IBM Spectrum Copy Data Management restore job. IBM Spectrum Copy Data Management supports two types of restore jobs:

- Instant database restore: An instant database restore operation restores the database to an immediate usable state. The database is recovered as part of the restore operation. The database is restored at the PiT that the snapshot was created, and no further logs can be applied. This type of restore is useful for scenarios such as restoring an original system from a reference backup or PiT snapshot, restoring a production database to a test system, or database cloning.
- Instant disk restore: This restore job mounts the snapshot data from storage to the database server with ability to access and check the data, copy it, or put it into production. SAP HANA database recovery must be performed manually. The recovery logs can be applied from a log recovery area if it is available, or if you use the log backup function, the log backup volumes are also made available to the host. The restore process allows applying redo logs to recover the database to a specific PiT.

Selecting one of the two templates is the primary operation in the job definition flow. In the next step, you must provide extra parameters for the restore job definition:

1. Select the source of the data copy on the SAP HANA system that is restored, as shown in Figure 2-20. More details can be displayed, including the disks that are mapped to data, and the log area for the selected SAP HANA instance.



<New DB/FS Restore Job>

Name:* Instant DB Restore

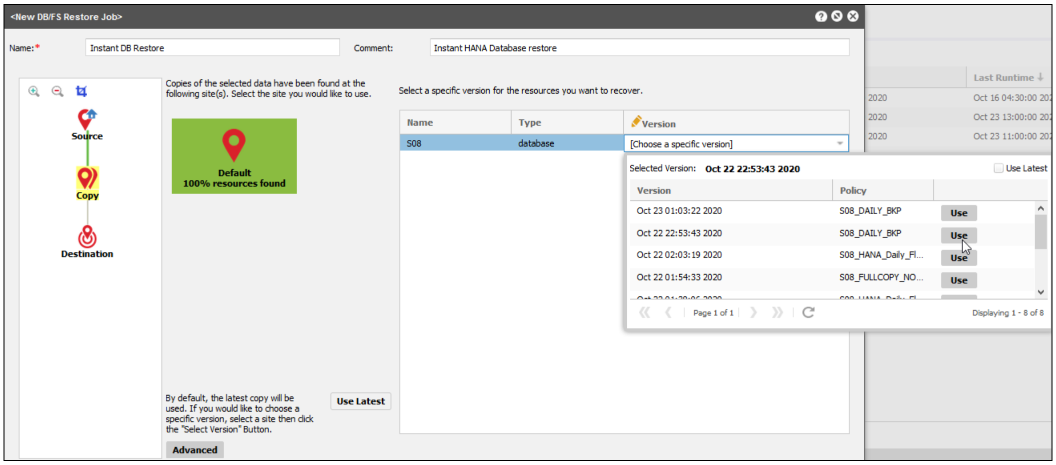
Comment: Instant HANA Database restore

About S08

Instance	S08
Name	S08
Type	saphana
Server Type	appserver
Host	SAP HANA S08

Figure 2-20 Selecting the source SAP HANA system of the snapshot backups

2. Select the copy of the data that you want to use. If the data is replicated, you can select a data copy from a different location than the source. By default, the latest snapshot version is selected, but you can select a specific PiT version, as shown in Figure 2-21 on page 27.



<New DB/FS Restore Job>

Name:* Instant DB Restore

Comment: Instant HANA Database restore

Copies of the selected data have been found at the following site(s). Select the site you would like to use.

Select a specific version for the resources you want to recover.

Name	Type	Version
S08	database	[Choose a specific version]

Selected Version: **Oct 22 22:53:43 2020** □ Use Latest

Version	Policy	
Oct 23 01:03:22 2020	S08_DAILY_BKP	Use
Oct 22 22:53:43 2020	S08_DAILY_BKP	Use
Oct 22 02:03:19 2020	S08_HANA_Daily_Fl...	Use
Oct 22 01:54:33 2020	S08_FULLCOPY_NO...	Use

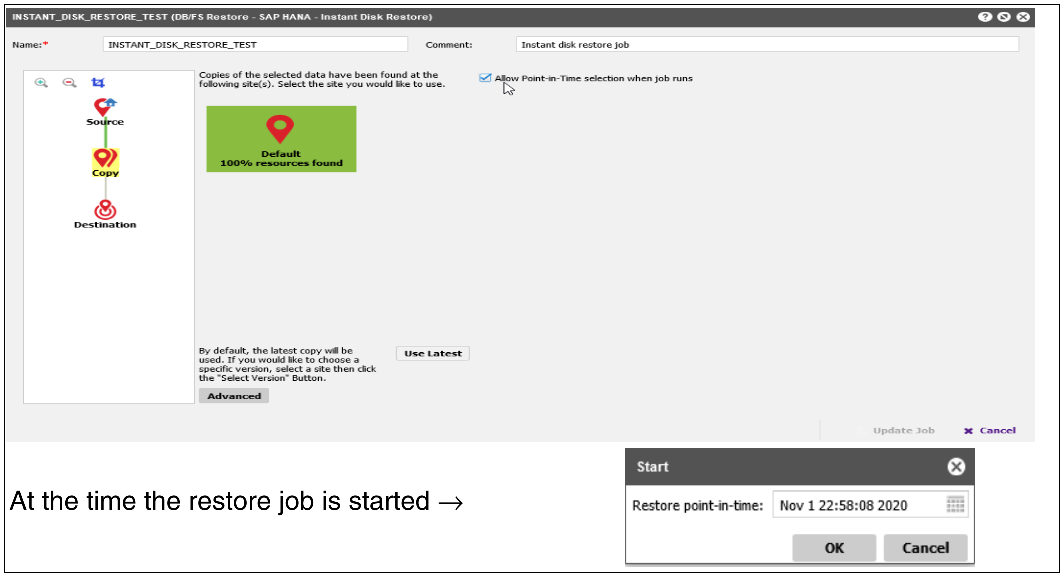
Page 1 of 1 Displaying 1 - 8 of 8

By default, the latest copy will be used. If you would like to choose a specific version, select a site then click the "Select Version" Button.

Figure 2-21 Selecting the copy version to be used for restore

> **Note:** Starting with IBM Spectrum Copy Data Management V2.2.11, you can use the log backup feature to include the log backup volume snapshot with the SAP HANA data snapshot. With this feature, you can make a PiT recovery of an SAP HANA database between two consecutive snapshots by mounting at restore time the SAP HANA data snapshot with the next in time snapshot of the log backups.

PiT recovery is enabled in the Instant Disk Restore template when you provide the copy of data to be used by selecting the **Allow Point-in-Time selection when job runs** checkbox, as shown in Figure 2-22. When the check box is selected, there is no option to select a snapshot copy version from the list of available snapshots, and the user is prompted to specify a PiT when the restore job is started.



INSTANT_DISK_RESTORE_TEST (DB/FS Restore - SAP HANA - Instant Disk Restore)

Name:* INSTANT_DISK_RESTORE_TEST

Comment: Instant disk restore job

Copies of the selected data have been found at the following site(s). Select the site you would like to use.

☑ Allow Point-in-Time selection when job runs

By default, the latest copy will be used. If you would like to choose a specific version, select a site then click the "Select Version" Button.

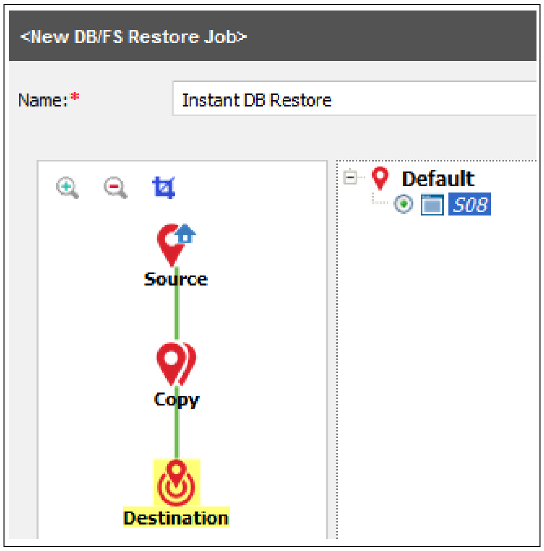
At the time the restore job is started →

Start

Restore point-in-time: Nov 1 22:58:08 2020

Figure 2-22 Selecting the point-in-time recovery option in the restore job

The destination SAP HANA system where the selected data copy is applied is shown in Figure 2-23.



Name:* Instant DB Restore

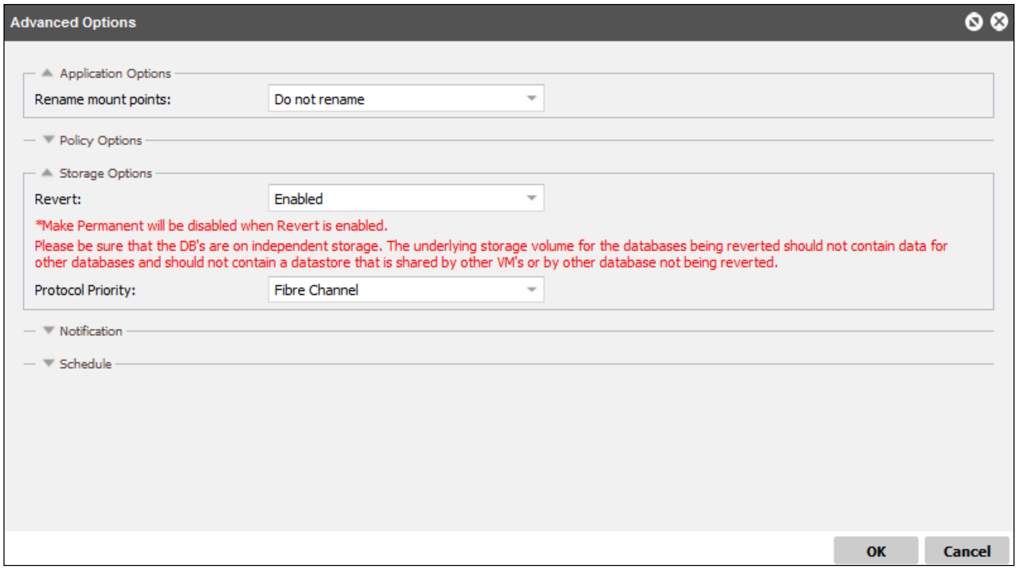
Figure 2-23   Destination SAP HANA system to which to apply the snapshot restore

There are also more advanced options for the restore jobs where an IBM Spectrum Copy Data Management user can select various options for the restore process:

- Application options: You can provide rename options for the mount point of the SAP HANA database data file system, such as append a timestamp (default), do not change the mount point or append a suffix or prefix, or replace a substring (for example, ‘PROD’ with ‘TEST’).
- Policy options: You can provide extra pre-scripts and post-scripts for the restore process.
- Storage options:
  - Make Permanent: The database recovery operations can take advantage of prod (Enabled), or test (Disabled) mode and then either be deleted or promoted to permanent (prod) mode. This option specifies whether the volumes hosting the cloned database after the restore are used as FlashCopy targets (can be easily canceled) or promoted to volume copies that are fully synchronized with the snapshot source data and at the end running independently.
  - Revert: If enabled, the restore job performs a reverse copy of data on the storage system from the target to the source volumes, which overwrites the original database data volumes with the content of the snapshot copy.
  - Protocol priority: FC or iSCSI. If more storage network protocols are available, select the one to take priority on the restore job.

> **Note:** The Make Permanent and Revert options cannot be enabled concurrently because they are mutually exclusive. You can choose the **User Selection** option on both, which leaves the decision to be made later after mounting the file systems on the target system.

Figure 2-24 shows an example of the options that are used for an Instant Database Restore template for a production system with the **Revert** option enabled, and using the same mount point name for the SAP HANA data as the original mount point. Hence, the job restores the database with the selected snapshot image onto the original volumes.



Advanced Options

Application Options

Rename mount points: Do not rename

Policy Options

Storage Options

Revert: Enabled

*Make Permanent will be disabled when Revert is enabled.

Please be sure that the DB's are on independent storage. The underlying storage volume for the databases being reverted should not contain data for other databases and should not contain a datastore that is shared by other VM's or by other database not being reverted.

Protocol Priority: Fibre Channel

Notification

Schedule

Figure 2-24 Advanced storage options

- Notification options: Job results can be sent to specify mail server and recipients. The mail server must be defined as an SMTP provider in the IBM Spectrum Copy Data Management Configure section.
- Schedule: A scheduler can be applied. In this case, it must be defined in the IBM Spectrum Copy Data Management Configure section.

The restore job can be run immediately after the job is defined, scheduled, or run on demand. The IBM Spectrum Copy Data Management user has also control over the job to start it on demand, to hold on schedule, or pause and resume during the run time.

> **Important:** Before starting a restore job, shut down the database and unmount the SAP HANA data file system.

2.5 Retention policies and placement of backup copies

This section presents several considerations for backup and recovery SLAs and SAP HANA backup retention policies.

Service levels that the business agrees to set the expectations of how quickly the SAP HANA service can be brought back in case of outage or data corruption. Although the scenarios can differ, it is crucial that proper objectives are set as part of the planning of the solution. The objectives are the guideline of the frequency of protection, data placement, and data retention.

2.5.1 Backup service levels

The backup and recovery service levels begin with the requirements for each data type. Because different options and costs are available, the business requirements for data protection are key to a good and functional data retention policy.

Disaster recovery has a different objective than operational restore capabilities, so various objectives have different elements to consider.

Figure 2-25 shows the RPO in the checkboxes (green). So, you get the best RPO with SAP HSR. Tape backup at the other end of the scale does not work for short data protection windows. The figure also shows the balance between the recovery time objective (RTO) and cost of the solution.

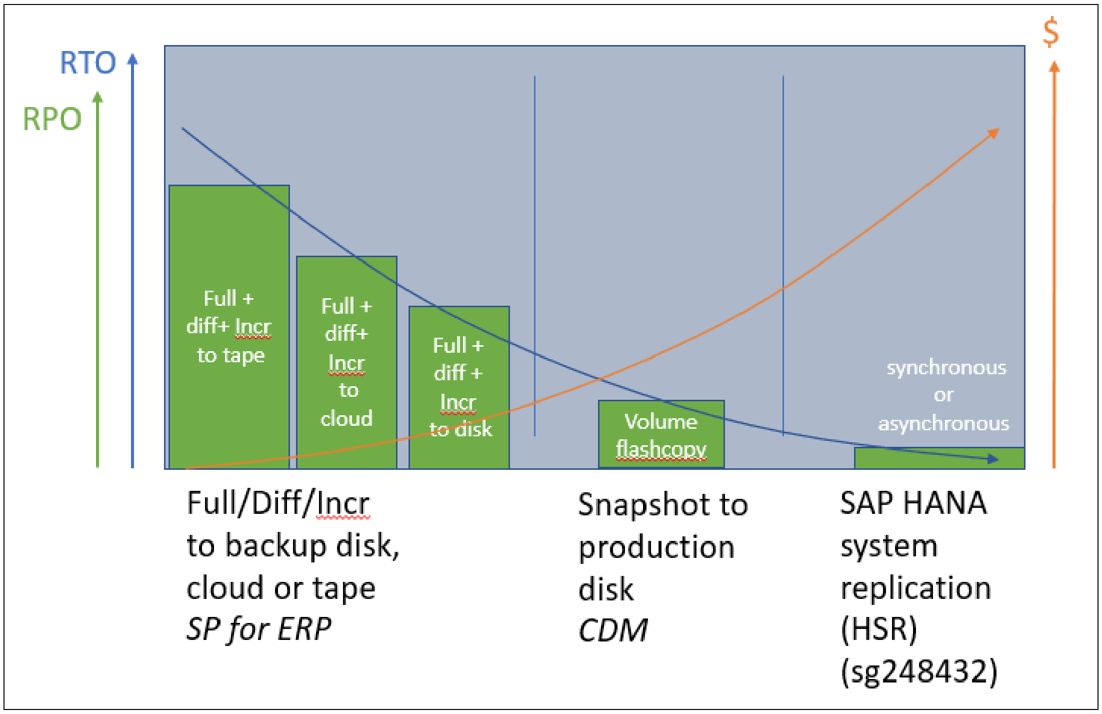

RTO
RPO
$
Full + diff+ Incr to tape
Full + diff+ Incr to cloud
Full + diff + Incr to disk
Volume flashcopy
synchronous or asynchronous
Full/Diff/Incr to backup disk, cloud or tape
SP for ERP
Snapshot to production disk
CDM
SAP HANA system replication (HSR) (sg248432)

Figure 2-25 RPO and RTO with different backup solutions

Consider the capabilities of the following solutions for protecting data:

- RPO: Smaller backup windows
- RTO: Near to instant recoveries
- Version retention objective (VRO): Backup (short term) versus archive (long term)
- Geographic redundancy objective (GRO): Physical placement in more copies

In an SAP HANA solution, there are different types of data to protect that have different objectives for protection. (For more information, see Chapter 3, “Planning and sizing” on page 45.) For example, the Linux OS must be rebuilt from a boot image, but it does not need to be protected each day because only updates change the binary files. Configuration files can be changed by an administrator, and an hourly backup of the files is required if they change.

SAP HANA tenant databases might need to be restored in a near-instant fashion in normal operations, but if a disaster strikes and the snapshots are destroyed, then it might be acceptable to get the most critical database back from offsite storage within 4 - 10 hours.

2.5.2 SAP HANA backup retention policies

SAP HANA backups are stored on various types of back-end storage or backup solutions, such as disk, Backint supported solutions, or snapshots, which are maintained on the storage devices. Over time, the SAP HANA catalog and the backup data can grow unexpectedly. If appropriate retention policies or cleaning operations are not implemented, there is a significant impact on the backup or restore operations when the catalog size increases or there is growth of the storage occupancy on the back-end devices.

There are two types of operations that are must be correlated:

- Cleaning up obsolete SAP HANA backup catalog records: This operation is supported by SAP tools like SAP HANA Cockpit and SAP HANA Studio or by using native SQL statements.
- Cleaning up obsolete backup data: Backup data is grouped on generations of backups that make up a complete (full) backup or data snapshot, subsequent differential or incremental backups, and archive logs until the next successful complete snapshot backup.

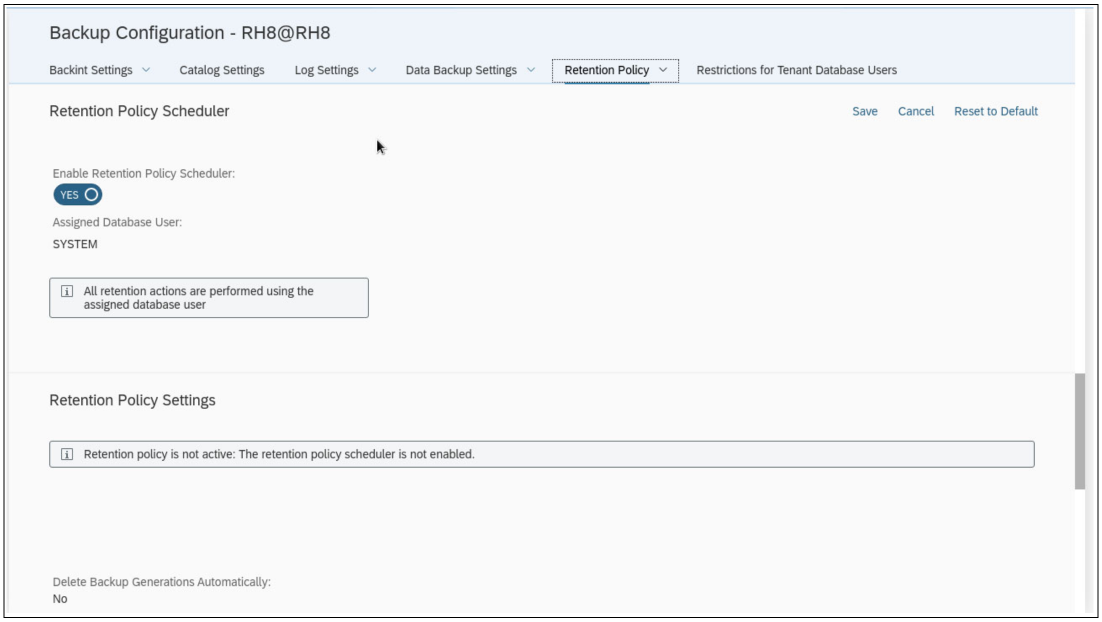
The recovery process involves both types of data, so maintaining the appropriate catalog entries is important for fetching the backup data on restore cases. However, in particular situations restores can be done without the backup catalog, but the administrator must provide manually the input information, such as backup type, location, and prefix. For more information, see Recover a Database from a Data Backup (SAP HANA Studio).

There are controls for maintaining the SAP HANA backup data and expire the obsolete backups on all levels: SAP HANA side configuration, and IBM Spectrum Protect that includes the Data Protection for SAP HANA configuration of retention and snapshot-specific retention policies. These controls are aligned to expire data per required policies and clean up the obsolete data from back-end storage devices and the associated entries in the backup catalog. You should align the expiration policies with the backup policies for a database.

The following sections describe each of retention policy options.

Retention policy in SAP HANA

Maintaining retention policies in SAP HANA provides an advantage by offering the capability to remove both catalog entries and the obsolete backups from disk and Backint. Starting with SAP HANA 2.0 SP 03, the configuration of retention policies can be performed by using the SAP HANA Cockpit interface in the respective database context. Configuration can be done from the **Backup Configuration** menu of the database under **Retention Policy**. You must enable the retention policy scheduler first, as shown in Figure 2-26, and save your change before configuring the retention options.



Backup Configuration - RH8@RH8

Retention Policy Scheduler

Enable Retention Policy Scheduler: YES

Assigned Database User: SYSTEM

All retention actions are performed using the assigned database user

Retention Policy Settings

Retention policy is not active: The retention policy scheduler is not enabled.

Delete Backup Generations Automatically: No

Figure 2-26 Enabling the policy retention scheduler

Edit the **Retention Policy Settings** menu and enable **Delete Backup Generations Automatically**. The following options are available for setting up the retention of the backups:

- Retention time: Specify the period for keeping the backup generations.
- Minimum number of backup generations to be kept.

> **Note:** The deletion occurs only when both conditions are met. The settings are always correlated with the backup policy.

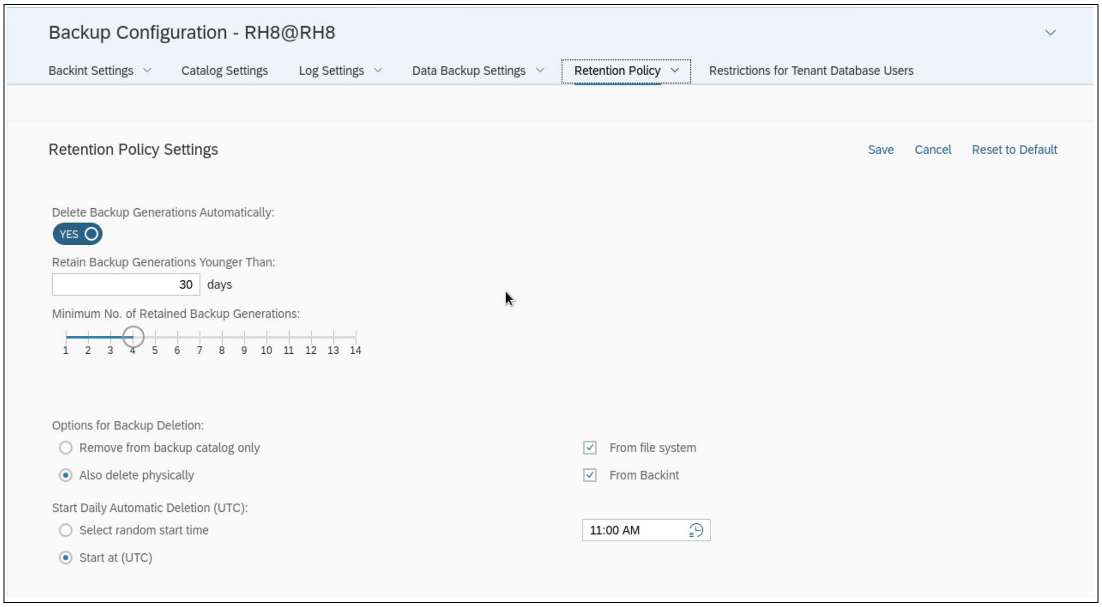
For example, if a database backup series is started as a daily full backup with subsequent log backups between the full backups, the retention time is set to 7 days and the minimum number of generations to 7. On the eighth day from starting the backup series, the older generation is automatically deleted. If a manual backup is taken within the 7 days interval (for the eighth version), no backup is deleted until 7 days elapses. If a backup is not taken for several days, after 7 days no data is deleted until the minimum number of versions (7) is exceeded.

More options are available in the retention policy settings:

- Backup deletion:
  - Remove only the backup catalog entries.
  - Remove the catalog entries and physical data from file and Backint.
- Time to run the daily deletion job: This value can be selected randomly by SAP HANA or specified for a fixed time. Eligibility for deletion for a backup generation is evaluated during the job run.

Note: Backups from snapshots are registered in the SAP HANA backup catalog. When using IBM Spectrum Copy Data Management, the data is deleted from the catalog but not from the storage device when using the SAP HANA Cockpit configuration for automatic backup deletion. The management of the snapshots and expiration of data is performed by IBM Spectrum Copy Data Management. As a best practice, align the retention policy that is set on SAP HANA Cockpit with the IBM Spectrum Copy Data Management backup and retention policies for the snapshots so that SAP HANA does not delete backups that are still available in IBM Spectrum Copy Data Management.

An example of setting up a retention policy for a weekly generated set (weekly full, daily incremental, and log backup) with 30 days retention of backups and four generations kept is shown in Figure 2-27. The backup generations are also automatically deleted from disk and Backint storage, and the retention policy job is scheduled daily at 11:00 UTC time.



Retention Policy Settings

Delete Backup Generations Automatically: YES

Retain Backup Generations Younger Than: 30 days

Minimum No. of Retained Backup Generations: 4

Options for Backup Deletion:

○ Remove from backup catalog only

● Also delete physically

☑ From file system

☑ From Backint

Start Daily Automatic Deletion (UTC):

○ Select random start time

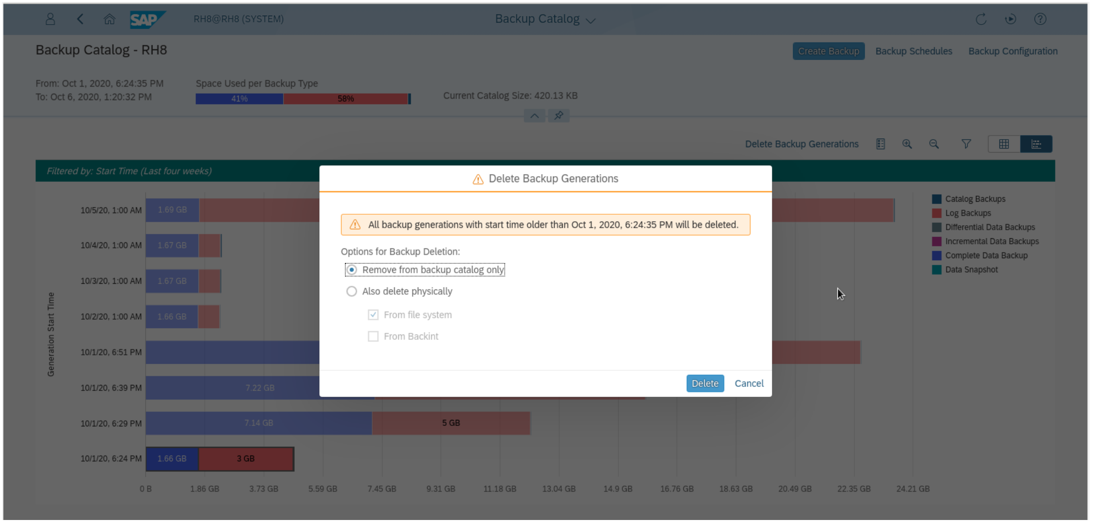
● Start at (UTC) 11:00 AM

Figure 2-27 Configuring retention settings with SAP HANA Cockpit

Manual cleanup of backups in SAP HANA

When backup data is expired by the underlaying layer, such as IBM Spectrum Protect for the Backint data or IBM Spectrum Copy Data Management for the snapshots, the backup catalog entries must be periodically cleaned up. SAP HANA provides the capability to manually delete the backup data by using a GUI (SAP HANA Cockpit or SAP HANA Studio) or a CLI. Regardless of the interface type, the deletion process provides an option to delete data older than a reference backup and extra options to delete physical data (Backint and disk). You cannot delete the snapshot physical data, but the catalog entries for all type of backups including snapshots satisfying the “older than” criteria are removed.

Using SAP HANA Cockpit, you can visualize the backup generations and select the reference backup for deletion process. The administrator must click the **Database Backups** item on the dashboard, which opens the backup catalog context where all backups are listed. By selecting the chart icon, the databases generations are displayed in a bar chart view and a reference line item can be selected for deletion by clicking **Delete Backup Generations**, as shown in Figure 2-28.



Backup Catalog - RH8

From: Oct 1, 2020, 6:24:35 PM
To: Oct 6, 2020, 1:20:32 PM

Current Catalog Size: 420.13 KB

Filtered by: Start Time (Last four weeks)

Delete Backup Generations

All backup generations with start time older than Oct 1, 2020, 6:24:35 PM will be deleted.

Options for Backup Deletion:

- ● Remove from backup catalog only
- ○ Also delete physically
  - ☑ From file system
  - □ From Backint

Figure 2-28 Deleting backup generations in SAP HANA Cockpit

For more information about deleting older backups, see Housekeeping: Deleting and Archiving Backups.

Retention policy in IBM Spectrum Protect

When using SAP HANA backup with Backint and IBM Spectrum Protect, the retention of the backup data can also be set in the Data Protection for SAP HANA configuration. Starting with Data Protection for SAP HANA V8.1.4, it is possible to automatically remove the older backups from the IBM Spectrum Protect server by using the `MAX_VERSIONS` parameter within the `initSID.utl` file. The versions are the backup generations that are maintained on the IBM Spectrum Protect server. Retaining backups provides a trace of all redo log files and differential or incremental backups that are associated with a full backup. All objects are removed together with the full backup.

> **Important:** If a backup is created during the time when the data protection profile parameter `MAX_VERSIONS` is set to zero, this particular backup is excluded from the backup versions processing. It is not considered when counting the number of backup generations, and it is not deleted when it becomes older than the backups that are retained.

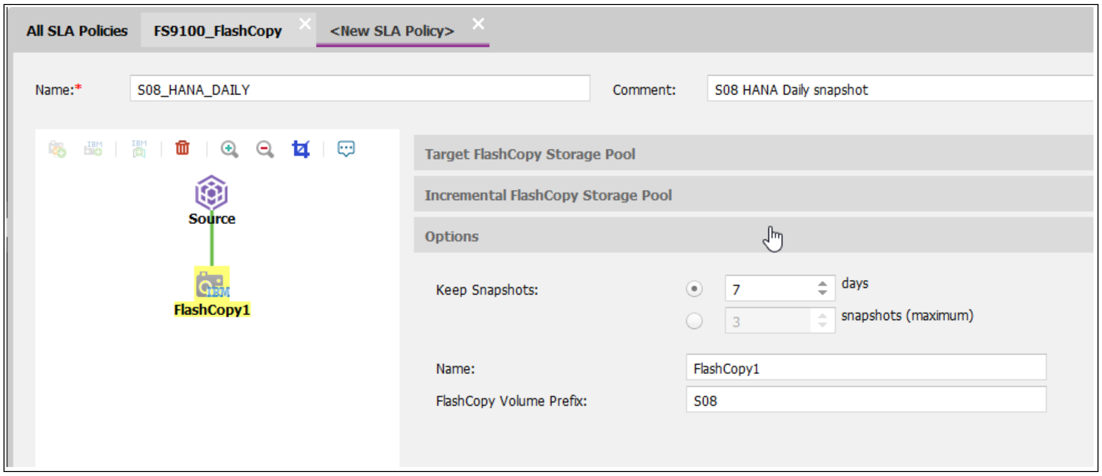
To configure the retention policy, use the Data Protection for SAP HANA features:

- When the retention policy is enabled in SAP HANA and Backint data is automatically deleted with the catalog entries, `MAX_VERSIONS` can be set to 0, which provides full control on the data deletion process to SAP HANA in a top-down approach.
- When expiration of backups is performed by Data Protection for SAP HANA, the parameter `MAX_VERSIONS` determines how many generations of Backint complete (full) backups are maintained on the IBM Spectrum Protect server. An older backup generation than `MAX_VERSIONS` is deleted on IBM Spectrum Protect server upon successful generation of a new full backup. The backup catalog is managed by an SAP HANA instance for cleaning up the obsolete entries in the backup catalog. The operation can be accomplished by using the SAP HANA retention settings for catalog only operations (`delete backint data` must not be set). In this case, the retention period for the catalog records covers the retention that is determined by `MAX_VERSIONS` and the frequency of backups that is used. As a best practice, use a larger period for the retention of the catalog entries to ensure that the generations that are kept on a Backint device are covered in the SAP HANA backup catalog. The catalog entries can also be managed manually, as described in “Manual cleanup of backups in SAP HANA” on page 33.

Data Protection for SAP HANA stores both backup data and archived logs on the IBM Spectrum Protect server in the archive copygroup. The retention for the data is based on the `RETVER` value for the copygroup settings. When an expire process runs, it removes any data that exceeds the `RETVER` value, but there is no correlation between the backup data of the same generation, so this parameter is not considered for the retention policy configuration. As a best practice, set this parameter to not expire the data.

Retention policy for snapshots

The snapshot backups are triggered outside of SAP HANA. Although the snapshots are listed in the SAP HANA backup catalog, they cannot be physically deleted by SAP HANA. When using IBM Spectrum Copy Data Management, the SLAs that are defined in IBM Spectrum Copy Data Management have their own retention settings, as shown in Figure 2-29.



Name:* S08_HANA_DAILY

Comment: S08 HANA Daily snapshot

Keep Snapshots: ● 7 days
○ 3 snapshots (maximum)

Name: FlashCopy1

FlashCopy Volume Prefix: S08

Figure 2-29 Retention parameters for an IBM Spectrum Copy Data Management SLA policy

There are two ways to configure the retention of SAP HANA snapshots in IBM Spectrum Copy Data Management:

- By specifying a retention period (number of days) for keeping storage snapshots.
- By specifying the maximum number of snapshots to be kept.

Snapshots are also included in the backup generations of SAP HANA in a similar manner with full backups. The retention settings in IBM Spectrum Copy Data Management do not impact the HANA backup catalog. The obsolete entries must be deleted due to housekeeping activities or the HANA retention policies. The preferred method is to align the settings in IBM Spectrum Copy Data Management with the settings in SAP HANA so that SAP HANA does not delete backups on the catalog that are still available in IBM Spectrum Copy Data Management.

A typical use case for SAP HANA backup is using IBM Spectrum Copy Data Management for snapshot backup and log backup by using Backint and IBM Spectrum Protect. In this case, the SAP HANA retention policy can be activated to automatically delete obsolete backups from the catalog, including the logs on IBM Spectrum Protect, while snapshots are physically removed by IBM Spectrum Copy Data Management SLA policy. Retention settings must be correlated with the backup plan and they can be aligned by retention period or number of snapshots. For example, in the case of an IBM Spectrum Copy Data Management snapshot backup job running daily with automatic log backup in IBM Spectrum Protect and a retention of 7 days, the retention time of 7 days is set on both the IBM Spectrum Copy Data Management SLA policy and SAP HANA duration of backup generations.

2.6 Cyber resiliency aspects of an SAP HANA solution

Data protection plays a key part of a cyber resilient SAP HANA solution. The goal of cyber resilience is to maintain the confidentiality, integrity, and availability of data and business operations.

Cybersecurity refers to the processes and practices that you use to protect your data and systems. Cybersecurity includes the tactics of implementing technology and best practices to secure your critical data and the underlying infrastructure to prevent hackers from gaining access. Cybersecurity is a continuous effort to adapt the organization and make the infrastructure more resilient against cyberattacks.

This section describes the technologies and practices that are available to the organization to withstand, respond to, and recover from a cyberattack. The mindset has changed from reactive to proactive, that is, how to respond when disaster strikes.

The key elements of cyber resiliency are described in the cybersecurity framework National Institute of Standards and Technology (NIST), as shown in Figure 2-30 on page 37. IBM technology has a comprehensive set of capabilities that supports the NIST framework.

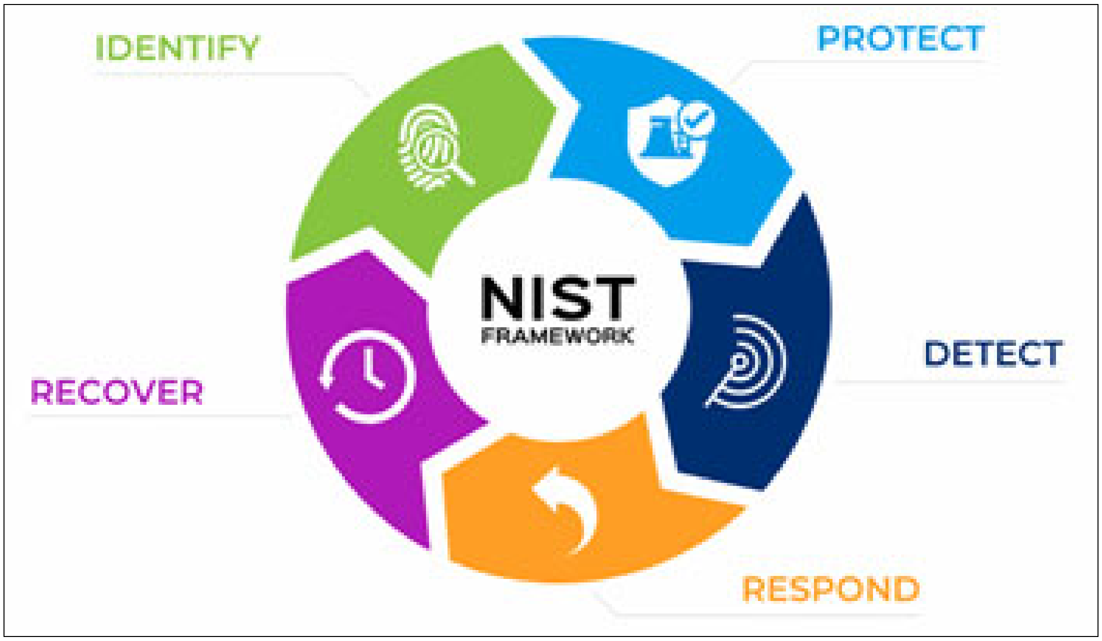
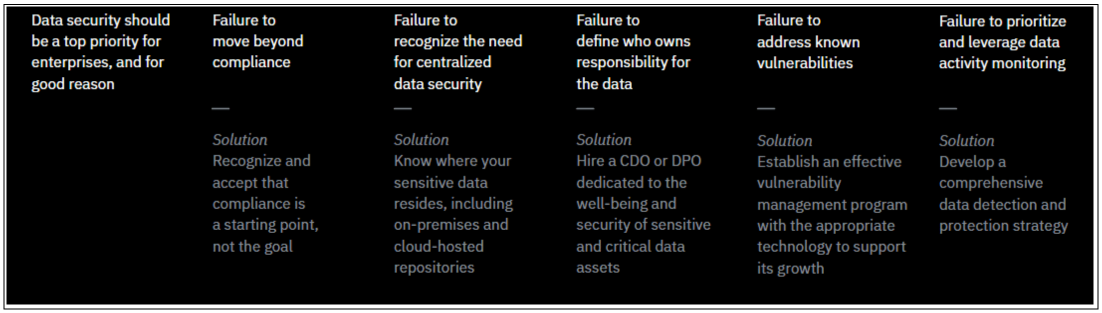


Figure 2-30 National Institute of Standards and Technology framework

For more information, see NIST Cybersecurity Framework.

A data security strategy is about processes and procedures around the services that are delivered. IBM Security™ has many services and products that are available to help improve the security level within your organization. This improvement is an on-going process to make sure that you do not fall into the pitfalls that are described in Figure 2-31.



Data security should be a top priority for enterprises, and for good reason	Failure to move beyond compliance	Failure to recognize the need for centralized data security	Failure to define who owns responsibility for the data	Failure to address known vulnerabilities	Failure to prioritize and leverage data activity monitoring
	—	—	—	—	—
	Solution Recognize and accept that compliance is a starting point, not the goal	*Solution* Know where your sensitive data resides, including on-premises and cloud-hosted repositories	*Solution* Hire a CDO or DPO dedicated to the well-being and security of sensitive and critical data assets	*Solution* Establish an effective vulnerability management program with the appropriate technology to support its growth	*Solution* Develop a comprehensive data detection and protection strategy

Figure 2-31 Data security strategy[1]

In an SAP HANA infrastructure, cybersecurity must be reviewed at all levels. The capabilities in the NIST framework are listed in Appendix A, “Scheduling an SAP HANA backup by using IBM Spectrum Protect” on page 113, and they provide an overview of what is available and must be considered when configuring the SAP HANA solution.

[1] Five Common Data Security Pitfalls to Avoid: https://www.ibm.com/downloads/cas/LKV1EVYD

Security platform

IBM Security Guardium® is a comprehensive platform for the security of different data sources like SAP HANA databases.

IBM Guardium Data Protection for SAP HANA is an end-to-end solution that increases the cyber resiliency of the SAP HANA system. It assesses vulnerabilities by scanning the entire SAP HANA system for Common Vulnerabilities and Exposures (CVEs), and it suggest industry best practices and SAP recommended security practices.

IBM Guardium Data Protection for SAP HANA also enables you to understand where sensitive data is based on compliance and privacy regulations, such as CCPA, SOX, PCI, GDPR, and personally identifiable information (PII).

The results of the tests make it possible to quickly remediate risks and take advantage of per-built integrations with CyberArk, Splunk, IBM Security QRadar®, ServiceNow, and other IT/SecOps tools for incident orchestration and response.

For more information, see the YouTube video IBM Security Guardium Data Protection for SAP HANA.

Data access isolation

With data access isolation, the environment is more resilient at the physical layer. Here are the data access isolation options:

- Air gap
- Non-erasable and non-rewritable (immutable/Write Once Read Many (WORM))
- Cold storage and object storage
- Data vaults
- Isolated infrastructure
- Separation of duties and separate administration zones

The section “Air-gap example” shows an air-gapped solution with SAP HANA and IBM Spectrum Protect. The method can be expanded as needed to more sites.

Air-gap example

Figure 2-32 on page 39 shows that one of the sites is a production site, and the other site is an air-gapped site where only authorized personnel and processes have access. The IBM Spectrum Protect server acts as intermediary between two physical dispersed SAP HANA environments. It is possible to store the backup data on air-gapped tapes. These tapes can physically be transported to a secure place.

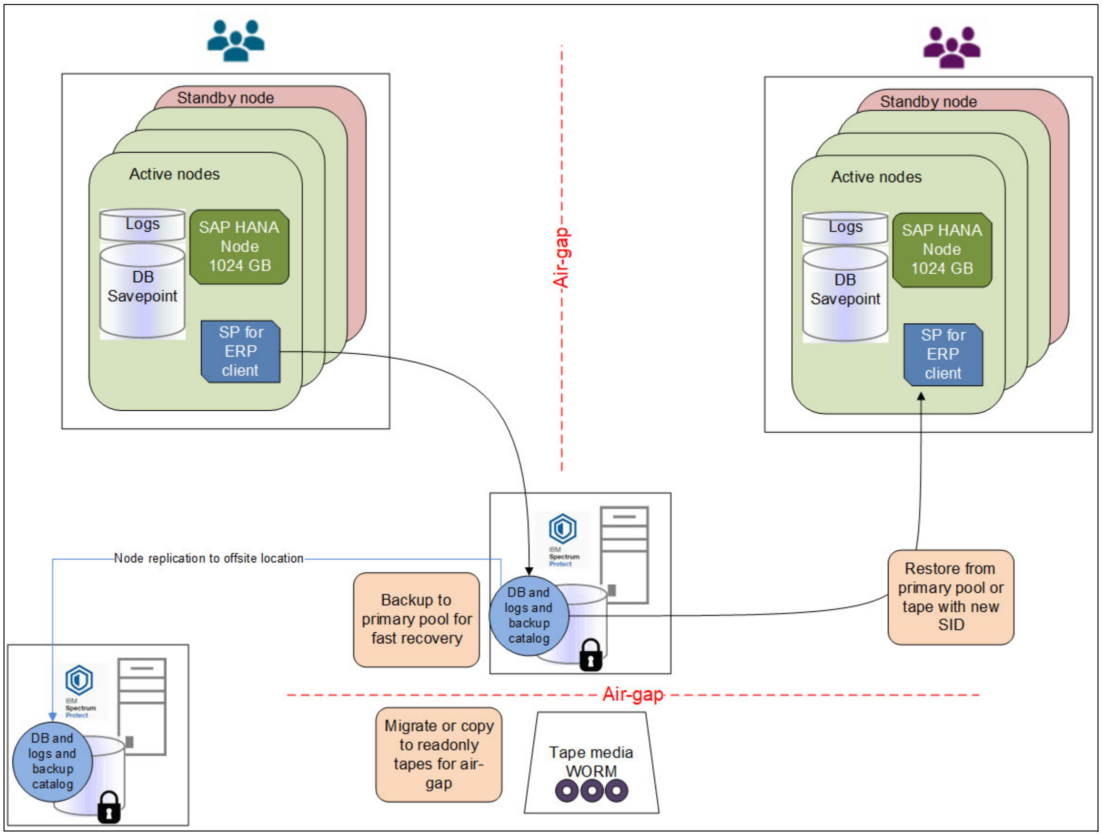

Standby node
Active nodes
Logs
DB Savepoint
SAP HANA Node 1024 GB
SP for ERP client
Standby node
Active nodes
Logs
DB Savepoint
SAP HANA Node 1024 GB
SP for ERP client
Air-gap
Node replication to offsite location
Backup to primary pool for fast recovery
IBM Spectrum Protect
DB and logs and backup catalog
Restore from primary pool or tape with new SID
IBM Spectrum Protect
DB and logs and backup catalog
Air-gap
Migrate or copy to readonly tapes for air-gap
Tape media WORM

Figure 2-32 Air-gap example

The IBM Spectrum Protect baclient and client for ERP is used to synchronize the two sites by restoring the essential components to make the SAP HANA databases available on the secondary air-gapped site.

Then, the alternative restore operation method is used to restore the database data to the secondary site.

For more information, see Running an alternative restore operation for an SAP HANA database.

Data placement considerations and role-based access

The 3-2-1 backup rule is a proven approach to ensuring data recovery. The rule is: Keep at least three copies of your data, and store two backup copies on different storage media, with one of them offsite.

IBM Spectrum Protect supports replication at the node level (logical) or storage level (physical) to protect against errors and corruptions. The target can be an IBM Spectrum Protect server in the cloud or with tape access. Tape management is built in if physical storage offsite is required.

With IBM Spectrum Copy Data Management, you can copy data snapshots from various storage providers to multiple locations.

The roles and responsibilities must be divided so that administrators of SAP HANA do not have access to delete the backup data or have root access to the OS of the Power Systems machines.

The backup and restore team sometimes has access to the backup clients, which then gives them too many privileges and potentially can remove both the backup data and the production data. Be cautious when these access rights overlap.

2.6.1 Encryption for data at rest and data in flight

Encryption capabilities can be enabled at different levels in the infrastructure. As a best practice, enable data encryption at one point only. The closer to the application the better, but encrypted data in-flight does not deduplicate well at the backup storage repository level.

For backup copies and snapshots, encryption is available at the IBM Spectrum Protect server or by using external key management services like IBM Security Key Lifecycle Manager.

IBM Guardium Data Encryption for Files and Databases

IBM Guardium Data Encryption (GDE) for Files and Databases offers SAP HANA system encryption for data at rest on the file system level of a savepoint. When a backup is taken, IBM Spectrum Protect data is decrypted and sent to the IBM Spectrum Protect server. In this way, both savepoints and backup data can be encrypted.

IBM Spectrum Protect encryption techniques

IBM Spectrum Protect server can encrypt data in flight from API clients, for example, for SAP HANA to the server or at rest when the data is in directory container pools or on tape.

SAP HANA database encryption is also an option. Then, client encryption rules also apply, as shown in Table 2-1.

Table 2-1 Server and client encryption rules

Server encryption	Client encryption
Server controls encryption at the storage pool level.	Client controls encryption at the objects level by using **`include.encryption`** and **`encryptiontype`** options.
Server encrypts at the chunk level.	Client encrypts at the file level.
Server manages all its encryption keys	Client optionally stores keys in the `TSM.PWD` file.
Server uses AES encryption with a minimum key length of 256-bit.	Client uses AES256, AES128, or DES56 bit.
Server signs encrypted data to detect tampering or corruption.	Client does not sign encrypted data.
Data encrypted by the server can be deduplicated.	Data that is encrypted by the client cannot be deduplicated.

With IBM Spectrum Protect V8.1.2, there was a change to how encrypted chunks are sent across to a replication target server.

To enable encryption, the server uses a master encryption key, which is created when the server password is set, and it is stored as part of the server password file `dsmserv.pwd`.

The target encrypts the chunk key with its master key and stores it with the chunk. There is only one master key per IBM Spectrum Protect instance.

Table 2-2 on page 41 shows what happens with the data on the replication target.

Table 2-2 Data encryption replication target

Target source	Version 8.1.2 (Encrypt=yes)	Version 8.1.2 (Encrypt=no)	Legacy server
Version 8.1.2	1. Encrypted chunk is sent *as is* to the target server. 2. Non-encrypted chunk is encrypted on target server.	1. Encrypted chunk is sent *as is* to the target server. 2. Non-encrypted chunk is sent *as is* to the target server.	1. Server encrypted chunk is decrypted on the source server before being sent over. 2. Non-encrypted chunk is sent *as is* to the target server.
Legacy server	Chunk is encrypted on the target server.	Chunk is sent *as is* to the target server.	Chunk is sent *as is* to the target server.

Dbbackup protects the master encryption key. The master key protects directory and cloud encryption keys and is needed to restore an encrypted pool.

As a best practice, enable *PROTECTKEYS=YES* with the **SET DBRECOVERY** command.

Note: If you lose the master key, you lose all of the data that is stored in encrypted container storage pools. If you lose the master key, you lose all the admin and client passwords.

When using cloud options, data is always encrypted both in flight and at rest. This setting cannot be disabled.

For more information, see the following YouTube video IBM Spectrum Protect encryption options as of Version 8.1.1.

IBM Spectrum Copy Data Manager snapshot encryption

IBM Spectrum Copy Data Management relies on the underlying storage to encrypt the data volumes holding snapshots. For IBM storage, disk, and tape, there are different options to use, for example, Key Management Interoperability Protocol (KMIP) to an external key manager to encrypt data at rest. Having an external key manager like IBM Security Key Lifecycle Manager makes it easier for an organizational perspective to keep these encryption keys safe and protected.

Transparent Cloud Tiering uses IBM FlashCopy techniques that provide full and incremental snapshots of several volumes. Snapshots are encrypted and compressed before being uploaded to the cloud.

2.6.2 Immutable backup storage

Immutable storage is also known as WORM, where data cannot be erased after it is written to the media. Immutability is a feature of the storage that is used.

IBM Spectrum Protect can write data to offline WORM tape devices, immutable Spectrum Scale file systems, and cloud storage. Backups are stored and cannot be erased after they are written.

SAP HANA data snapshots can be encrypted by SAP HANA if the volume is encrypted and backup encryption is enabled.

IBM Spectrum Copy Data Management can make full and incremental snapshots and replicate these snapshots offsite to immutable cloud storage.

2.6.3 System hardening

System security hardening tools help to increase the system security in an easier way than doing the configuration changes manually.

SUSE Linux Enterprise Server, Red Hat Enterprise Linux, and IBM PowerSC solutions all have predefined SAP Profiles that can be used to automate these settings.[2]

IBM PowerSC is designed for enterprise security and compliance in cloud virtualized environments running IBM Power Systems servers.

IBM Spectrum Protect access security model

Each IBM Spectrum Protect client node has its own password that is encrypted. Only that node can access its own data. No other node can do so unless explicitly permitted to do so (by running the **SET ACCESS** command or Grant Proxy node).

In a scale-out environment, configure Data Protection for SAP HANA in a way that each SAP HANA node uses a dedicated IBM Spectrum Protect node for authentication and stores the data on behalf of a single proxy node. This way ensures that each SAP HANA node has access to all backups of all other SAP HANA nodes.

Each IBM Spectrum Protect administrator authenticates with their own encrypted password. An administrator has no authority other than read-only (formerly called *analyst authority*) unless explicitly granted. Rough role-based authority levels exist for administrators, and administrators can have their scope limited to specific domains, storage pools, nodes, and others.

Complex password rules for nodes and administrators can be enforced by an external LDAP or AD.

There is an increased level of security in IBM Spectrum Protect TLS 1.2 to secure point-to-point communication (SHA signature (`cert256.arm`)).

IBM Spectrum Copy Data Management snapshot security

With role-based access control, you can tailor the resources and permissions that are available to accounts, including the actual objects that are defined in the system. The defined roles can be associated to LDAP groups for easy user management.

User access can be granted to storage devices or application servers depending on their role.

SAP HANA authentication is done through a registered password or SSH private key. Specific privileges are granted on the SAP HANA system to limit the access to specific tasks, for example, discover, mount, and unmount of disks.

2.6.4 Backup data verification

To check the consistency of a backup, use the tool **hdbbackupcheck** with file-based and third-party backup tools. The tool cannot be used to check the consistency of data snapshots. For more information, see Example 5-7 on page 88.

[2] https://www.suse.com/media/guide/os_security_hardening_guide_for_sap_hana.pd

IBM Spectrum Copy Data Management based snapshots can be verified by manually mounting the database to a different host or as a scheduled task. For more information, see Running an alternative restore operation for an SAP HANA database.

2.6.5 More considerations

For more information about the available support and alerting tools and how to apply flashes from the IBM support website, see IBM Support.

At the website, you can select different platforms to protect against OS-targeted ransomware attacks, and learn to follow strong testing and currency policies.

2.7 Other tools to use for backup and recovery of SAP HANA

This section focuses on protecting SAP HANA databases. However, other components such as the OS and the configuration files cannot be forgotten.

Based on the SAP layout suggestion for the file systems shown in Figure 2-33, all other file systems not under `/data` and `/log` also must be backed up by using traditional backup methods.

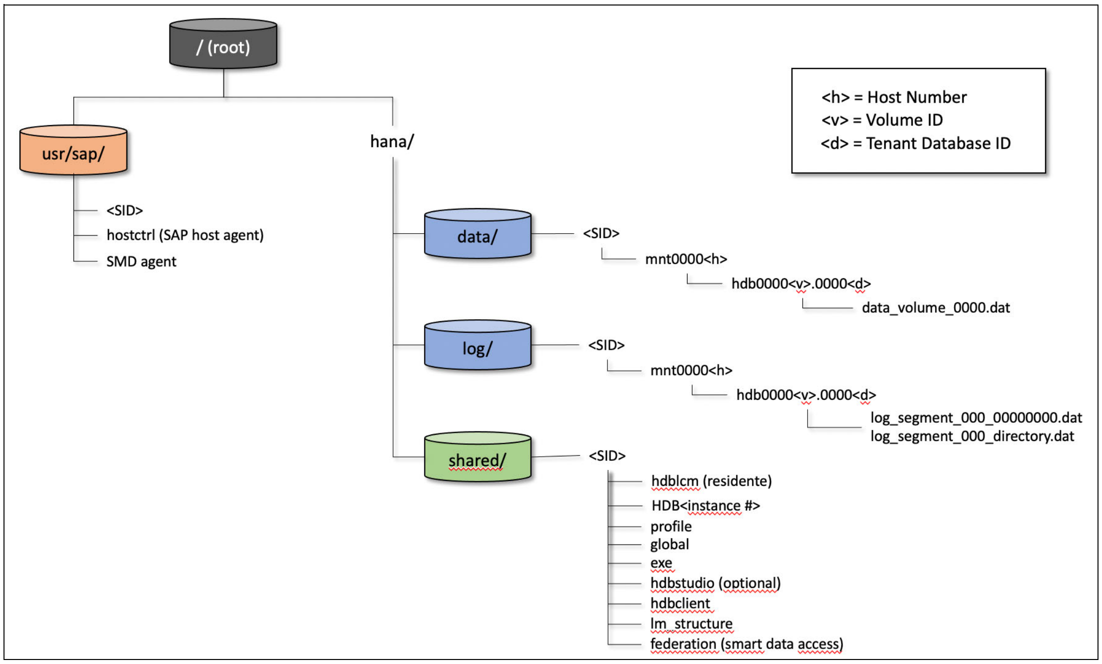


Figure 2-33 Default file system layout

During the planning phase and architectural design, consider the backup of the OS and all application file systems that are not part of the database. Also, if the environment contains application servers (physical or virtual), they also must be backed up.

Consider the following backup tools:

- IBM Spectrum Protect Backup and Archive client
- Christie's TBMR, Relax And Recover (ReAR), or Storix
- IBM Spectrum Protect Plus (for application servers in VMs)
- The **`mmbackup`** command

Note: When using the IBM Spectrum Protect Backup-Archive client, check that the /data and /log file systems are excluded from the file-level backup.

2.7.1 Scale-out environment

Consider that the file system /hana/shared, depending on the SAP HANA implementation, for example, in a scale-out solution, is mounted on every node of the SAP HANA environment, but in fact is only one. There is no need to back up this file system from all nodes.

If IBM Spectrum Scale is used, consider creating the schedules with IBM Spectrum Protect Backup-Archive client by running **mmbackup**. In this case, create one node in IBM Spectrum Protect as a proxy node, with each of the SAP HANA nodes as proxy agents.

In this example, we use the following command on the IBM Spectrum Protect server to register the cluster nodes as clients (repeat for each node):

```
register node <hana_node> <password> domain=<domain>
```

Then, we register the proxy node that acts on behalf of the cluster nodes:

```
register node <hana_proxy_node> <password> domain=<domain>
```

Lastly, we associate the cluster nodes with the proxy node:

```
grant proxy target=<hana_proxy_node> ag=hana_node1, hana_node2,...
```

Here an example of the script to run, which is associated to only one of the nodes:

```
/usr/lpp/mmfs/bin/mmbackup /shared/<SID> -t incremental -N <node1>, <node2>
--backup-threads 4 -v -L 1 --tsm-servers <proxy_node> | tee -a <log_file>
```

For more information about the **mmbackup** command, see the mmbackup command.

3

Planning and sizing

There are three options for SAP High-performance Analytic Appliance (HANA) backup: file system, Backint, and snapshot. You can mix the backup methods. Depending on the method, the backup can be full, incremental, or differential.

This chapter describes considerations for planning data protection for an SAP HANA environment running on an IBM Power Systems server.

The metrics for sizing the data protection of an SAP HANA landscape are described.

The elements include sizing IBM Spectrum Protect for Enterprise Resource Planning (ERP) by using SAP Backint, IBM Spectrum Copy Data Management for SAP data snapshots, and the IBM Spectrum Protect server to use as a repository.

Using IBM Spectrum Protect Blueprint guidelines to size the IBM Spectrum Protect server and the required throughput to support the daily backup workload are described.

This chapter contains the following topics:

3.1 Planning

SAP HANA backups consist of individual strategies for the SAP HANA database, log, and configuration files.

Other components such as application servers, multitenant databases, system database, catalog, and operating systems (OSs), including configurations, are also as important as the data in the databases. Looking at the complete SAP HANA system landscape from a data protection perspective provides a focus for keeping the service running for users to access.

For a complete backup strategy, consider the following topics:

- Backup of the SAP HANA database and optional data tiering store itself
- Backup multitenant databases
- Automatic backup of the database logs
- Backup of the system database
- Backup of the Linux OS, usually a bootable OS image
- Backup of the file systems `/usr/sap/<SID>`, `/hana/shared/<SID>`, and the configuration files
- Backup of specific corresponding file systems

3.1.1 Selecting the backup method for the SAP HANA databases

All available backup method options can be used exclusively or in combination. There are pros and cons for each method, but combining them can elevate the options for recovery scenarios and meet the recovery objectives.

Table 3-1 on page 47 shows an overview of the comparative features of complete data snapshot, data backup to file, and data backup by using Backint.

Table 3-1 Comparison of data snapshots and data backups[1]

Category	Data snapshot	Data backup to file	Data backup by using Backint
Advantages	► Short recovery time. ► Fast data copy. ► Negligible impact on network. ► Can be encrypted (if data volume encryption is active).	► Integrity checks at block level. ► Can be encrypted.	► Integrity checks at block level. ► Integrated into existing data center infrastructure. ► Using IBM Spectrum Protect offers more features such as inline deduplication and compression by using directory or cloud container pools. ► Encryption for data at rest (container pools or tape-based encryption) or in-flight (client-side encryption). ► Backups are immediately available for recovery.
Disadvantages	No integrity checks at block level.	► Requires more storage. ► Generates more network load during offload to a different location. ► File system must be monitored (usage level). ► More time is needed to make backups available for recovery (recovery time objective (RTO)) from an offloaded copy.	► Generates more network load.
Backup size	Size of the data area (but it can be compressed or deduplicated based on the storage features).	► Payload only.	► Payload only.

[1] https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.03/en-US/4fe5eacc1890434c8ba4b0aaeacc56eb.html

Category	Data snapshot	Data backup to file	Data backup by using Backint
Backup duration (recovery point objective (RPO))	Negligible (depending on the storage tool implemented).	► I/O-bound (reading from data volume, writing to target). ► Network-bound (writing to target file system).	► I/O-bound (reading from data volume). ► Network-bound (writing to backup server). ► Depends on chosen method: full, differential, or incremental.
Backup copies	Replicate data by using Global Mirror with Changed Volumes to the secondary site.	► Back up a file copy by using the IBM Spectrum Protect backup client.	► Most flexible solution with backup directly to cloud (AWS). ► By using IBM Spectrum Protect to other cloud storage (IBM Cloud, Azure, or AWS). ► IBM Spectrum Protect node replication to other locations. ► IBM Spectrum Protect migrate and copy to tape.

The planning and sizing focuses on data snapshots and backup by using Backint.

Consider using a combination of data backups, automatic log backups, and data snapshots to minimize the risk of data loss and to ensure quick restore.

3.1.2 Online SAP HANA database backup by using Backint

There are two types of databases to protect: the system database and tenant databases.

Note: The SYSTEMDB backup is always a full backup copy.

For tenant databases, there are full, differential, and incremental backup options. First, choose the method from the RTO and RPO requirements, and then choose by the network load and storage utilization in the backup repository.

Log backups store the content of closed log segments. SAP HANA closes log segments when they are full, for example, reach a certain size, or when a time threshold is reached. The default time threshold is 900 seconds. The log backups are automatically created by reading the content from the log segment files asynchronously and writing it to the backup location. Specify an appropriate timeout for log backups that enables you to recover an SAP HANA database with the RPO defined.

For most production SAP HANA installations, the log files are backed up twice and to different locations. This feature is available with IBM Spectrum Protect for ERP from Version 8.1.1 onward.

SAP HANA Backint backups can also go directly to the AWS cloud service, which is SAP HANA certified as a backup target by using a cloud gateway. Cache, upload buffer settings, and best practices are defined in the AWS documentation. Plan to install the cloud gateway on SSD or flash storage to improve the data movement to and from the cloud.

To speed the transfer to and from the cloud, the IBM Aspera® FASP® solution can increase the throughput by a factor of 8 - 9 by removing the latency and WAN bottleneck per data stream.[2] Aspera supports several cloud vendors, and SAP opened up for partners to create a certified S3 Backint adapter.

3.1.3 Online SAP HANA database snapshot

Database snapshots are recovery points that are saved in the storage layer as storage snapshots.

IBM Spectrum Copy Data Management creates copies of data by using the hardware snapshot function of modern storage subsystems. Snapshots must not be considered as a backup alone because they are stored within the same storage system. The 3-2-1 data protection rule is still met.

IBM Spectrum Virtualize can store the snapshots in different storage systems and on other locations by using replication, and it can make those copies available for various use cases, including backup, recovery, and cloning.

IBM Spectrum Virtualize offers full and incremental copies of the storage volumes. It is not possible to protect a single database from an SAP HANA tenant setup. The snapshot is one that includes all volumes that are used for the tenant databases.

Note: As a best practice, perform a database backup in the following situations:

- After the initial database load.
- At regular intervals (at least daily).
- A combination of online backups and snapshots must be considered.
- Before the database software is upgraded to a new version to be able to fall back to the database state before the upgrade.
- After any situation that causes log writing to be interrupted. For example, immediately after the log mode was changed.

The log file system is not included in the snapshots, so these files can be protected by using Backint and automatic data protection to the IBM Spectrum Protect server.

3.1.4 Protecting other SAP HANA environment components

This section describes how to protect other SAP HANA components.

Backup catalog

The backup catalog contains information about the backup history.

The backup catalog is backed up after each backup operation, for example, after each full backup and each redo log backup.

[2] https://www.ibm.com/cloud/smartpapers/aspera/transfer-large-files/
https://www.ibm.com/aspera/file-transfer-calculator/

Note: With SAP HANA Multitenant Database Containers (MDCs), the system database and each tenant database have their own backup catalog.[a]

[a] https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.00/en-US/c3d31debbb5710148100a43bfe990b4a.html

Linux operating system

A daily file_level backup protects the most recent changes of, for example, configuration files. A file-level backup to an IBM Spectrum Protect server with the IBM Spectrum Protect baclient can make a daily incremental backup of all files that are not part of the SAP HANA database files.

Note: As a best practice, perform a bootable backup of the Linux OS in the following situations:

- After the initial installation and successful configuration of the OS.
- After every update of a software component (for example, Linux kernel and security patches).
- After a major OS update (such as after the migration from SUSE Linux Enterprise Server 12 SP1 to SP2).
- At regular intervals (at least monthly).

Different third-party options like Relax And Recover (ReAR), Cristie, or Storix[3] are available and integrated with IBM Spectrum Protect servers to run a bootable backup of the Linux OS.

SAP HANA instance-specific information

The file systems `/usr/sap/<SID>` and `/hana/shared/<SID>` contain SAP HANA instance-specific information, log files, spool files, audit files, archiving files, and the SAP HANA executable files and their required configuration files. As a best practice, back up these file systems regularly.

Note: File system backups are performed after the following situations:

- After the initial installation of the SAP HANA system.
- After every update of SAP HANA components or configurations (SAP HANA kernel and SAP HANA config files).
- At regular intervals, make daily incremental backups.

File system backups can be part of the daily scheduled incremental backup of the OS file systems.

3.1.5 Backup and recovery objectives

This publication is about data protection and not how to solve high availability. Other options like SAP HANA System Replication (SAP HSR) or storage replication handle high availability. From a strategy perspective, you must consider what is possible with file-level backup, Backint, or snapshot.

A sample data protection strategy is shown in Table 3-2 on page 51.

[3] More licensing can be required to use these three bare metal recovery tools.

Table 3-2 Data protection strategy

Database backups	File-level backup
► RPO: 1 hour ► RTO: 1 hour ► Version retention objective (VRO): 32 versions ► Geographic redundancy objective (GRO): 2 copies ► Front-end DB size: 40 TB	► RPO: 25 hours ► RTO: 4 hours ► VRO: 32 versions ► GRO: 2 copies ► Front-end file size: 15 TB

To fulfill the database RTO requirement, for the SAP HANA databases, use both Backint and snapshot. Backint provides RPO, VRO and GRO, and snapshot meets RPO and RTO.

In this example, we create two policies to meet the requirements: One policy for databases and one for files, as shown in Table 3-3.

Table 3-3 Policies for databases and files

Policies for databases	Policies for files
Scheduled weekly full and daily differential backup of databases and continuous log backup by using Backint and IBM Spectrum Protect for ERP.	Scheduled daily incremental backup by using IBM Spectrum Protect baclient.
Hourly snapshot by using IBM Spectrum Copy Data Management.	ReAR boot image to recover Linux file systems.
Keep 32 versions of full and incremental backups in IBM Spectrum Protect. Keep 4 snapshots in IBM Spectrum Copy Data Management (last 4 hours).	Keep 32 versions in IBM Spectrum Protect.
Use IBM Spectrum Protect node replication to a secondary site.	Use IBM Spectrum Protect node replication to a secondary site.

When backing up databases as part of a tenant, SYSTEMDB needs protection separately.

3.1.6 Infrastructure considerations

There are specific infrastructure considerations when planning the data protection model for SAP HANA:

- Physical data placement:
  - Where are the backup copies (Backint and snapshot) to make sure you have three copies of data on at least two different media and one copy offsite?
  - Is it required to have access to data copies on an instantaneous basis?
- Connectivity:
  - Which peak throughput is required for backup and restore from the different locations of backup copies?
  - Does data need to be air-gapped?
- Operations:
  - Is separation of duties required and what does that mean to daily operations?

3.1.7 Backing up to an IBM Spectrum Protect container pool with inline deduplication and compression

Deduplication savings can be increased by setting the correct buffer size that is used by the IBM Spectrum Protect for ERP client for transferring the database backup data. The BUFFSIZE parameter has a default value of 1 MB, but can be up to 32 MB.

Experiments show that larger buffer sizes yield better deduplication savings. An 8 MB buffer size (BUFFSIZE 8388608) seems to strike a good balance between deduplication efficiency and memory consumption. Savings of 70 - 80% (from both deduplication and compression) were observed with an 8 MB buffer size.

However, this change has the side effect of causing more data to be stored during log backups. Log backups still use a small buffer size (for example, 256 KB) for best efficiency. SAP HANA can specify different configuration files for data and log backups. To overcome this issue, use a separate options file for data and log file backups. The only option that needs to vary between these two files is the BUFFSIZE setting.

In SAP HANA 2.0 SPS 05, a new global.ini profile parameter was introduced, parallel_data_backup_Backint_size_threshold, which specifies the threshold for the database size in GB. The default value is 128 GB.

By default, SAP backups do not use multiple sessions, which can limit backup throughput. Multiple sessions can be used for databases that are larger than the parallel_data_backup_Backint_size_threshold. More parallel Backint channels are configured with parallel_data_backup_Backint_channels.

The following recommended starting values provide good performance and storage reduction for repeated full backups, which approaches 80% savings:

- In the SAP HANA administration studio, set the following options:

  ```
  data_backup_parameter_file
  /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
  log_backup_parameter_file
  /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08_log.utl
  ```

  parallel_data_backup_Backint_channels 4 is also configured when running the IBM Spectrum Protect for ERP **setup.sh** script.

  The parameter data_backup_buffer_size must not be changed. It is adjusted automatically.

- In the IBM Spectrum Protect for ERP option file for data backups, include the following options:

  ```
  MAX_SESSIONS 4
  MAX_BACK_SESSONS 4
  MAX_ARCH_SESSIONS 2
  RL_COMPRESSIONS NO
  MULTIPLEXING 1
  BUFFSIZE 8388608
  ```

- In the Tivoli Data Protection for SAP HANA option file for log backup, include the same options except for the following ones:

  ```
  MAX_SESSIONS 4
  MAX_BACK_SESSONS 4
  MAX_ARCH_SESSIONS 2
  RL_COMPRESSIONS NO
  ```

```
MULTIPLEXING 2
BUFFSIZE 262144
```

Data compression is done after deduplication is performed for optimal data reduction. The function requires more CPU and memory from the IBM Spectrum Protect server during backup. There is almost no impact on the restoration of data even though extents must be read from different areas of the disk.

For more information about the detailed configuration, see 4.4.2, “Configuring Data Protection for SAP HANA” on page 67.

There was a fix in SPS 09 to set the sync points for the log recovery to be outside of log volume processing so that multiple services can be recovered in parallel. Although the restriction is lifted in the current release, storing log data to tape can result in performance degradation, so this approach is not a best practice.

3.1.8 Planning for restore

SYSTEMDB has a central administration role. It contains information about all tenant databases, grants and keeps privileges for the tenant databases, and other important information.

A complete system recovery starts with a restore of the SYSTEMDB and only after that completes can the tenant databases be restored.

If a full backup is physically available but not recorded in the backup catalog, that backup can still be used to recover the database, but without using log backups. A recovery to a point-in-time (PiT) is not possible if the full backup is not recorded in the backup catalog.

> **Note:** At the time of writing, it is not possible to copy a tenant database by using Backint because it is not possible to change the system ID (SID) or the name of the tenant database.

In a tenant system, SYSTEMDB is restored before the tenant databases.

Rebuilding the SAP HANA backup catalog

The backup catalog that holds all information about backups is needed to recover SAP HANA databases.

The procedure to restore to an alternative machine can be used to restore the backup catalog.

When using the option **Recover using the backup catalog** (which is selected by default) together with **Search for the backup catalog in Backint only**, the processing first restores the backup catalog from the IBM Spectrum Protect Server and obtains a list of backups from this catalog information. Then, you can select the backup that you want to use for the restore.[4]

> **Note:** `hdbbackupdiag` can be used only to rebuild a backup catalog from a file backup. All backups that use Backint or storage snapshot backups will not be re-created.

[4] https://www.ibm.com/support/pages/selecting-sap-hana-backup-will-be-used-alternate-restore

3.2 Sizing for backup and restore with Backint

The IBM Spectrum Protect blueprints[5] provide documentation and automated scripts to configure small, medium, and large IBM Spectrum Protect server architectures.

The solution design is based on using the IBM Spectrum Protect disk-based directory container pool where deduplication and compression are enabled. This design also includes the required network throughput to meet the backup and restore window.

This section goes through a sample sizing specifically for the solution landscape, which is described in 3.2.2, "SAP HANA landscape solution" on page 54.

3.2.1 IBM Spectrum Protect blueprint

General rules of thumbs are used to quickly decide the size of an IBM Spectrum Protect server, which are shown in Table 3-4.

Table 3-4 Selecting the size of the IBM Spectrum Protect server[6]

If your total managed data is in this range	And the amount of new data of your backup is in this range	Build a server of this size
60 TB - 240 TB	Up to 10 TB per day	Small
360 TB - 1440 TB	10 TB - 30 TB per day	Medium
1000 TB - 4000 TB	30 TB - 100 TB per day	Large

Support is available by requesting assistance for sizing a specific solution design.[7]

3.2.2 SAP HANA landscape solution

SAP Application Performance Standard (SAPS) is a hardware-independent unit of measurement that describes the performance of a system configuration in an SAP environment.

In the certification of IBM Power System models[8] for SAP applications, each server model configuration must be measured for its maximum SAPS capacity. SAP and IBM work closely to ensure that the server hardware meets all SAP criteria for certification.

Selecting a server is usually determined by the total number of SAP HANA databases and their combined database size for a server. As a rule of thumb, the amount of RAM for an SAP HANA database is twice as much as its size, that is, if an SAP HANA database size is 512 GB, the minimum RAM that must be available is 1 TB.

The IBM Power System H922 and IBM Power System H924 (or similarly configured IBM Power System S922, IBM Power System L922, and IBM Power System E980) satisfy the requirements for most installations, and they can host one or more SAP application landscapes. A solution architecture is shown in Figure 3-1 on page 55.

[5] https://www.ibm.com/support/pages/node/3608691 and https://www.ibm.com/cloud/blog/announcements/sap-hana-and-sap-netweaver-certified-for-ibm-power-systems-virtual-server

[6] https://www.ibm.com/support/pages/node/1146352

[7] https://www.ibm.com/it-infrastructure/services/lab-services

[8] https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/power-systems.html

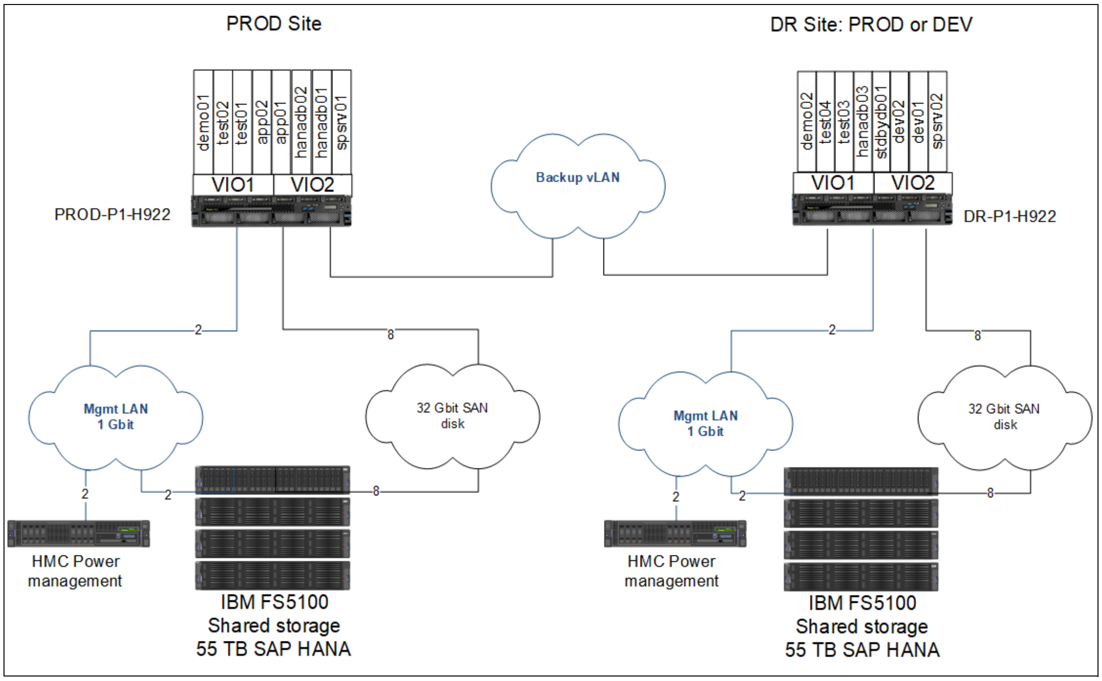


Figure 3-1 SAP HANA solution architecture

Using logical partitions (LPARs) and IBM PowerVM, a physical host can host many SAP HANA database and application servers. In this scenario, the IBM Spectrum Protect server is also running in the same hosts with replication to the IBM Cloud that is based on IBM Power Systems Virtual Servers for disaster recovery of the IBM Spectrum Protect service itself.

IBM FlashSystem uses fast storage and the FlashCopy function to support SAP HANA snapshots that use IBM Spectrum Copy Data Management. The snapshots can be replicated from the production site to the secondary site to protect them against storage failures.

3.2.3 General sizing metrics

A few general metrics are needed for the global environment. The default values are listed in Table 3-5.

Table 3-5 Global values for sizing

Metric	Value	Metric	Value
CPU architecture	IBM POWER	Replication window	8 hrs
Storage pool reserve	20%	IBM Spectrum Protect DB space reserve	20%

3.2.4 SAP HANA DB sizing metrics

When backing up databases, front-end capacity is required. Retention and frequency of backups are also metrics that are needed, as shown in Table 3-6.

Table 3-6 Database sizing metrics

Metric	Value	Metric	Value
Front-end SAP DB	40 TB	Daily change rate	5%
Daily retention (days)	32	Backup window	4 hr
Daily backup model	Full+Differential	Periodic full interval (days)	7
Periodic full workload calculation	Average	Long term	None

In this scenario, a weekly full and daily differential is selected with a retention of 32 days. The daily change rate is considered to be 5% of the front-end capacity.

With a backup window of 4 hours, it is then possible to estimate the required network bandwidth that is required to complete backups within that window.

Average means that full backups are spread evenly over the days of the week.

3.2.5 File-level sizing metrics

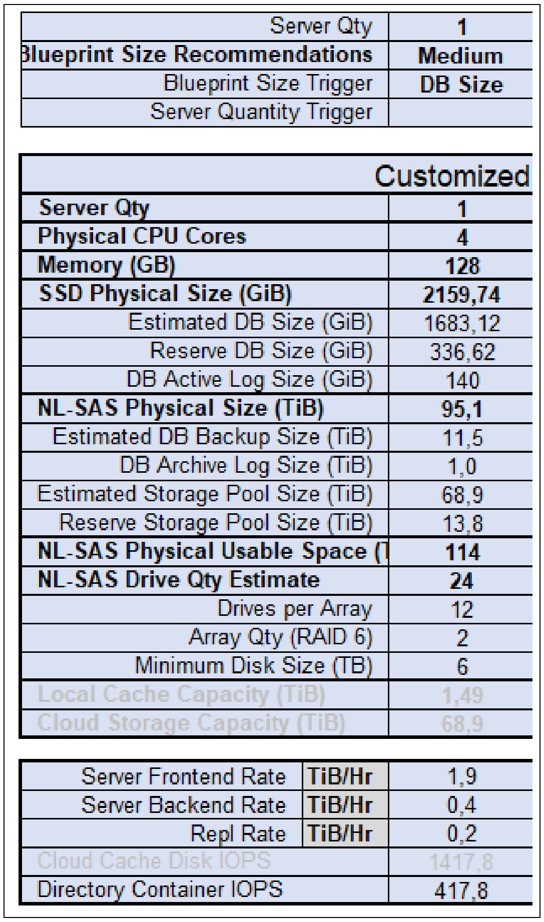
Only the daily changes of the files are backed up. There is no need for full backups afterward. In this scenario, the daily changes are retained for 32 days (Table 3-7), which applies to keeping all versions (`nolimit`) of a file for 32 days. There is a daily backup that saves up to 32 copies of a file if it changes every day.

Table 3-7 File-level sizing metrics

Metric	Value	Metric	Value
Front-end file level	15 TB	Daily change rate	2%
Daily retention (days)	32	Backup window	8 hr
Daily backup model	Incremental forever once a day	Long term	None

3.2.6 Sizing results

The blueprint result shows that we need one medium IBM Spectrum Protect server instance with four CPU cores and 128 GB of memory. The IBM Spectrum Protect database size will be 1683 GB. Other details are listed in Figure 3-2 on page 57.



Server Qty	1
Blueprint Size Recommendations	Medium
Blueprint Size Trigger	DB Size
Server Quantity Trigger	

	Customized
Server Qty	**1**
Physical CPU Cores	**4**
Memory (GB)	**128**
SSD Physical Size (GiB)	**2159,74**
Estimated DB Size (GiB)	1683,12
Reserve DB Size (GiB)	336,62
DB Active Log Size (GiB)	140
NL-SAS Physical Size (TiB)	**95,1**
Estimated DB Backup Size (TiB)	11,5
DB Archive Log Size (TiB)	1,0
Estimated Storage Pool Size (TiB)	68,9
Reserve Storage Pool Size (TiB)	13,8
NL-SAS Physical Usable Space (T	**114**
NL-SAS Drive Qty Estimate	**24**
Drives per Array	12
Array Qty (RAID 6)	2
Minimum Disk Size (TB)	6
Local Cache Capacity (TiB)	1,49
Cloud Storage Capacity (TiB)	68,9

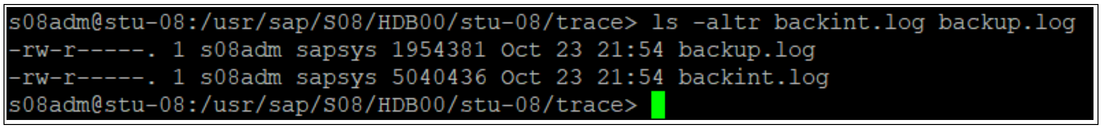
Server Frontend Rate	**TiB/Hr**	1,9
Server Backend Rate	**TiB/Hr**	0,4
Repl Rate	**TiB/Hr**	0,2
Cloud Cache Disk IOPS		1417,8
Directory Container IOPS		417,8

Figure 3-2 Sizing details

The sizing results show that the average daily ingest is 7.7 TB. To run this backup, the bandwidth from IBM Spectrum Protect clients to the IBM Spectrum Protect server must be 2.4 Gbps at a minimum to fulfill the backup window requirement of 8 hours, but in some situations full backups must run in parallel, which requires more bandwidth because of larger daily ingest. So, be sure provision more resources to meet these needs.

Automatic log file rotation

Information about backups is logged in the Backint log files `backint.log` and `backup.log`, as shown in Figure 3-3. By default, rotation is disabled and the files increase in storage usage over time.



```
s08adm@stu-08:/usr/sap/S08/HDB00/stu-08/trace> ls -altr backint.log backup.log
-rw-r-----. 1 s08adm sapsys 1954381 Oct 23 21:54 backup.log
-rw-r-----. 1 s08adm sapsys 5040436 Oct 23 21:54 backint.log
s08adm@stu-08:/usr/sap/S08/HDB00/stu-08/trace> 
```

Figure 3-3 Backup log files

Set `max_trace_file_size` and `max_trace_files` to hold enough information to troubleshoot failures and the retention of the backups. Monitor the file logs over the period of retention and adjust the maximum file size as needed.

3.2.7 Sizing for restore from Backint

During the restore of the database, first the data backup is read from the backup location and written into the SAP HANA data volumes. The I/O write orders of this data recovery with a size of 64 MB. Also, the redo log can be replayed during a database recovery, for example the log backups are read from the backup location, and the log volumes and the log entries get replayed.

> **Note:** The restore can run with the same number of channels and parallel sessions as the backup. Do not change the parameters in the SAP HANA profile.

It is paramount that data becomes available within the RTO timeframe. When sizing the bandwidth daily backups, it does not necessarily mean that the RTO is fulfilled.

For the case that is described in 3.2.4, “SAP HANA DB sizing metrics” on page 56, 3.2.5, “File-level sizing metrics” on page 56, and 3.2.6, “Sizing results” on page 56, we must restore 40 TB within 1 hour.

However, if the storage that also holds a copy of the snapshots fails, then the latest copy becomes relevant, so the bandwidth for restore can be different from the bandwidth for backup.

With parallel sessions of four, we must restore 10 TB per thread. With a 4 x 10 Gbit connections and an efficiency of 80%, we can theoretically restore this amount within 3 hours and 7 minutes. Jumbo frames can improve the throughput even more, but network adapters and LAN switches must support it.

Restores from backup disk storage must perform with the same speed as the network to not become a bottleneck.

Database backups are read from backup storage with 8 MB block sizes. Reading 40 TB of data within 3 hours requires some amount of read IOPS to be delivered by the shared storage system. Log files are read with 256 K block sizes.

After the full databases are restored, then the logs must be applied. The log files take time to recover and depend on the number of files to apply.

During the rollforward recovery portion of the restore, the logs attempt to be restored across the sessions, in this case four sessions. Log files are restored from the backup storage disks or cloud storage and not from tape, which degrades performance.

3.3 Sizing for snapshot

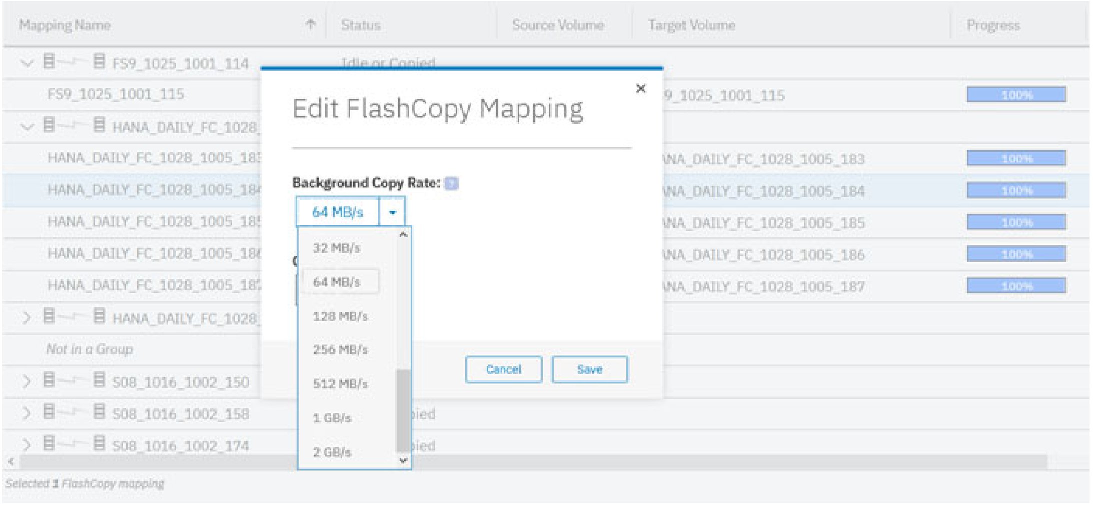
We must size for RPO, required capacity, and snapshot replication to auxiliary storage (if configured).

Sizing for RPO relates to how often a snapshot can run. With IBM Spectrum Virtualize FlashCopy (a function in IBM FlashSystem 5100) feature, the first snapshot is a regular FlashCopy with a full copy of the source volume into the target volume. The FlashCopy operation, either full or incremental, takes place almost instantly on the storage device. A background operation is also started to synchronize the written area between the source and target volumes.

Note: Incremental FlashCopy copies look like a full copy to SAP HANA, but hold only the block that is changed on the first full FlashCopy.

The first full FlashCopy takes some time. After that, if you are using incremental, the FlashCopy option changes only need to be copied, which makes the operation run faster. The background copy rate, as shown in Figure 3-4, can be increased to complete the copy operation faster, but this adds more load on the storage controller. Especially be aware when running multiple snapshots of several databases concurrently.

Only one FlashCopy process and one at a time per source volume can be performed. So, plan the schedule to what can be completed in the disk device.



Mapping Name	Status	Source Volume	Target Volume	Progress
FS9_1025_1001_114	Idle or Copied			
FS9_1025_1001_115			9_1025_1001_115	100%
HANA_DAILY_FC_1028_				
HANA_DAILY_FC_1028_1005_18			NA_DAILY_FC_1028_1005_183	100%
HANA_DAILY_FC_1028_1005_18			NA_DAILY_FC_1028_1005_184	100%
HANA_DAILY_FC_1028_1005_18			NA_DAILY_FC_1028_1005_185	100%
HANA_DAILY_FC_1028_1005_18			NA_DAILY_FC_1028_1005_186	100%
HANA_DAILY_FC_1028_1005_18			NA_DAILY_FC_1028_1005_187	100%
HANA_DAILY_FC_1028_				
Not in a Group				
S08_1016_1002_150				
S08_1016_1002_158	ied			
S08_1016_1002_174	ied			

Selected 1 FlashCopy mapping

Edit FlashCopy Mapping

Background Copy Rate: 64 MB/s

Figure 3-4 FlashCopy Mapping options window

The quicker the copy completes, the more often a snapshot can run. But with IBM Spectrum Virtualize, the maximum FlashCopy targets per volume are 256, and the maximum FlashCopy capacity per I/O group is 4096 TB.[9]

With instant database restore, the SAP HANA database snapshot becomes immediately available for access, which can be useful for cloning, data analysis, validation, and other data reuse processes. This operation does not require more space in the back-end storage.

With an instant disk restore job, a full volume copy completes and requires the size of the source volume in the back-end storage.

When replicating snapshots by using asynchronous mirror to another storage system at a different site, then the bandwidth between the sites must be considered. Calculate for initial full copy and subsequent peak workloads.

[9] https://www.ibm.com/support/pages/v830x-configuration-limits-and-restrictions-ibm-system-storage-san-volume-controller

3.4 Sizing for growth

Periodically, check the size of the SAP HANA database in-memory and validate that the growth is as expected to adjust the data volume and the required size for its backup. This situation is particularly true for snapshots that store more data in the production disk systems.

> **Note:** Even though on IBM Spectrum Protect duplication and compression reduces the required capacity for backup data, it must be monitored.

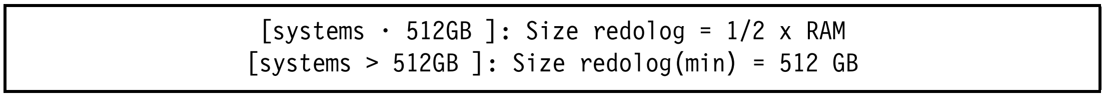
The `M_BACKUP_SIZE_ESTIMATIONS` in the SAP HANA systems view shows the estimated size of the database. The estimated size can differ from actual size.

The default log mode in an SAP HANA system is normal mode, which is recommended when using Backint to support PiT recovery.

In this normal mode for logs, the redo log files are saved on disk. Log files are overwritten when the log segment is backed up. If a backup is not frequent enough, the log area becomes full and no more log segments can be created, making the database freeze.

With Backint, the offload is automatic, and if its initial sizing is correct for `/hana/log`, the system does not reach an out of space condition unless an extreme workload is triggered or if the IBM Spectrum Protect server is unavailable.

Size the log space for normal operations with the rule of thumb shown in Figure 3-5.



```
[systems · 512GB ]: Size redolog = 1/2 x RAM
[systems > 512GB ]: Size redolog(min) = 512 GB
```

Figure 3-5 Log space rule of thumb[10]

[10] https://assets.cdn.sap.com/sapcom/docs/2015/03/74cdb554-5a7c-0010-82c7-eda71af511fa.pd

4

Installation and deployment

This chapter describes the steps to install and deploy IBM Spectrum Protect for Databases: Data Protection for SAP High-performance Analytic Appliance (HANA).

This chapter contains the following topics:

- 4.1, “Prerequisites” on page 62
- 4.2, “IBM Spectrum Protect server configuration” on page 62
- 4.3, “Installing and configuring the IBM Spectrum Protect Backup-Archive client application programming interface” on page 63
- 4.4, “Installing and configuring Data Protection for SAP HANA” on page 67
- 4.5, “More considerations” on page 71

4.1 Prerequisites

Requirements for Data Protection for SAP HANA are available in the hardware and software requirements technote for each release at Hardware and Software Requirements: Version 8.1 IBM Spectrum Protect for Enterprise Resource Planning.

Before you install Data Protection for SAP HANA, verify that the system meets the following prerequisites:

- SAP HANA is installed with the required version.
- IBM Spectrum Protect client is installed and configured on all SAP HANA nodes where you are going to install and configure Data Protection for SAP HANA.
- The SAP HANA database is configured on the system where you are going to install and configure Data Protection for SAP HANA.
- The SAP HANA Database (SAP HDB) client is installed on the system.
- During the installation and configuration of Data Protection for SAP HANA, root access to the appliance host operating system (OS) is required.

4.2 IBM Spectrum Protect server configuration

When a new server needs to be set up, follow the IBM Spectrum Protect Blueprint for planning, installation, and configuration at IBM Spectrum Protect Blueprints.

Also, for the latest version information, see Installing and upgrading the server.

Configure IBM Spectrum Protect server policies to receive SAP HANA backups to meet local requirements. Plan for the retention periods, and backup and archive destinations. Note the management classes that are created because they are used during agent configuration.

In our lab environment for this publication, we made the following configuration, as shown in Figure 4-1 on page 63.

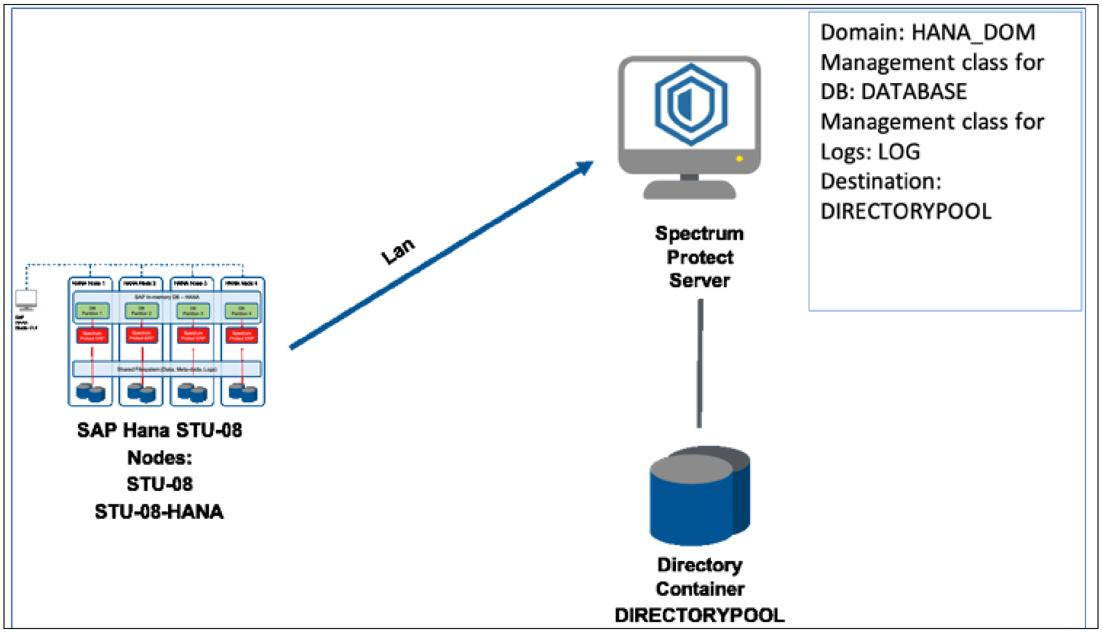


Figure 4-1 Lab configuration

In our lab, both management classes DATABASE and LOGS back up data to the same directory container pool, each one with its own retention period.

Note: For this publication, we created only one node for the SAP HANA database: STU-08-HANA. In steady state environments with several tenant databases, more than one node can be created with different management classes for the retention of database and logs.

Data Protection for SAP HANA stores data in the archive copy group of the management classes. This data expires after a defined number of days. When no backup is being done within this timeframe, all backup data expires and is no longer available for restore. As an alternative, the copy group parameter **`retver`**, which specifies the number of days a file is to be kept, can be set to unlimited (`9999` or **`nolimit`**). Obsolete backups can be deleted manually by using SAP HANA Studio.

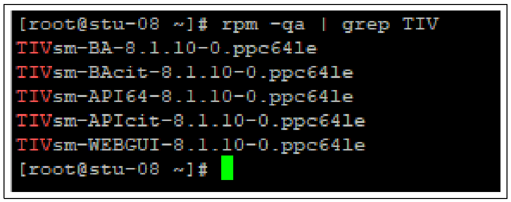
4.3 Installing and configuring the IBM Spectrum Protect Backup-Archive client application programming interface

The IBM Spectrum Protect client must be installed and configured on all nodes of the SAP HANA cluster, including the application and database servers. These clients include the backup-archive client for the file system backups, and the application programming interface (API) client for interface programs. The API client is used to enhance existing applications with backup, archive, restore, and retrieve services. An installed and confirmed API client is a prerequisite for Data Protection for SAP HANA.

4.3.1 Installing the IBM Spectrum Protect Backup-Archive client

Follow the procedure in IBM Spectrum Protect UNIX and Linux Backup-Archive Clients Version 8.1.9: Installation and User's Guide.

In our lab, we installed the GSKit packages and the full package of the API and baclient, as shown in Figure 4-2.



```
[root@stu-08 ~]# rpm -qa | grep TIV
TIVsm-BA-8.1.10-0.ppc64le
TIVsm-BAcit-8.1.10-0.ppc64le
TIVsm-API64-8.1.10-0.ppc64le
TIVsm-APIcit-8.1.10-0.ppc64le
TIVsm-WEBGUI-8.1.10-0.ppc64le
[root@stu-08 ~]#
```

Figure 4-2 IBM Spectrum Protect Backup-Archive Packages installed

4.3.2 Configuring the IBM Spectrum Protect Backup-Archive client

In our lab environment, the following steps were followed after the installation of the client code:

1. Configuration and options files.

   The following files are created, as shown in Example 4-1 and Example 4-2.

Example 4-1 dsm.sys

```
SErvername AIX-AW
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   10.0.240.164
   Nodename STU-08
   Passwordaccess generate
   ERRORLOGName /tsm/dsmerror.log
   SCHEDLOGName /tsm/dsmsched.log
   SCHEDLOGRetention 30 D
   InclExcl /opt/ ivoli/tsm/client/ba/bin/inclexcl.list

Servername AIX-AW-HANA
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   10.0.240.164
   Nodename STU-08-HANA
   PASSWORDACCESS GENERATE
   ERRORLOGName /tsm/S08/dsmerror_dec.log
   PASSWORDDIR /tsm/S08
   SCHEDLOGName /tsm/S08/dsmsched_dec.log
   SCHEDLOGRetention 30 D
```

Example 4-2 dsm.opt

```
Servername AIX-AW
```

2. Create a symbolic link from the API folder to the `dsm.sys` file in the BA folder.

   When the IBM Spectrum Protect API client is installed in an UNIX or Linux system, check that a link exists that points to the IBM Spectrum Protect API installation directory, /usr/tivoli/tsm/client/api/ bin64:

```
[root@stu-08 bin64]# pwd
/opt/ ivoli/tsm/client/api/bin64
[root@stu-08 bin64]# ln -s /opt/ ivoli/tsm/client/ba/bin/dsm.sys dsm.sys
[root@stu-08 bin64]# ls -l dsm.sys
lrwxrwxrwx. 1 root root 37 Oct 15 22:27 dsm.sys -> /opt/
ivoli/tsm/client/ba/bin/dsm.sys
```

3. Connect to the IBM Spectrum Protect server.

   Use **`dsmc`** to connect to the IBM Spectrum Protect server and register the password, as shown in Example 4-3.

Example 4-3 Registering the password in the IBM Spectrum Protect server

```
[root@stu-08 ~]# dsmc
IBM Spectrum Protect
Command-Line Backup-Archive Client Interface
  Client Version 8, Release 1, Level 10.0
  Client date/time: 10/15/2020 22:42:08
(c) Copyright by IBM Corporation and other(s) 1990, 2020. All Rights Reserved.

Node Name: STU-08
Enter your user ID <STU-08>:

Enter password for user ID "STU-08":

Session established with server AIX-AW: AIX
  Server Version 8, Release 1, Level 10.000
  Server date/time: 10/15/2020 21:55:27  Last access: 10/15/2020 18:37:46

Protect> q ses
IBM Spectrum Protect Server Connection Information

Home Server Name........: AIX-AW
Server Type.............: AIX
Archive Retain Protect..: "No"
Server Version..........: Ver. 8, Rel. 1, Lev. 10.0
Last Access Date........: 10/15/2020 18:37:46
Delete Backup Files.....: "No"
Delete Archive Files....: "Yes"
Deduplication...........: "Server Only"

Node Name...............: STU-08
User Name...............: root

SSL Information.........: TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Secondary Server Information
Not configured for failover

Protect> quit
```

4.3.3 Environment variables

IBM Spectrum Protect provides two features for specifying the location of the IBM Spectrum Protect API Client error log: the environment variable DSMI_LOG and the IBM Spectrum Protect system client option ERRORLOGName in dsm.sys. For DSMI_LOG, a directory is specified to which a file that is named dsierror.log is written. For ERRORLOGName, a path and user-defined file name are defined.

To achieve conclusive logical linking of the environment, configuration, and log files in your SAP backup-archive system, use the IBM Spectrum Protect system client option ERRORLOGName rather than the environment variable DSMI_LOG.

When you use ERRORLOGName, you can include the system ID (SID) in the file name. This information can speed up problem determination by simplifying identification of the correct error log file. You can match log file names to the active user client options file name, which must also contain the SID and be stored in environment variable DSMI_CONFIG. This information is especially useful on systems with several SIDs.

To set up the environment variables, edit the files sapenv.sh (for bash shell) and .sapenv.csh (for C shell) from the <sid>adm user home folder to include the lines for the variables DSMI_DIR, DSMI_CONFIG, and DSMI_LOG, as shown in Example 4-4.

Example 4-4 Lab environment variables

```
s08adm@stu-08:/usr/sap/S08/home> pwd
/usr/sap/S08/home
s08adm@stu-08:/usr/sap/S08/home> cat .sapenv.sh | grep -i dsmi
export DSMI_DIR=/opt/tivoli/tsm/api/bin64
export DSMI_CONFIG=/tsm/S08/dsm.opt
export DSMI_LOG=/tsm/S08

s08adm@stu-08:/usr/sap/S08/home> cat .sapenv.csh | grep -i dsmi
setenv DSMI_DIR /opt/tivoli/tsm/api/bin64
setenv DSMI_CONFIG /tsm/S08/dsm.opt
setenv DSMI_LOG /tsm/S08
```

Log out and log in to ensure that the environment variables are activated, as shown in Example 4-5.

Example 4-5 Active environment variables

```
[root@stu-08 linux]# su - s08adm
Last login: Thu Oct 15 23:03:41 CEST 2020 on pts/0
s08adm@stu-08:/usr/sap/S08/HDB00>
s08adm@stu-08:/usr/sap/S08/HDB00> env | grep -i dsmi
DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
DSMI_LOG=/tsm/S08
DSMI_CONFIG=/tsm/S08/dsm.opt
```

If the variable DSMI_LOG exists in your environment from an earlier setup, it is overridden by the dsm.sys option ERRORLOGName. However, to avoid confusion, check that the DSMI_LOG path is identical to the path in ERRORLOGName. Alternatively, you can remove DSMI_LOG from your environment.

4.4 Installing and configuring Data Protection for SAP HANA

The Data Protection for SAP HANA agent must be installed in all nodes that make up the SAP HANA environment that has an instance of the SAP HANA database.

4.4.1 Installing Data Protection for SAP HANA agent

Download and extract the required package to a temp folder. As root, run the binary file according to your OS. In our lab, we used the following procedure:

1. Extract the `.gz` file with the command:

   ```
   tar -xgvf
   ```

2. Run the binary file for the corresponding OS under `erp_dvd_hana/linux`, which in our case is `8.1.9.0-ERP-HANA-LinuxPPCle.bin`, and follow the wizard by selecting the language and accepting the license.
3. Review the pre-installation summary to check that all prerequisites are met, and note the installation folder (`/opt/tivoli/tsm/tdp_hana`). When the installation is successfully complete, you receive the information that is shown in Example 4-6.

Example 4-6 Installation completion message

```
Installation Complete
---------------------

Congratulations! IBM Spectrum Protect for Enterprise Resource Planning Data
Protection for SAP HANA(R) has been successfully installed.

Configure IBM Spectrum Protect for Enterprise Resource Planning Data
Protection for SAP HANA(R) now.

Use the script setup.sh in /opt/tivoli/tsm/tdp_hana

Press "Done" to quit the installer.

PRESS <ENTER> TO EXIT THE INSTALLER:
```

4.4.2 Configuring Data Protection for SAP HANA

The configuration of the Data Protection for SAP HANA agent is done by using the script **`setup.sh`** that is shown at the end of the installation wizard. As a root user, go to `/opt/Tivoli/tsm/tdp_hana` and run the script.

You need the following information for the system and the tenant databases:

- SAP HANA system ID (SAP HSID).
- Username and password of the database user with system privileges.
- Stanza name for the IBM Spectrum Protect SAP HANA backup in `dsm.sys`.
- Nodename.
- Number of parallel sessions that are required.
- Retention of full backups (`MAX_VERSIONS`).
- Management class for the database backups.
- Management class for the log backups.

Example 4-7 shows the steps and information for our lab in bold.

Example 4-7 Lab environment details

```
[root@stu-08 tdp_hana]# ./setup.sh

     IBM Spectrum Protect for Enterprise Resource Planning
                Data Protection for SAP HANA(R)
                  Version 8.1.9.0 build 759
    (c) Copyright IBM Corporation, 2011-2018, All Rights Reserved.

Enter the SAP HANA(R) system ID [S08]: S08
Enter instance number [00]: 00
Enter the name of the database user with System Privileges INIFILE ADMIN, CATALOG
READ, SERVICE ADMIN and DATABASE ADMIN [SYSTEM]: SYSTEM
Enter password of database user 'SYSTEM': XXXXX

Pre-installation checks completed successfully. Press enter to start installation.

Creating directory "/usr/sap/S08/SYS/global/hdb/opt/hdbconfig"
Do you want to set up the IBM Spectrum Protect configuration now [y/n] y
Enter the number of full backups that shall be retained (MAX_VERSIONS): 4
Do you want to use automatic password handling (passwordaccess generate) [y/n] y
Enter the IBM Spectrum Protect server name as defined in dsm.sys: AIX-AW-HANA

Found server stanza for server "AIX-AW-HANA".
Parameter "PASSWORDACCESS GENERATE" is set correctly for server "AIX-AW-HANA".
Parameter "NODENAME" is set for server "AIX-AW-HANA".
Enter the number of Sessions to the IBM Spectrum Protect server you want to use:
4
Enter one or more IBM Spectrum Protect management classes for database backups:
DATABASE
The number of IBM Spectrum Protect management classes specifies the number of
backup copies of redo logs. Enter one or more IBM Spectrum Protect management
classes for log file backups:  LOG

Creating/updating keystore entries ...
   Setting key "TSM" in the hdbuserstore on host stu-08.


               IBM Spectrum Protect for Enterprise Resource Planning

                         Data Protection for SAP HANA(R)


            - Version 8, Release 1, Modification 9.0 for Linux on POWER 64-bit LE
-
                  Build: 759  compiled on Sep 20 2019

                        Licensed Materials - Property of IBM.
            (c) Copyright IBM Corporation 1996, 2019  All Rights Reserved.

#SOFTWAREID "backint 1.05" "IBM Spectrum Protect for Enterprise Resource Planning
- Data Protection for SAP HANA(R) 8.1.9.0"
BKI2027I: Using IBM Spectrum Protect-API Version 8.1.10.0 (compiled with 8.1.0.2).
BKI2000I: Successfully connected to ProLE on port tdphana.
```

```
BKI0005I: Start of program at: Thu 15 Oct 2020 11:35:26 PM CEST.
BKI0049I: Enter the password for node STU-08-HANA on server AIX-AW-HANA:
BKI0051I: Password successfully verified for node STU-08-HANA on server
AIX-AW-HANA.
BKI0020I: End of program at: Thu 15 Oct 2020 11:35:37 PM CEST.
BKI0021I: Elapsed time: 11 sec.
BKI0024I: Return code is: 0.

Creating link '/usr/sap/S08/SYS/global/hdb/opt/hdbbackint' ->
'/opt/tivoli/tsm/tdp_hana/hdbbackint'


Changed the following configuration parameter in global.ini in section [backup]:
log_backup_parameter_file = /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
catalog_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
data_backup_parameter_file = /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
log_backup_using_backint = true
catalog_backup_using_backint = true
parallel_data_backup_backint_channels = 4


Activated the configuration changes successfully.

Tenant databases detected ...
The following tenant databases were found: S08
```

Note: At this point, if you want to enter 'n', the tenant DB (S08) uses the same configuration as the system DB. If you created different nodes and management classes for the tenant DB, note them here.

```
Do you want to configure IBM Spectrum Protect for ERP Data Protection for SAP
HANA(R) to protect the tenant database S08? [y/n] y


Starting configuration for tenant database S08 ...
Existing configuration files in /usr/sap/S08/SYS/global/hdb/opt/hdbconfig will be
reused.
Do you want to reenter the passwords for all IBM Spectrum Protect nodes now? [y/n]
y

               IBM Spectrum Protect for Enterprise Resource Planning

                         Data Protection for SAP HANA(R)


             - Version 8, Release 1, Modification 9.0 for Linux on POWER 64-bit LE
-
                  Build: 759  compiled on Sep 20 2019

                        Licensed Materials - Property of IBM.
            (c) Copyright IBM Corporation 1996, 2019  All Rights Reserved.
```

```
#SOFTWAREID "backint 1.05" "IBM Spectrum Protect for Enterprise Resource Planning
- Data Protection for SAP HANA(R) 8.1.9.0"
BKI2027I: Using IBM Spectrum Protect-API Version 8.1.10.0 (compiled with 8.1.0.2).
BKI2000I: Successfully connected to ProLE on port tdphana.
BKI0005I: Start of program at: Thu 15 Oct 2020 11:46:38 PM CEST.
BKI0049I: Enter the password for node STU-08-HANA on server AIX-AW-HANA:
BKI0051I: Password successfully verified for node STU-08-HANA on server
AIX-AW-HANA.
BKI0020I: End of program at: Thu 15 Oct 2020 11:46:49 PM CEST.
BKI0021I: Elapsed time: 11 sec.
BKI0024I: Return code is: 0.

Changed the following configuration parameter in global.ini in layer 'DATABASE,
S08' section [backup]:
log_backup_parameter_file = /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
catalog_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
data_backup_parameter_file = /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/initS08.utl
log_backup_using_backint = true
catalog_backup_using_backint = true
parallel_data_backup_backint_channels = 4


Configuration changes for tenant database S08 must be activated MANUALLY
  either by restarting the tenant database or by using the
  SQL statement 'ALTER SYSTEM RECONFIGURE SERVICE'.

Press enter to continue



[Thu Oct 15 23:46:52 CEST 2020] *** Setup finished successfully! ***
```

For correct planning, up to Version 8.1.9 of the Data Protection for SAP HANA, a restart of the tenant databases must be done before any backup attempt as mentioned in the configuration procedure, either manually or by running **ALTER SYSTEM RECONFIGURE SERVICE**.

Log in as <sid>adm and restart the tenant services, as shown in Example 4-8.

Example 4-8 Restarting the tenant services

```
[root@stu-08 tdp_hana]# su - s08adm
Last login: Thu Oct 15 23:54:01 CEST 2020 on pts/0
s08adm@stu-08:/usr/sap/S08/HDB00> hdbsql -d S08

Welcome to the SAP HANA Database interactive terminal.

Type:  \h for help with commands
       \q to quit

hdbsql=>
Username: SYSTEM
Password:
hdbsql S08=>
hdbsql S08=> ALTER SYSTEM RECONFIGURE SERVICE ('','',0);
0 rows affected (overall time 312.803 msec; server time 311.226 msec)
```

```
hdbsql S08=> quit
s08adm@stu-08:/usr/sap/S08/HDB00> hdbsql -d COCKPITDB

Welcome to the SAP HANA Database interactive terminal.

Type:  \h for help with commands
       \q to quit

hdbsql=>
Username: SYSTEM
Password:
hdbsql COCKPITDB=>
hdbsql COCKPITDB=>
hdbsql COCKPITDB=>
hdbsql COCKPITDB=> ALTER SYSTEM RECONFIGURE SERVICE ('','',0);
0 rows affected (overall time 193.603 msec; server time 192.060 msec)

hdbsql COCKPITDB=> \q
```

To test the backup, run the following command:

```
hdbsql -i 00 -u SYSTEM -p <password>  "backup data using backint ('DAILY')"
```

4.5 More considerations

Some parameters in the configuration files can be changed for a better performance and better deduplication when backing up to container pools.

4.5.1 BUFFSIZE

As mentioned in 3.1.7, “Backing up to an IBM Spectrum Protect container pool with inline deduplication and compression” on page 52, when using an IBM Spectrum Protect container storage pool (cloud or directory type), deduplication savings can be achieved by increasing the buffer size that is used by the Data Protection for SAP HANA client for transferring the database backup data.

The `buffsize` parameter has a default value of 128 KB, but can be up to 32 MB. Experimentation has shown that larger buffsizes yield better deduplication savings. However, an 8 MB buffer size (`BUFFSIZE 8388608`) is a good balance between deduplication efficiency and memory consumption. Log backups must still use a small buffer size (for example, 256 KB) for best efficiency.

SAP HANA can specify different configuration files for data and log backups by using the following parameters in the `.utl` file:

- `data_backup_parameter_file`
- `log_backup_parameter_file`

To change these parameter values, copy the original `utl` file to a new file for log backup, as shown in Example 4-9.

Example 4-9 Copying the .utl file

```
[root@stu-08 hdbconfig]# cd /usr/sap/S08/SYS/global/hdb/opt/hdbconfig/
[root@stu-08 hdbconfig]# ls -l
total 36
-rw-r--r--. 1 s08adm sapsys    33 Oct 15 23:31 agent.lic
-rw-r-----. 1 s08adm sapsys   347 Oct 15 23:46 initCOCKPITDB.bki
-rw-r-----. 1 s08adm sapsys 11868 Oct 15 23:46 initCOCKPITDB.utl
-rw-r-----. 1 s08adm sapsys   347 Oct 15 23:46 initS08.bki
-rw-r-----. 1 s08adm sapsys 11838 Oct 15 23:35 initS08.utl

[root@stu-08 hdbconfig]# cp -p initS08.utl initS08_log.utl
```

In the file `initS08.utl`, change the `BUFFSIZE` parameter to the following line:

```
BUFFSIZE                8388608             # block size in bytes
```

These changes can also be done from SAP HANA Studio or SAP HANA Cockpit.

Note: Parameter change is dynamic and does not require an SAP HANA restart. The effectiveness of the SAP HANA changes on Backint and the new buffer settings can be checked in the `backint.log` file for the data and log backup sessions that are established with the IBM Spectrum Protect server.

4.5.2 MAX_SESSIONS

As a best practice for using multiple backup streams, check that the number of parallel streams (`parallel_data_backup_backint_channels`) is aligned with the `MAX_SESSIONS` parameter in the `utl` file (in our case, four parallel sessions are used), and also with the `MAXNUMMP` node parameter on the IBM Spectrum Protect server, which must support the parallel mount points for the data transfer.

Note: If the backup goes directly to tape, then the performance of the SAP HANA system must deliver data fast enough so that all required tapes remain in streaming mode. Otherwise, drives must stop and rewind, which impacts performance. Check the available number of tapes that can be used during the whole backup period and use this number of tapes for this parameter.

5

Backup, restore, and recovery scenarios for SAP HANA

This chapter provides practical examples for backing up and recovering an SAP High-performance Analytic Appliance (HANA) database by creating snapshot backups. This task is accomplished by using IBM Spectrum Copy Data Management and data backups that use an IBM Spectrum Protect Data Protection for SAP HANA Backint agent.

This chapter contains the following topics:

5.1 The backup environment

This chapter provides several scenarios for backing up and recovering an SAP HANA database. The environment that is used for the tests is illustrated in Figure 5-1.

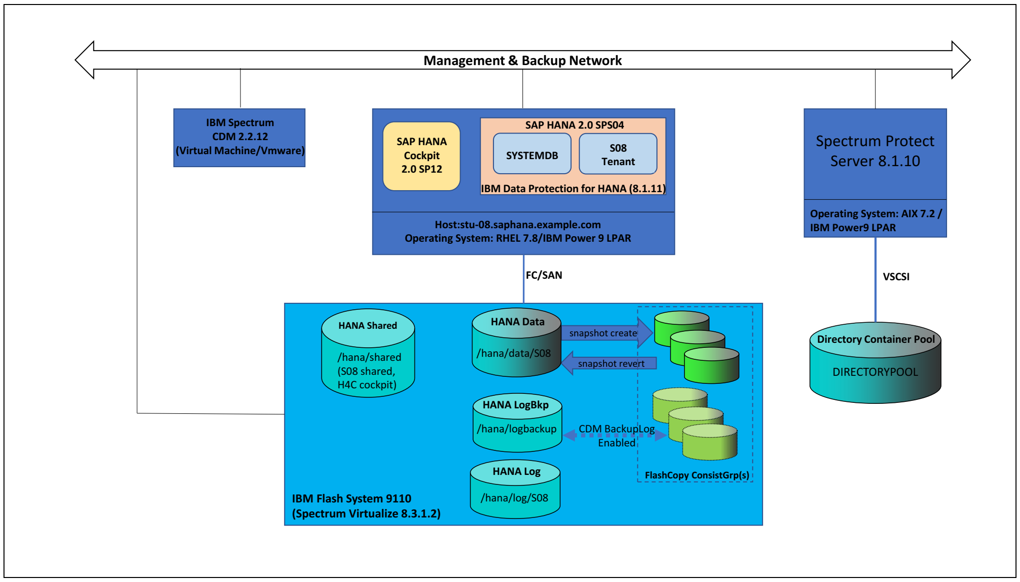

Management & Backup Network
IBM Spectrum CDM 2.2.12 (Virtual Machine/Vmware)
SAP HANA Cockpit 2.0 SP12
SAP HANA 2.0 SPS04
SYSTEMDB
S08 Tenant
IBM Data Protection for HANA (8.1.11)
Host:stu-08.saphana.example.com
Operating System: RHEL 7.8/IBM Power 9 LPAR
Spectrum Protect Server 8.1.10
Operating System: AIX 7.2 / IBM Power9 LPAR
FC/SAN
VSCSI
HANA Shared
/hana/shared (S08 shared, H4C cockpit)
HANA Data
/hana/data/S08
snapshot create
snapshot revert
HANA LogBkp
/hana/logbackup
CDM BackupLog Enabled
HANA Log
/hana/log/S08
FlashCopy ConsistGrp(s)
IBM Flash System 9110 (Spectrum Virtualize 8.3.1.2)
Directory Container Pool
DIRECTORYPOOL

Figure 5-1 Test environment for SAP HANA backup and recovery

The following software components are deployed:

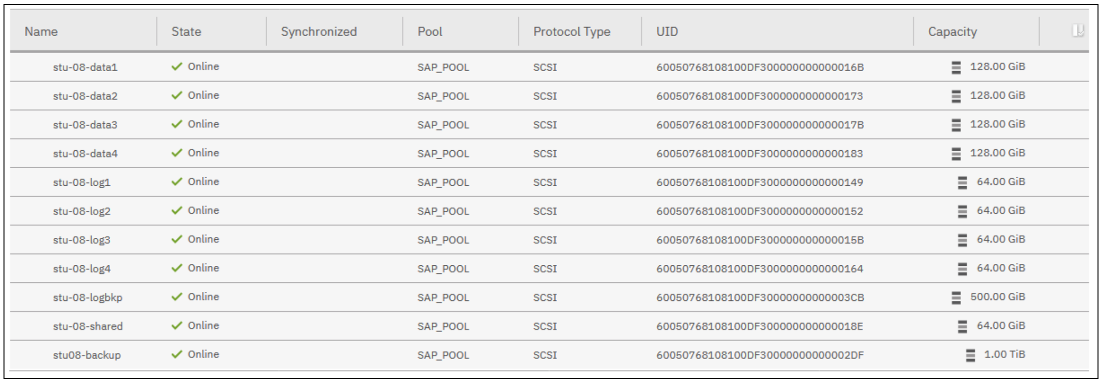
- SAP HANA environment:
  - SAP HANA Database (SAP HDB) 2.0 SPS 04.
  - SAP HANA Cockpit 2.0 SP 12.
  - Operating system (OS): Red Hat Enterprise Linux 7.8 Little Endian (LE) on an IBM POWER9 LPAR.
  - SAP HANA Studio 2.3.53 installed on an external Windows workstation.
- SAP HANA storage environment:
  - IBM FlashSystem 9110 with IBM Spectrum Virtualize V8.3.1.2.
  - Fibre Channel (FC) attachment to SAP HANA on an IBM POWER9 server.
- Backup management:
  - IBM Spectrum Protect 8.1.10 Server on an IBM POWER9 LPAR with IBM AIX® 7.2.
  - IBM Data Protection for SAP HANA 8.1.11 deployed on an SAP HANA logical partition (LPAR).
  - IBM Spectrum Copy Data Management 2.2.12 deployed on a VMware 6.5 environment.

The disk layout that used in our environment is summarized in Table 5-1 on page 75.

Table 5-1 File systems created for an SAP HANA S08 instance on the server (stu-08)

File system	Role	File system type	Logical volume manager information	Disk composition
`/hana/shared/S08`	SAP HANA shared folder and SAP HANA Cockpit environment	XFS	VG: `VG_S08_SHARED` LV: `LV_S08_SHARED`	1x 64 GB
`/hana/data/S08`	SAP HANA data files location	XFS	VG: `VG_S08_DATA` LV: `LV_S08_DATA`	4x 128 GB
`/hana/log/S08`	SAP HANA redo log location	XFS	VG: `VG_S08_LOG` LV: `LV_S08_LOG`	4x 64 GB
`/hana/logbackup`	Location for backup of redo logs with IBM Spectrum Copy Data Management	XFS	VG: `VG_S08_LOGBKP` LV: `LV_S08_LOGBKP`	1x 500 GB
`/hana/backup`	General-purpose database backups to file	XFS	VG: `VG_S08_BACKUP` LV: `LV_S08_BACKUP`	1x 1 TB

The LUNs that are allocated from the IBM Spectrum Virtualize storage (IBM FlashSystem 9110) are displayed in Figure 5-2. The disk sizes are used only to support the SAP HANA build and the backup environment for the current test cases that are shown in this chapter.



Name	State	Synchronized	Pool	Protocol Type	UID	Capacity
stu-08-data1	✓ Online		SAP_POOL	SCSI	60050768108100DF300000000000016B	128.00 GiB
stu-08-data2	✓ Online		SAP_POOL	SCSI	60050768108100DF3000000000000173	128.00 GiB
stu-08-data3	✓ Online		SAP_POOL	SCSI	60050768108100DF300000000000017B	128.00 GiB
stu-08-data4	✓ Online		SAP_POOL	SCSI	60050768108100DF3000000000000183	128.00 GiB
stu-08-log1	✓ Online		SAP_POOL	SCSI	60050768108100DF3000000000000149	64.00 GiB
stu-08-log2	✓ Online		SAP_POOL	SCSI	60050768108100DF3000000000000152	64.00 GiB
stu-08-log3	✓ Online		SAP_POOL	SCSI	60050768108100DF300000000000015B	64.00 GiB
stu-08-log4	✓ Online		SAP_POOL	SCSI	60050768108100DF3000000000000164	64.00 GiB
stu-08-logbkp	✓ Online		SAP_POOL	SCSI	60050768108100DF30000000000003CB	500.00 GiB
stu-08-shared	✓ Online		SAP_POOL	SCSI	60050768108100DF300000000000018E	64.00 GiB
stu08-backup	✓ Online		SAP_POOL	SCSI	60050768108100DF30000000000002DF	1.00 TiB

Figure 5-2 Allocation of the storage LUNs to the SAP HANA system stu-08

5.2 SAP HANA backup

This section presents practical examples for backing up an SAP HANA database in various scenarios that are based on IBM Spectrum Protect and IBM Spectrum Copy Data Management with storage snapshot technology that is based on IBM Spectrum Virtualize.

5.2.1 Backing up an SAP HANA database with IBM Spectrum Protect

IBM Spectrum Protect for Enterprise Resource Planning (ERP) provides data protection for an SAP HANA database by using the Data Protection for SAP HANA Backint agent, which transfers the backup data to the IBM Spectrum Protect server for managing the data backups according to the configured policies. For the configuration guidelines of Data Protection for SAP HANA agent and the IBM Spectrum Protect server, see Chapter 4, “Installation and deployment” on page 61.

This scenario performs the SAP HANA database backup and the log backup by using the IBM Spectrum Protect Data Protection for SAP HANA agent.

Automatic log back up to IBM Spectrum Protect

As result of running the configuration script of the IBM Spectrum Protect Backint agent for SAP HANA database (**setup.sh**), the log backup is configured for automatic backup to the IBM Spectrum Protect server. SAP HANA ensures that the logs are backed up after a log file becomes full or a specified length of time elapses. By default, the time interval for the log backup is 15 minutes (900 seconds), and it can be tuned for a different value according to your recovery point objective (RPO) by changing the parameter `log backup_timeout_s`. For more information about this parameter, see Change the Log Backup Interval.

For our scenario, log backup was enabled with the default time interval (900 seconds), and by default it is not showing up in the `global.ini` configuration file unless it is explicitly set to a value. Our environment uses an IBM Spectrum Protect directory container pool as the target pool for both database and log backups. For this case, we suggest changing the default `MAXBUFFSIZE` parameter in the Data Protection for SAP HANA `initSID.utl` configuration file to maximize the deduplication achievements for the database backups on the IBM Spectrum Protect server while maintaining the default value of the parameter for the log and catalog backups. Thus, distinct `initSID.utl` files are used for database and log backups. For more information about configuration details and recommendations for using IBM Spectrum Protect container pools for SAP HANA backup, see 4.4, “Installing and configuring Data Protection for SAP HANA” on page 67.

The SAP HANA `global.ini` for the system and the tenant database (S08) is shown in Example 5-1.

Example 5-1 The global.ini configuration files for system and S08 tenant

```
****Global system configuration file ************************************
[root@stu-08 ~]# cat /hana/shared/S08/global/hdb/custom/config/global.ini
# global.ini last modified 2020-11-10 16:54:09.507168 by hdbnameserver
[backup]
log_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(SAPSYSTEMNAME)_log.utl
catalog_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(SAPSYSTEMNAME)_log.utl
parallel_data_backup_backint_channels = 4
data_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(SAPSYSTEMNAME).utl
```

```
catalog_backup_using_backint = true
log_backup_using_backint = true

[communication]
ssl = systempki

[multidb]
mode = multidb
database_isolation = low

[persistence]
basepath_datavolumes = /hana/data/S08
basepath_logvolumes = /hana/log/S08

[system_information]
xsa_sizing = M
************Global configuration file for tenant database S08***************
[root@stu-08 ~]# cat /hana/shared/S08/global/hdb/custom/config/DB_S08/global.ini
# global.ini last modified 2020-11-10 16:54:07.753783 by hdbindexserver -port
30003
[backup]
log_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(DBNAME)_log.utl
catalog_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(DBNAME)_log.utl
parallel_data_backup_backint_channels = 4
data_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(DBNAME).utl
catalog_backup_using_backint = true
log_backup_using_backint = true
```

Observe that catalog and redo log backups are using the same `utl` file that is specific to the `utl` file that is used by the database backups.

The database and log activity with Backint can be monitored by using the file `backint.log`, which is specific for each database, including the system database, and it is located by default at the following paths:

- System database: `$DIR_INSTANCE/<HOST>/trace`
- Tenant database: `$DIR_INSTANCE/<HOST>/trace/DB_<DBNAME>`

Running a full backup job by using the command-line interface

The command-line interface (CLI) uses a minimal SQL client environment that is provided by the **`hdbsql`** command, which is available on any SAP HANA system. The use of native SQL CLI for generating database backups is also useful for generating scripts that can be scheduled for running at certain time intervals. IBM Spectrum Protect offers a central scheduling mechanism for such a script running the database backup, which can be used on one or even multiple SAP HANA instances, which integrates the backup of SAP HANA databases into the IBM Spectrum Protect centralized monitoring framework of the entire enterprise backup. An example of SAP HANA full backup script is shown in Appendix A, “Scheduling an SAP HANA backup by using IBM Spectrum Protect” on page 113.

For performing a database backup, connect to the SAP HANA system as `<sid>adm` user and run the **`hdbsql`** command. Connectivity to the SAP HANA database requires a database user and password, but when Data Protection for SAP HANA agent is configured, a new key that is called TSM is created in the SAP HANA secure user store for database access (see Example 5-2). The management of the secure user store can be performed by using the **`hdbuserstore`** command. For more information about this command, see Secure User Store (hdbuserstore).

Example 5-2 Listing SAP HANA Secure User Store that contains the TSM key entry

```
s08adm@stu-08:/usr/sap/S08/home> hdbuserstore LIST
DATA FILE       : /usr/sap/S08/home/.hdb/stu-08/SSFS_HDB.DAT
KEY FILE        : /usr/sap/S08/home/.hdb/stu-08/SSFS_HDB.KEY

KEY GENDATA
  ENV : stu-08:30015
  USER: SYSTEM
  DATABASE: S08
KEY S08SAPDBCTRLS08
  ENV : stu-08:30015
  USER: SAPDBCTRL
KEY TSM
  ENV : stu-08:30013
  USER: SYSTEM
```

We perform a full backup of the S08 database by using a prefix of ‘**`FULL_BACKUP_S08_TEST’`** with the following command:

```
hdbsql -U TSM -d S08 “backup data using backint ('FULL_BACKUP_S08_TEST')”
```

Observe in the previous command where we connected to the tenant DB to perform the database backup. The same backup of the tenant database can also be done by connecting to the system database by running the following command:

```
hdbsql -U TSM -d SYSTEMDB “backup data for S08 using backint
('FULL_BACKUP_S08_TEST')”
```

We can check the database backup in the catalog by using native SQL too. A sample output for an SQL query of the database files that are correlated with the backup `PREFIX` that is provided at the time of backup (“`FULL_BACKUP_S08_TEST`”) is provided in Example 5-3.

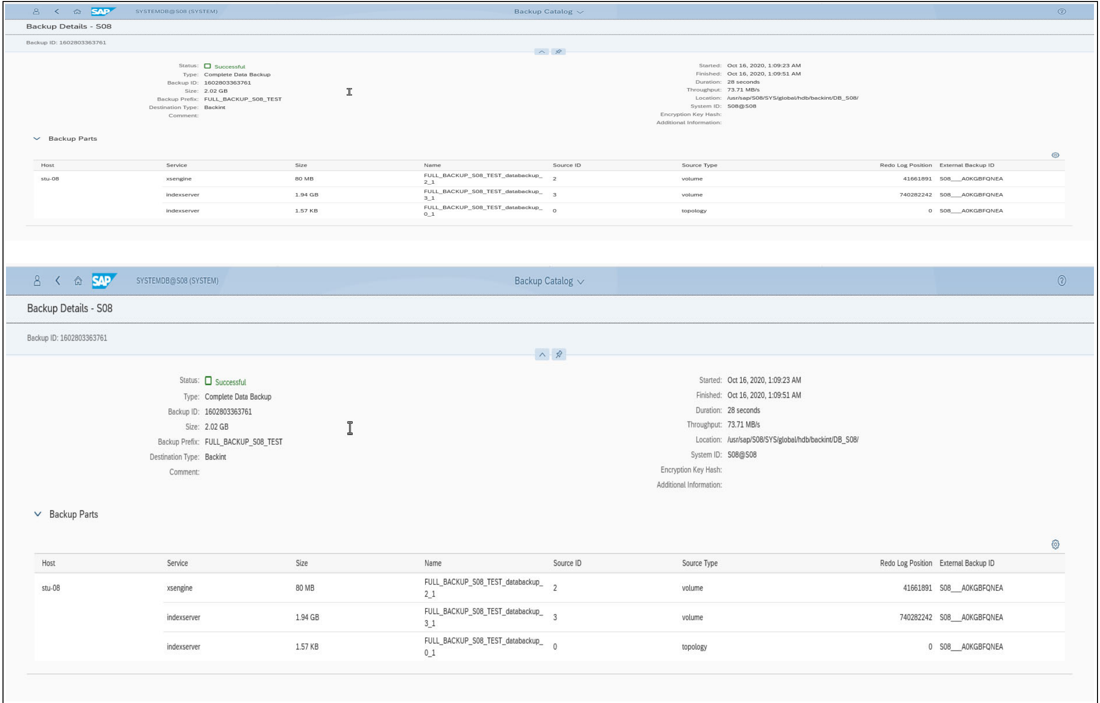
Example 5-3 Checking the backup catalog entries for a specific backup PREFIX

```
s08adm@stu-08:/usr/sap/S08/home> hdbsql -U TSM -d S08

Welcome to the SAP HANA Database interactive terminal.

Type:  \h for help with commands
       \q to quit

hdbsql S08=> SELECT A.BACKUP_ID, A.ENTRY_TYPE_NAME,
A.SYS_START_TIME,A.SYS_END_TIME,B.BACKUP_SIZE,B.DESTINATION_PATH,B.DESTINATION_TYPE_NAME,B.EXTERNAL_BACKUP_ID FROM
M_BACKUP_CATALOG A, M_BACKUP_CATALOG_FILES B WHERE A.BACKUP_ID=B.BACKUP_ID and A.STATE_NAME = 'successful' AND
A.ENTRY_TYPE_NAME = 'complete data backup' and B.DESTINATION_PATH like '%FULL_BACKUP_S08_TEST%' ORDER BY
A.UTC_START_TIME desc;

BACKUP_ID,ENTRY_TYPE_NAME,SYS_START_TIME,SYS_END_TIME,BACKUP_SIZE,DESTINATION_PATH,DESTINATION_TYPE_NAME,EXTERNAL_BACKUP
_ID
1602803363761,"complete data backup","2020-10-16 01:09:23.762000000","2020-10-16
01:09:51.797000000",83886080,"/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_datab
ackup_2_1","backint","S08___AOKGBFQNEA"
```

```
1602803363761,"complete data backup","2020-10-16 01:09:23.762000000","2020-10-16
01:09:51.797000000",2080374784,"/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_dat
abackup_3_1","backint","S08___AOKGBFQNEA"
1602803363761,"complete data backup","2020-10-16 01:09:23.762000000","2020-10-16
01:09:51.797000000",1608,"/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databacku
p_0_1","backint","S08___AOKGBFQNEA"
3 rows selected (overall time 60.839 msec; server time 9495 usec)
```

Observe in Example 5-3 on page 78 that all files that are generated as part of the same backup operation have a common backup ID (first field in the output) in the SAP HANA backup catalog and also the same external backup ID (last field in the output), which is generated when the Backint type of backup is used.

We can also verify that the CLI-generated backup is present in the catalog by using the SAP HANA Cockpit GUI. We access the catalog database for S08 and filter by “complete data backups”. See the catalog entry and the backup details in Figure 5-3.



Backup Details - S08

Backup ID: 1602803363761

Status: □ Successful
Type: Complete Data Backup
Backup ID: 1602803363761
Size: 2.02 GB
Backup Prefix: FULL_BACKUP_S08_TEST
Destination Type: Backint
Comment:

Started: Oct 16, 2020, 1:09:23 AM
Finished: Oct 16, 2020, 1:09:51 AM
Duration: 28 seconds
Throughput: 73.71 MB/s
Location: /usr/sap/S08/SYS/global/hdb/backint/DB_S08/
System ID: S08@S08
Encryption Key Hash:
Additional Information:

Backup Parts

Host	Service	Size	Name	Source ID	Source Type	Redo Log Position	External Backup ID
stu-08	xsengine	80 MB	FULL_BACKUP_S08_TEST_databackup_2_1	2	volume	41661891	S08___A0KGBFQNEA
	indexserver	1.94 GB	FULL_BACKUP_S08_TEST_databackup_3_1	3	volume	740282242	S08___A0KGBFQNEA
	indexserver	1.57 KB	FULL_BACKUP_S08_TEST_databackup_0_1	0	topology	0	S08___A0KGBFQNEA

Backup Details - S08

Backup ID: 1602803363761

Status: □ Successful
Type: Complete Data Backup
Backup ID: 1602803363761
Size: 2.02 GB
Backup Prefix: FULL_BACKUP_S08_TEST
Destination Type: Backint
Comment:

Started: Oct 16, 2020, 1:09:23 AM
Finished: Oct 16, 2020, 1:09:51 AM
Duration: 28 seconds
Throughput: 73.71 MB/s
Location: /usr/sap/S08/SYS/global/hdb/backint/DB_S08/
System ID: S08@S08
Encryption Key Hash:
Additional Information:

Backup Parts

Host	Service	Size	Name	Source ID	Source Type	Redo Log Position	External Backup ID
stu-08	xsengine	80 MB	FULL_BACKUP_S08_TEST_databackup_2_1	2	volume	41661891	S08___A0KGBFQNEA
	indexserver	1.94 GB	FULL_BACKUP_S08_TEST_databackup_3_1	3	volume	740282242	S08___A0KGBFQNEA
	indexserver	1.57 KB	FULL_BACKUP_S08_TEST_databackup_0_1	0	topology	0	S08___A0KGBFQNEA

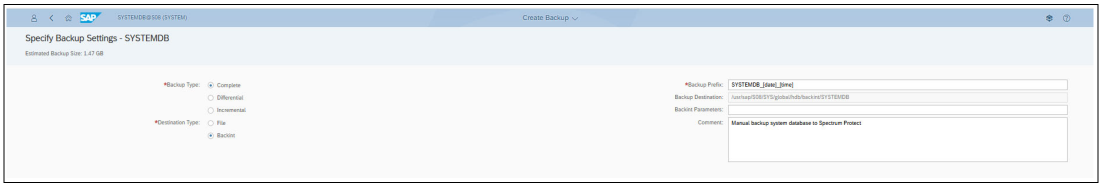
Figure 5-3 Verifying the backup completion in the database backup catalog by using SAP HANA Cockpit

Running a backup by using SAP HANA GUI

Both SAP HANA Cockpit and SAP HANA Studio can be used for performing a manual backup by using the GUI mode. This section shows the backup operations by using the SAP HANA Cockpit interface.

Performing the backup of a system database

From the catalog backup of the SYSTEMDB, click **Create Backup** and provide the input parameters for a full backup, as shown in Figure 5-4.



Specify Backup Settings - SYSTEMDB

Estimated Backup Size: 1.47 GB

*Backup Type: ● Complete ○ Differential ○ Incremental

*Destination Type: ○ File ● Backint

*Backup Prefix: SYSTEMDB_[date]_[time]

Backup Destination: /usr/sap/S08/SYS/global/hdb/backint/SYSTEMDB

Backint Parameters:

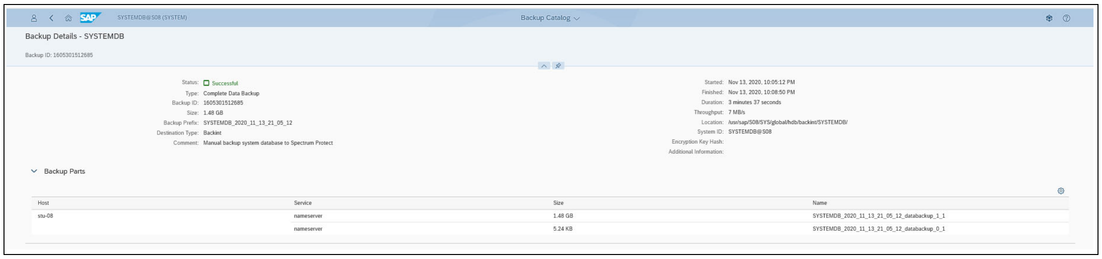
Comment: Manual backup system database to Spectrum Protect

Figure 5-4 Full database backup for the system database by using SAP HANA Cockpit

Here is the SQL statement that is associated with the full backup operation from SAP HANA Cockpit:

```
BACKUP DATA USING BACKINT ('SYSTEMDB_2020_11_13_21_04_16' ) ASYNCHRONOUS COMMENT
'Manual backup system database to IBM Spectrum Protect'
```

The final result is displayed in Figure 5-5.



Backup Details - SYSTEMDB

Backup ID: 1605301512685

Status: Successful
Type: Complete Data Backup
Backup ID: 1605301512685
Size: 1.48 GB
Backup Prefix: SYSTEMDB_2020_11_13_21_05_12
Destination Type: Backint
Comment: Manual backup system database to Spectrum Protect

Started: Nov 13, 2020, 10:05:12 PM
Finished: Nov 13, 2020, 10:08:50 PM
Duration: 3 minutes 37 seconds
Throughput: 7 MB/s
Location: /usr/sap/S08/SYS/global/hdb/backint/SYSTEMDB/
System ID: SYSTEMDB@S08
Encryption Key Hash:
Additional Information:

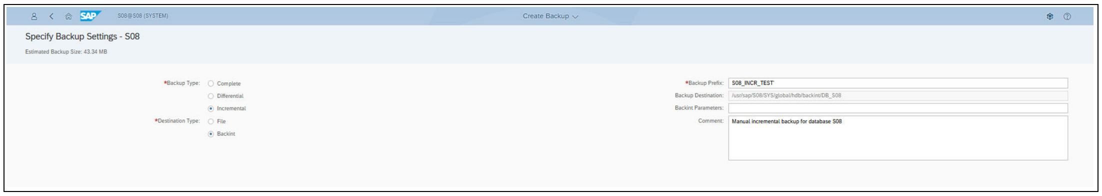
Backup Parts

Host	Service	Size	Name
stu-08	nameserver	1.48 GB	SYSTEMDB_2020_11_13_21_05_12_databackup_1_1
	nameserver	5.24 KB	SYSTEMDB_2020_11_13_21_05_12_databackup_0_1

Figure 5-5 Result of the full backup of system database

Creating a tenant DB backup series

This section generates a series of backups for an S08 tenant database consisting of full, differential, and incremental backups. All three types of backups are triggered from the same **Create Backup** action that is started from the **Catalog Backup** menu of the S08 database (see Figure 5-6).



Specify Backup Settings - S08

Estimated Backup Size: 43.34 MB

*Backup Type: ○ Complete ○ Differential ● Incremental

*Destination Type: ○ File ● Backint

*Backup Prefix: S08_INCR_TEST

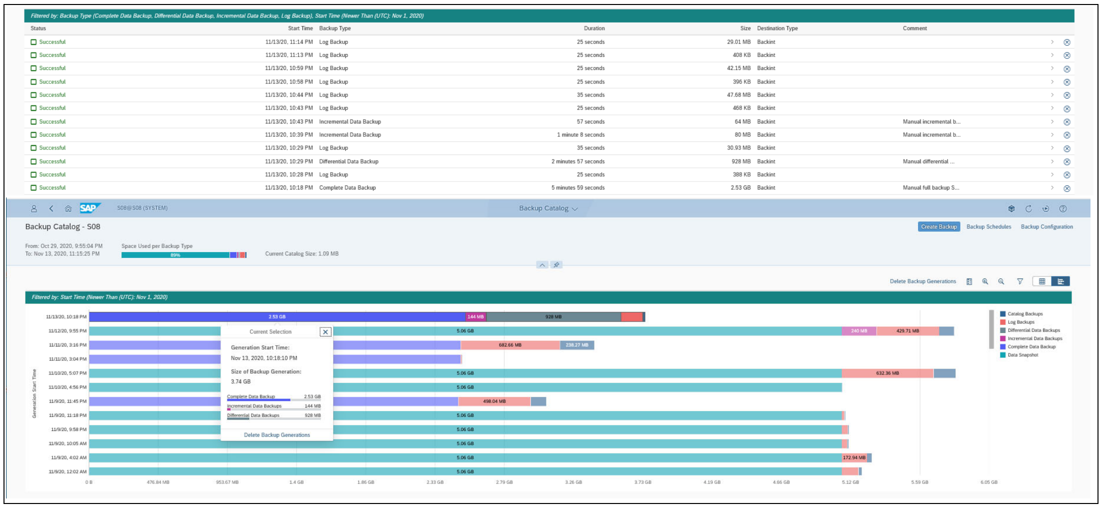
Backup Destination: /usr/sap/S08/SYS/global/hdb/backint/DB_S08

Backint Parameters:

Comment: Manual incremental backup for database S08

Figure 5-6 Incremental backup for an S08 database

All series of backups that are related to a full backup, including any differential, incremental, and log backups, are grouped into a backup generation. SAP HANA Cockpit offers a combined view of all types of backups that are part of backup generation, and an overall view of all generations, as shown in Figure 5-7 on page 81.



Filtered by: Backup Type (Complete Data Backup, Differential Data Backup, Incremental Data Backup, Log Backup), Start Time (Newer Than (UTC): Nov 1, 2020)

Status	Start Time	Backup Type	Duration	Size	Destination Type	Comment
Successful	11/13/20, 11:14 PM	Log Backup	25 seconds	29.01 MB	Backint	
Successful	11/13/20, 11:13 PM	Log Backup	25 seconds	408 KB	Backint	
Successful	11/13/20, 10:59 PM	Log Backup	25 seconds	42.15 MB	Backint	
Successful	11/13/20, 10:58 PM	Log Backup	25 seconds	396 KB	Backint	
Successful	11/13/20, 10:44 PM	Log Backup	35 seconds	47.68 MB	Backint	
Successful	11/13/20, 10:43 PM	Log Backup	25 seconds	468 KB	Backint	
Successful	11/13/20, 10:43 PM	Incremental Data Backup	57 seconds	64 MB	Backint	Manual incremental b...
Successful	11/13/20, 10:39 PM	Incremental Data Backup	1 minute 8 seconds	80 MB	Backint	Manual incremental b...
Successful	11/13/20, 10:29 PM	Log Backup	35 seconds	30.93 MB	Backint	
Successful	11/13/20, 10:29 PM	Differential Data Backup	2 minutes 57 seconds	928 MB	Backint	Manual differential ...
Successful	11/13/20, 10:28 PM	Log Backup	25 seconds	388 KB	Backint	
Successful	11/13/20, 10:18 PM	Complete Data Backup	5 minutes 59 seconds	2.53 GB	Backint	Manual full backup S...

S08@S08 (SYSTEM)

Backup Catalog - S08

From: Oct 29, 2020, 9:55:04 PM
To: Nov 13, 2020, 11:15:25 PM

Space Used per Backup Type

Current Catalog Size: 1.09 MB

Filtered by: Start Time (Newer Than (UTC): Nov 1, 2020)

Current Selection

Generation Start Time:
Nov 13, 2020, 10:18:10 PM

Size of Backup Generation:
3.74 GB

Complete Data Backup	2.53 GB
Incremental Data Backups	144 MB
Differential Data Backups	928 MB

Figure 5-7 Displaying a backup generation consisting of full, differential/incremental, and log backups

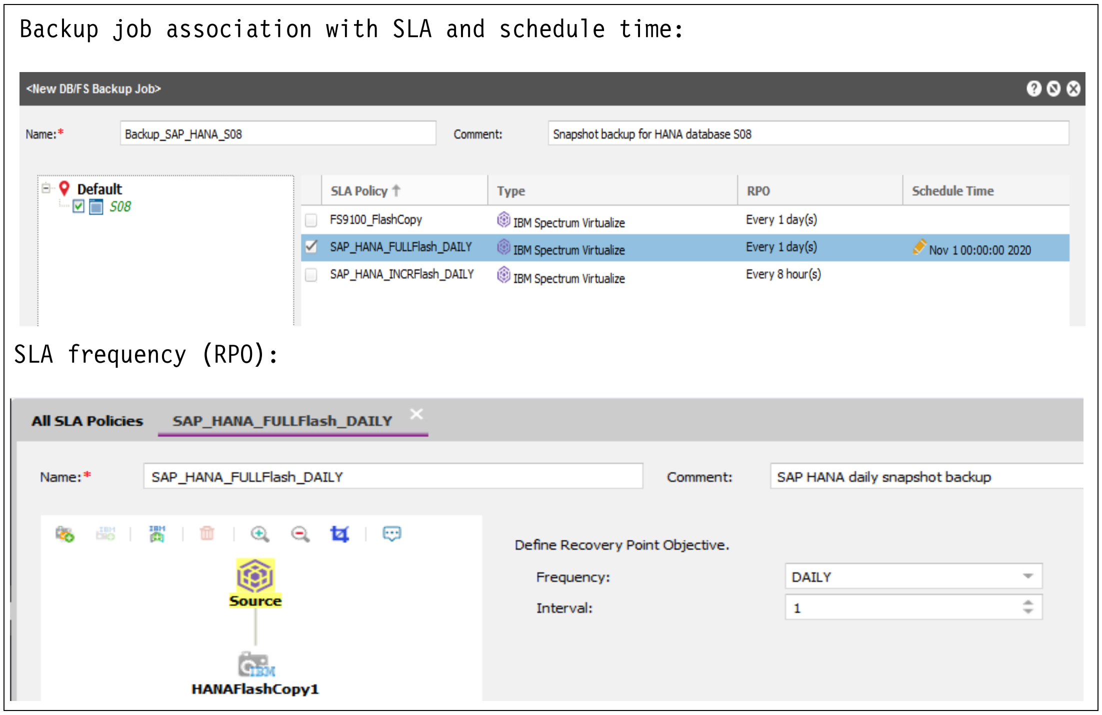
5.2.2 Performing a database snapshot backup by using IBM Spectrum Copy Data Management

This section provides practical examples for running SAP HANA snapshot backup by using IBM Spectrum Copy Data Management. The snapshot backup is an operation that is triggered outside SAP HANA by IBM Spectrum Copy Data Management, which manages the creation of the backups, automatic storage data copy deletion based on service-level agreement (SLA) policies, and the restore operations.

Enabling scheduled SAP HANA snapshot backups on IBM Spectrum Copy Data Management can be performed when defining the backup job configuration:

1. Specify the job initial date and time to run.
2. Define the job frequency by associating the backup job with an SLA policy, where the frequency interval is defined. Multiple SLA policies can be associated with a single backup job.

Figure 5-8 shows a daily full FlashCopy operation for SAP HANA database at noon.



```
Backup job association with SLA and schedule time:
```

<New DB/FS Backup Job>

Name:* Backup_SAP_HANA_S08

Comment: Snapshot backup for HANA database S08

Default
- ☑ S08

	SLA Policy	Type	RPO	Schedule Time
☐	FS9100_FlashCopy	IBM Spectrum Virtualize	Every 1 day(s)	
☑	SAP_HANA_FULLFlash_DAILY	IBM Spectrum Virtualize	Every 1 day(s)	Nov 1 00:00:00 2020
☐	SAP_HANA_INCRFlash_DAILY	IBM Spectrum Virtualize	Every 8 hour(s)	

```
SLA frequency (RPO):
```

All SLA Policies | SAP_HANA_FULLFlash_DAILY

Name:* SAP_HANA_FULLFlash_DAILY

Comment: SAP HANA daily snapshot backup

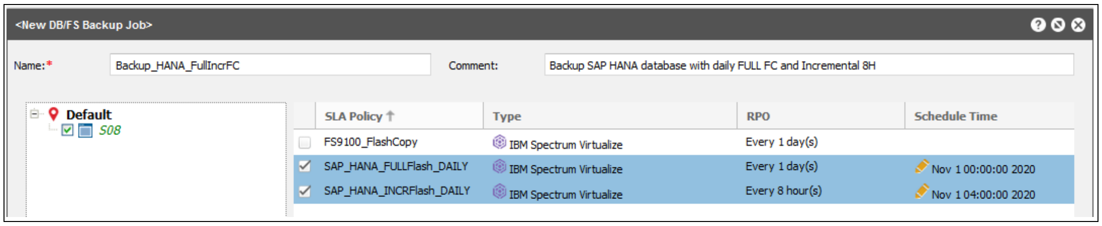
Define Recovery Point Objective.

Frequency: DAILY

Interval: 1

Figure 5-8 Running a daily backup job by using a full FlashCopy operation on storage

Multiple combinations can be established between a job and SLA policies to determine a more complex backup job definition. For example, establishing an SAP HANA backup job with daily Full FlashCopy and three incremental copies (RPO=8H) can accomplish by running two jobs where each is bound to the specific SLA policy (Full FlashCopy with daily frequency and Incremental FlashCopy with 8H frequency), or by using a single job and associating both SLA policies to it, as shown in Figure 5-9. Ensure that the scheduled time is defined so that the Full and Incremental operations do not overlap.



<New DB/FS Backup Job>

Name:* Backup_HANA_FullIncrFC

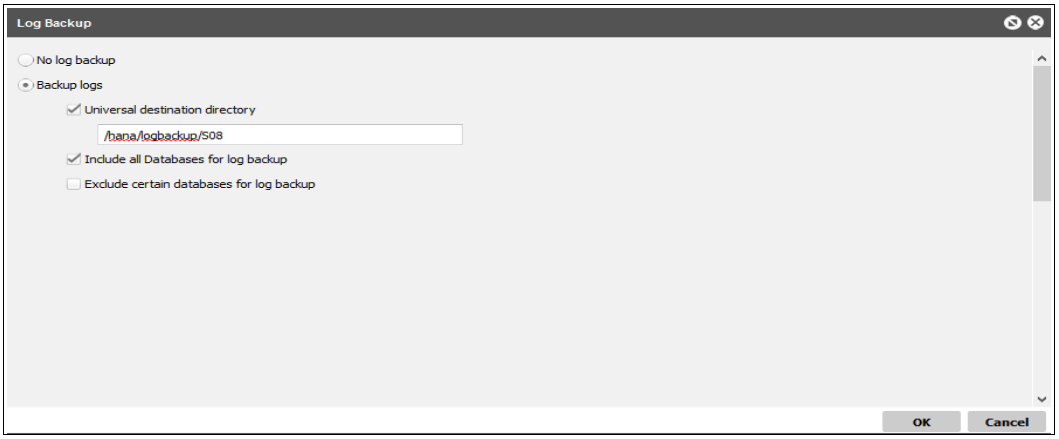
Comment: Backup SAP HANA database with daily FULL FC and Incremental 8H

Default
- ☑ S08

	SLA Policy	Type	RPO	Schedule Time
☐	FS9100_FlashCopy	IBM Spectrum Virtualize	Every 1 day(s)	
☑	SAP_HANA_FULLFlash_DAILY	IBM Spectrum Virtualize	Every 1 day(s)	Nov 1 00:00:00 2020
☑	SAP_HANA_INCRFlash_DAILY	IBM Spectrum Virtualize	Every 8 hour(s)	Nov 1 04:00:00 2020

Figure 5-9 Defining a backup job with two SLA policies

Starting with IBM Spectrum Copy Data Management V2.2.11, the backup of the SAP HANA logs can be enabled to go to a specific location that is also included in the storage FlashCopy operation. In our environment, we created a `/hana/logbackup` volume for enabling the backup of SAP HANA redo logs to this target. The location must exist in the subfolder `catalog` and it must have write permissions for the SAP HANA instance owner (`<sid>adm`). After setting up the IBM Spectrum Copy Data Management job option for SAP HANA log backup and running the job, the SAP HANA configuration is changed for automatic log backup to the new location, as shown in Figure 5-10 on page 83.



○ No log backup

● Backup logs

☑ Universal destination directory

/hana/logbackup/S08

☑ Include all Databases for log backup

□ Exclude certain databases for log backup

Figure 5-10 IBM Spectrum Copy Data Management backup with SAP HANA log backup

Example 5-4 shows the changes that occur in the `global.ini` files for system and tenant databases.

Example 5-4 Changes in the global.ini files for system and tenant databases

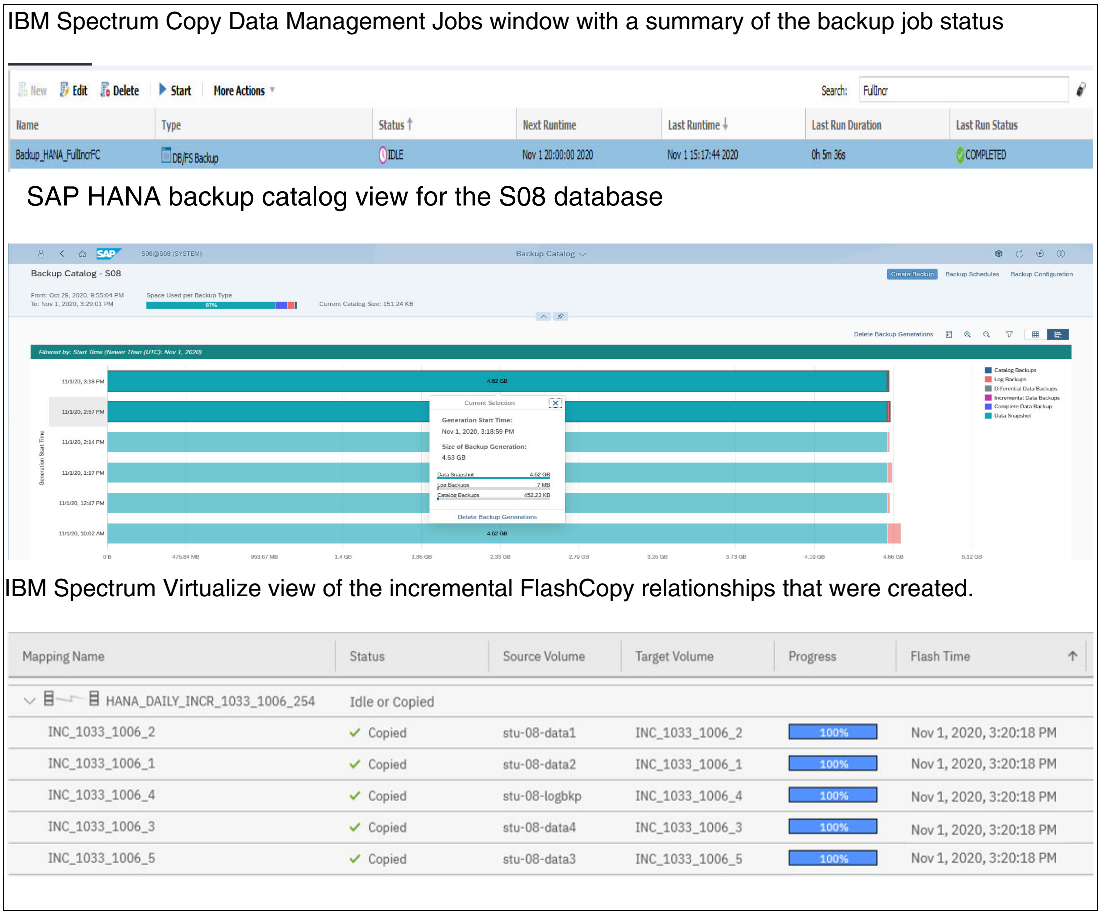
```
[root@stu-08 log]# cat /hana/shared/S08/global/hdb/custom/config/global.ini
# global.ini last modified 2020-11-01 16:18:24.637323 by hdbnameserver
[communication]
ssl = systempki

[multidb]
mode = multidb
database_isolation = low

[persistence]
basepath_catalogbackup = /hana/logbackup/S08/catalog
basepath_logbackup = /hana/logbackup/S08
basepath_datavolumes = /hana/data/S08
basepath_logvolumes = /hana/log/S08

[system_information]
xsa_sizing = M
[root@stu-08 log]# cat /hana/shared/S08/global/hdb/custom/config/DB_S08/global.ini
# global.ini last modified 2020-11-01 16:18:24.128549 by hdbindexserver -port 30003
[persistence]
basepath_catalogbackup = /hana/logbackup/S08/catalog
basepath_logbackup = /hana/logbackup/S08
```

You can also use log backup enablement to Backint by using the IBM Spectrum Protect agent for SAP HANA database. When log backup is enabled on an IBM Spectrum Copy Data Management job and IBM Spectrum Protect is also configured for SAP HANA database automatic redolog backup, the destination of the redo log backups is controlled by the parameter `log_backup_using_backint`. It is by default set during the configuration process of Data Protection for SAP HANA agent to save the redo logs files to IBM Spectrum Protect server. For a sample configuration of SAP HANA backup in an environment that uses both IBM Spectrum Copy Data Management an IBM Spectrum Protect, see 5.2.3, “Backing up SAP HANA by using IBM Spectrum Protect and IBM Spectrum Copy Data Management” on page 84.

The backup jobs can be run manually from the Jobs view. Right-click the job and select **Start**. Taking the job example from Figure 5-9 on page 82, we run a manual snapshot backup and select the SLA ‘`SAP_HANA_INCRFlash_DAILY`’. The backup job can be monitored from the Activity window while it is running.

After the job completes, it is moved to the History window. From the History window, you can download the entire log activity journal in CSV format by accessing the GUI details of the activity log and clicking **Download All**. The snapshot backups that are triggered from IBM Spectrum Copy Data Management are populated to the SAP HANA backup catalog and marked as Data Snapshot.

Observe the result details for the manual backup operation on all involved layers (IBM Spectrum Copy Data Management, SAP HANA database, and IBM Spectrum Virtualize storage), as shown in Figure 5-11.



IBM Spectrum Copy Data Management Jobs window with a summary of the backup job status

Name	Type	Status	Next Runtime	Last Runtime	Last Run Duration	Last Run Status
Backup_HANA_FullIncrFC	DB/FS Backup	IDLE	Nov 1 20:00:00 2020	Nov 1 15:17:44 2020	0h 5m 36s	✓ COMPLETED

SAP HANA backup catalog view for the S08 database

IBM Spectrum Virtualize view of the incremental FlashCopy relationships that were created.

Mapping Name	Status	Source Volume	Target Volume	Progress	Flash Time
HANA_DAILY_INCR_1033_1006_254	Idle or Copied				
INC_1033_1006_2	✓ Copied	stu-08-data1	INC_1033_1006_2	100%	Nov 1, 2020, 3:20:18 PM
INC_1033_1006_1	✓ Copied	stu-08-data2	INC_1033_1006_1	100%	Nov 1, 2020, 3:20:18 PM
INC_1033_1006_4	✓ Copied	stu-08-logbkp	INC_1033_1006_4	100%	Nov 1, 2020, 3:20:18 PM
INC_1033_1006_3	✓ Copied	stu-08-data4	INC_1033_1006_3	100%	Nov 1, 2020, 3:20:18 PM
INC_1033_1006_5	✓ Copied	stu-08-data3	INC_1033_1006_5	100%	Nov 1, 2020, 3:20:18 PM

Figure 5-11 Job result summary: IBM Spectrum Copy Data Management, SAP HANA Cockpit, and storage

5.2.3 Backing up SAP HANA by using IBM Spectrum Protect and IBM Spectrum Copy Data Management

This scenario uses both IBM Spectrum Protect for database and log backup, and snapshot backup based on IBM Spectrum Copy Data Management. This scenario is comprehensive, which provides the best protection option by combining the fast recovery time capability of snapshot backup with an enhanced recovery objective that is based on automatic log backup to IBM Spectrum Protect.

The following configuration example combines the capability of both IBM Spectrum Protect and IBM Spectrum Copy Data Management for a comprehensive backup scenario:

- Automatic log backup by using IBM Spectrum Protect Data Protection for SAP HANA agent (Backint).
- Weekly database full backup of type Backint to IBM Spectrum Protect by using IBM Spectrum Protect scheduler with a retention of 1 month.
- Daily database snapshot backup by using IBM Spectrum Copy Data Management and full FlashCopy operation on IBM Spectrum Virtualize storage maintaining up to seven snapshots on the storage device.

The following items summarize the configuration that is required to cover the previous requirements:

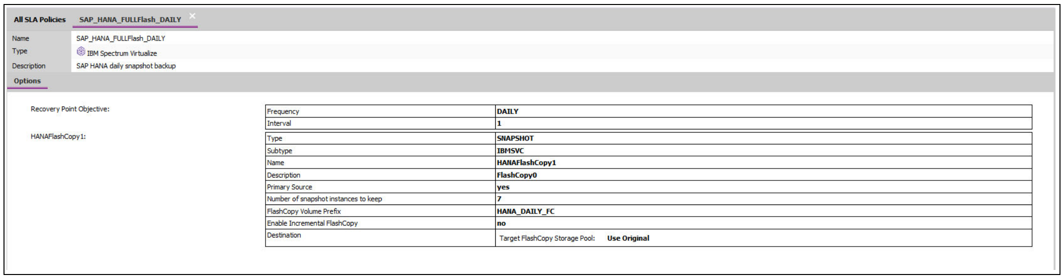
- IBM Spectrum Protect configuration:
  - `MAX_VERSIONS` is set to `4` in the `initSID.utl` file. The parameter is initially set by using the Data Protection for SAP HANA utility (**`setup.sh`**) and can be changed to a different value in the `utl` file according to the retention requirements. In our context, the parameter is set to `4` to cover a 1-month period with four weekly full backups.
  - The log backup is set to the Backint destination (`log_backup_using_backint = true`). By default, the log backup and catalog backup are set to Backint during the Data Protection for SAP HANA configuration.
  - An IBM Spectrum Protect scheduler is defined for a weekly SAP HANA full database backup by using the script **`/tsm/scripts/HANA_full_bkp.sh`** with the parameters that are shown in Example 5-5. For an example of the script that we used in our environment, see Appendix A, “Scheduling an SAP HANA backup by using IBM Spectrum Protect” on page 113.

Example 5-5 Sample scheduler definition for SAP HANA DB weekly backup to IBM Spectrum Protect

```
Protect: AIX-AW>q sched HANA_DOM HANA_WEEKLY_FULL f=d

            Policy Domain Name: HANA_DOM
                 Schedule Name: HANA_WEEKLY_FULL
                   Description: HANA Weekly Full Backup to IBM Spectrum
Protect
                        Action: Command
                     Subaction:
                       Options:
                       Objects: /tsm/scripts/HANA_full_bkp.sh
                      Priority: 5
               Start Date/Time: 11/14/20   20:00:00
                      Duration: 1 Hour
    Maximum Run Time (Minutes): 0
                Schedule Style: Classic
                        Period: 1 Week
                   Day of Week: Sunday
                         Month:
                  Day of Month:
                 Week of Month:
                    Expiration:
Last Update by (administrator): ADMIN
         Last Update Date/Time: 11/14/20   00:40:44
              Managing profile:
```

- IBM Spectrum Copy Data Management configuration

  An IBM Spectrum Copy Data Management backup job is scheduled for an automatic run, and it is associated with an SLA policy by using a daily frequency for running the backup job and maintaining seven snapshots on the storage device, as shown in Figure 5-12.



Name: SAP_HANA_FULLFlash_DAILY
Type: IBM Spectrum Virtualize
Description: SAP HANA daily snapshot backup

Recovery Point Objective:

Frequency	DAILY
Interval	1

HANAFlashCopy1:

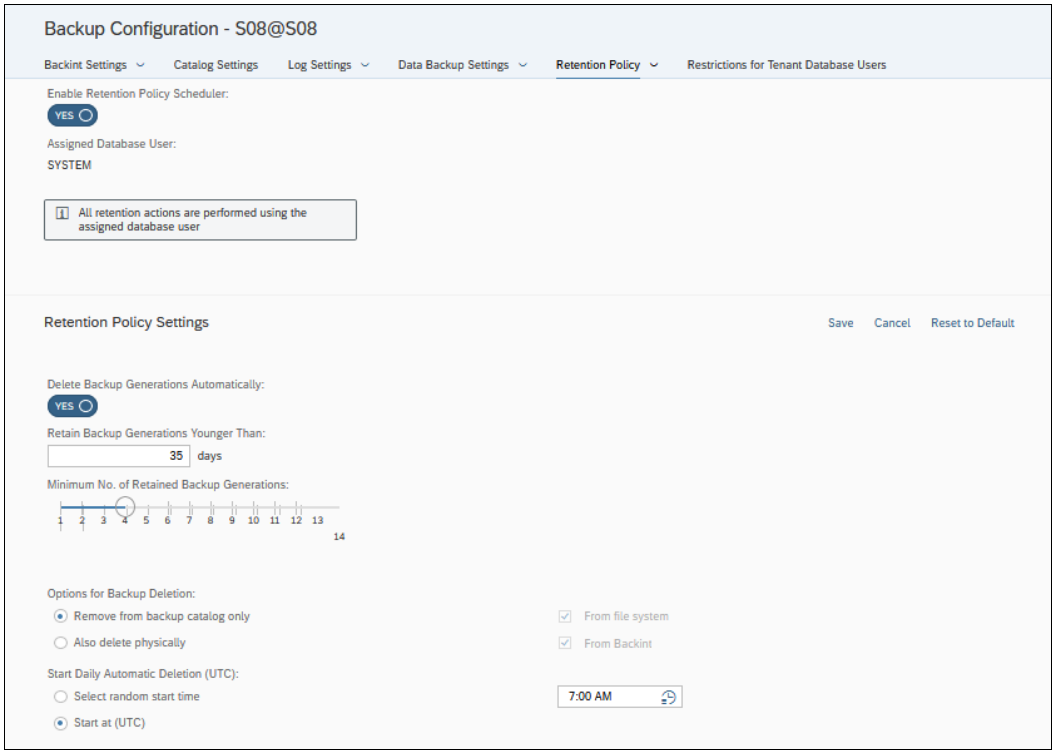
Type	SNAPSHOT
Subtype	IBMSVC
Name	HANAFlashCopy1
Description	FlashCopy0
Primary Source	yes
Number of snapshot instances to keep	7
FlashCopy Volume Prefix	HANA_DAILY_FC
Enable Incremental FlashCopy	no
Destination	Target FlashCopy Storage Pool: Use Original

Figure 5-12 IBM Spectrum Copy Data Management SLA policy definition

  Additionally, the backup job is set for not backing up the logs. The parameters `basepath_catalogbackup` and `basepath_logbackup` must not be set in the SAP HANA `global.ini` configuration file because the log backup is covered by the IBM Spectrum Protect Backint agent configuration.

- SAP HANA backup configuration

  The retention settings are also configured on SAP HANA Cockpit in the **Backup Configuration** menu of the selected database. They cover only the backup catalog entries' retention in correlation with the policies that are established for snapshot and data backups, as shown in Figure 5-13.



Enable Retention Policy Scheduler: YES

Assigned Database User: SYSTEM

All retention actions are performed using the assigned database user

Retention Policy Settings

Delete Backup Generations Automatically: YES

Retain Backup Generations Younger Than: 35 days

Minimum No. of Retained Backup Generations: 4

Options for Backup Deletion:
● Remove from backup catalog only
○ Also delete physically
☑ From file system
☑ From Backint

Start Daily Automatic Deletion (UTC):
○ Select random start time
● Start at (UTC) 7:00 AM

Figure 5-13 SAP HANA retention policy inline with the required backup policy

The following aspects are common to the retention aspects among the components:

- A minimum of four generations are maintained on the SAP HANA backup configuration, which correlate with weekly full backups that are performed to IBM Spectrum Protect.
- There are up to 35 days of generation entries in the backup catalog for covering the one month interval.
- Only SAP HANA backup catalog entries are deleted upon expiration of the backups in SAP HANA. The maximum retention of 35 days covers both data backups and data snapshots.
- The data backups on IBM Spectrum Protect server are expired by the IBM Spectrum Protect Backint agent by using parameter `MAX_VERSIONS=4`. An extra weekly full backup in addition to one month (4 weeks) triggers the expiration of the oldest backup generation data on the IBM Spectrum Protect server.
- The snapshot backups are maintained as seven versions (1 week) for storage capacity efficiency and managed by the IBM Spectrum Copy Data Management SLA policy. However, the entries in the SAP HANA backup catalog are managed by SAP HANA and kept for 35 days.

5.3 Restoring and recovering an SAP HANA database

This section presents various scenarios and practical examples for SAP HANA recovery and for using SAP HANA tools for backup verification when using the Backint agent and IBM Spectrum Protect.

5.3.1 Verifying an SAP HANA database backup

There are several tools that can be used for verifying the backups before the restoration. This section shows how to use them with the Backint type of backup in an IBM Spectrum Protect environment.

The hdbbackupdiag tool

The **`hdbbackupdiag`** tool determines which backups are required to complete a recovery to a specified point in time (PiT). It also checks whether these backups are available and can be accessed. It can be used for file and Backint types of backups.

Example 5-6 shows how to use the tool with the Backint parameters for the latest backup version that is available of tenant database S08.

Example 5-6 Using the hdbbackupdiag tool to check the latest available backup by using Backint

```
s08adm@stu-08:/usr/sap/S08/HDB00> hdbbackupdiag --check --useBackintForCatalog --databaseName
S08 --backintDataParamFile /hana/shared/S08/global/hdb/opt/hdbconfig/initS08.utl
--backintLogParamFile /hana/shared/S08/global/hdb/opt/hdbconfig/initS08_log.utl
--backintCatalogParamFile /hana/shared/S08/global/hdb/opt/hdbconfig/initS08_log.utl

found backup catalog 1602929598679 from backint
/usr/sap/S08/SYS/global/hdb/backint/DB_S08/diagVcsTVK/log_backup_0_0_0_0
using backup catalog 1602929598679 from backint
/usr/sap/S08/SYS/global/hdb/backint/DB_S08/diagVcsTVK/log_backup_0_0_0_0
Backup '/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databackup_0_1' ebid
'S08___A0KGDIVI1Y' successfully checked.
```

```
Backup '/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databackup_2_1' ebid
'S08___AOKGDIVI1Y' successfully checked.
Backup '/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databackup_3_1' ebid
'S08___AOKGDIVI1Y' successfully checked.
s08adm@stu-08:/usr/sap/S08/HDB00>
```

Example 5-6 on page 87 shows that different parameter files can be used for data, log, and catalog backups. In our case, they point to the `utl` configuration files of the IBM Spectrum Protect Data Protection for SAP HANA agent.

> **Note:** There is also a PiT option that is available for checking your PiT for recovery:
>
> `-u "YYYY-MM-DD hh:mm:ss"`

For backups containing large incrementals, differentials, and log backups, the output can also be large, so the output must be saved on file for further reference.

For more information about **`hdbbackupdiag`**, see Check the Backups Required for a Recovery (hdbbackupdiag).

The hdbbackupcheck tool

The **`hdbbackupcheck`** tool can be used to check the integrity of individual data backups and log backups for file-based SAP HANA databases. It can also be used for checking the backups with Backint by using the parameter '`--backintParamFile`' and providing the following information for the command-line processing:

- Backup storage location. In the case of Backint, the location starts with `"/usr/sap/<SID>/SYS/global/hdb/backint/"`.
- External backup ID (ebid).
- Optionally, the backup ID that was assigned to the backup by the SAP HANA database when it was created.

Such information can be determined from the **`hdbbackupdiag`** output or from journaled activities for the data and log backups from the `backint.log` file.

Example 5-7 performs a check on a backup file from the Backint backup:

`FULL_BACKUP_S08_TEST_databackup_3_1`

It uses option **`-v`** to get a detailed description of the contents of the backup file.

Example 5-7 Checking a Backint file by using the hdbbackupcheck tool

```
s08adm@stu-08:/usr/sap/S08/HDB00> hdbbackupcheck -v --backintParamFile
/hana/shared/S08/global/hdb/opt/hdbconfig/initS08.utl
/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databackup_3_1 -e
'S08___AOKGBFQNEA'
Check backup
'/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databackup_3_1'.
Destination of Type: backint, Version: 10
Destination header information:
        DatabaseId: a1c3d656-5343-264a-a850-c5263c6040ae
        InternalStartTime: 1602803363762 / 2020-10-16T01:09:23+02:00
        CurrDestInformation:
[BACKINT][/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databack
up_3_1]
```

```
        backupId: 1602803363761
        ServiceName: indexserver
        NumberOfVolumes: 2
        HostName: stu-08
        VolumeId: 3
        DestId: 1
        NumberOfDest: 1
        SID: S08
        DatabaseName: S08
        HanaVersion: 2.00.046.00.1581325702
        HanaWeekstone: 0000.00.0
        Architecture: little endian
        WorkerGroups: default
        SrcPoolInformation[0]: [DATABASE_SNAPSHOT]@node[3] BackupId: 1602803363761
        DstPoolInformation[0]:
[BACKINT][/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databack
up_3_1]
    Source header information:
        SrcType: 1
        SourceInformation: [DATABASE_SNAPSHOT]@node[3]
        srcVersion: 6
        sourceSize: 2080378880
        encryption: NOT ENCRYPTED
  Check backup content '[DATABASE_SNAPSHOT]@node[3]'.
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
  Backup content '[DATABASE_SNAPSHOT]@node[3]' successfully checked.
Backup
'/usr/sap/S08/SYS/global/hdb/backint/DB_S08/FULL_BACKUP_S08_TEST_databackup_3_1'
successfully checked.
```

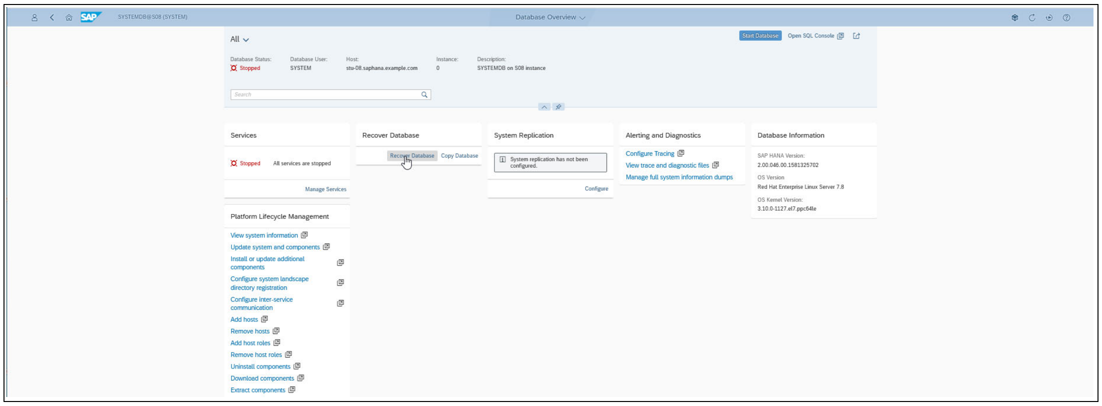
For more information about the **hdbbackupcheck** tool, see Checking Individual Backups (hdbbackupcheck).

5.3.2 Recovering the SAP HANA database by using IBM Spectrum Protect

This section describes the operations that are performed for recovery of the SAP HANA database in a multitenant (Multitenant Database Container (MDC)) environment where backup was performed by using the IBM Spectrum Protect Data Protection for SAP HANA Backint agent. Review the backup operation in 5.2.1, “Backing up an SAP HANA database with IBM Spectrum Protect” on page 76. The target recovery database in our lab environment is the tenant database S08. To recover the tenant database, the system database (SYSTEMDB) must be first restored and then all applicable tenant databases are restored. The recovery process for both system and tenant databases is performed by using the SAP HANA Cockpit interface, which is deployed in a distinct database environment on the same host stu-08, as described in 5.1, “The backup environment” on page 74.

Recovering the system database

To recover the system database, we use SAP HANA Cockpit. In the database directory context, select the SYSTEMDB@S08 database and Recover Database workspace (see Figure 5-14). Ensure that the database is stopped. If it is running, run **`HDB stop`** as `<sid>adm` to stop the system and tenant database environment before starting the recovery operations.



Database Status: Stopped
Database User: SYSTEM
Host: stu-08.saphana.example.com
Instance: 0
Description: SYSTEMDB on S08 instance

Stopped All services are stopped

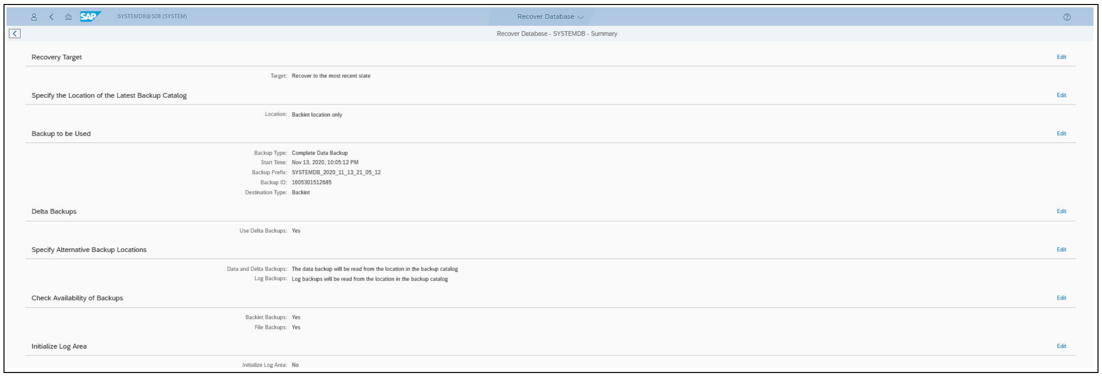
System replication has not been configured.

SAP HANA Version: 2.00.046.00.1581325702
OS Version: Red Hat Enterprise Linux Server 7.8
OS Kernel Version: 3.10.0-1127.el7.ppc64le

Figure 5-14 Starting the recovery wizard of the system database by using SAP HANA Cockpit

The recovery wizard starts and more inputs are provided during the process. During the running of the wizard when using SAP HANA Cockpit, only recovery to *the most recent state* is possible. Although some PiT options are possible when using SAP HANA Studio, SAP recommends using SAP HANA Cockpit to restore the system database, as described in Recover a System Database to a Point in Time.

We recover the system database to the most current state by providing the Backint only location for catalog and backup repository for restoring the database from IBM Spectrum Protect. An overall view of the restore settings is shown in Figure 5-15.



Recover Database - SYSTEMDB - Summary

Recovery Target

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog

Location: Backint location only

Backup to be Used

Backup Type: Complete Data Backup
Start Time: Nov 13, 2020, 10:05:12 PM
Backup Prefix: SYSTEMDB_2020_11_13_21_05_12
Backup ID: 1605301512685
Destination Type: Backint

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Log backups will be read from the location in the backup catalog

Check Availability of Backups

Backint Backups: Yes
File Backups: Yes

Initialize Log Area

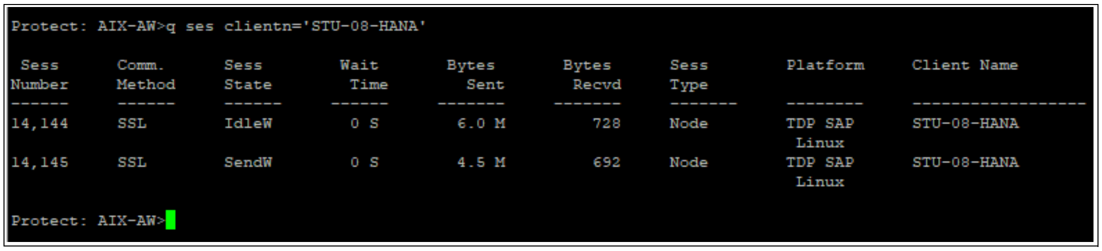
Initialize Log Area: No

Figure 5-15 Recovery options for the system database restore from IBM Spectrum Protect

The following SQL statement is used for the database recovery:

```
RECOVER DATABASE UNTIL TIMESTAMP '2021-11-15\ 01:32:42' USING CATALOG BACKINT
USING BACKUP_ID 1605301512685 CHECK ACCESS ALL
```

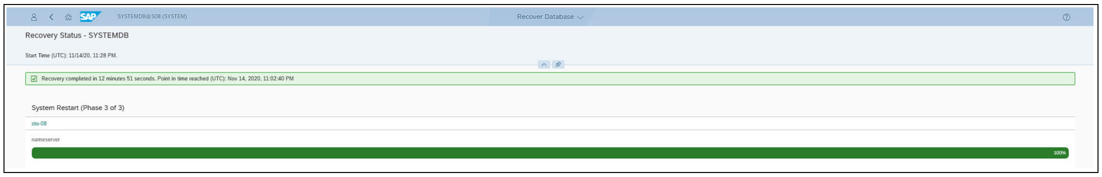
Monitor the transfer sessions between the IBM Spectrum Protect server and the SAP HANA server by using an administrative client (`dsmadmc`) as shown in Figure 5-16 on page 91.



```
Protect: AIX-AW>q ses clientn='STU-08-HANA'

 Sess     Comm.      Sess       Wait      Bytes       Bytes     Sess        Platform     Client Name
Number    Method     State      Time       Sent       Recvd     Type
------    ------     ------    ------    --------    --------   -------     --------     ------------------
14,144    SSL        IdleW       0 S       6.0 M         728    Node        TDP SAP      STU-08-HANA
                                                                             Linux
14,145    SSL        SendW       0 S       4.5 M         692    Node        TDP SAP      STU-08-HANA
                                                                             Linux

Protect: AIX-AW>
```

Figure 5-16 Restore sessions that are established between the SAP HANA and IBM Spectrum Protect servers

The final restore result is shown in Figure 5-17.



Recovery Status - SYSTEMDB

Start Time (UTC): 11/14/20, 11:28 PM.

☑ Recovery completed in 12 minutes 51 seconds. Point in time reached (UTC): Nov 14, 2020, 11:02:40 PM

System Restart (Phase 3 of 3)

stu-08

nameserver 100%

Figure 5-17 System database recovery complete

You can verify that the system database is started by using the `hdbsql` client, as shown in Example 5-8.

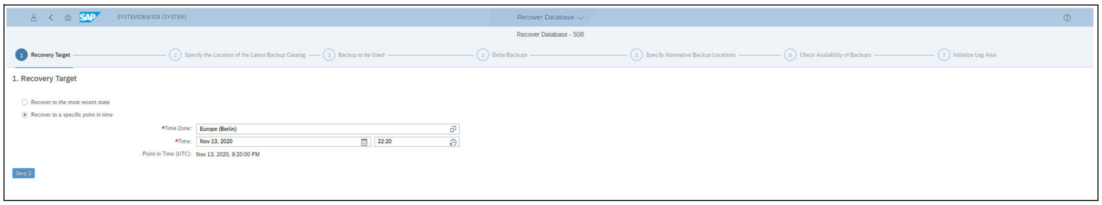
Example 5-8 Checking the system database status by using native SQL statement

```
hdbsql SYSTEMDB=> select * from M_DATABASES;
DATABASE_NAME,DESCRIPTION,ACTIVE_STATUS,ACTIVE_STATUS_DETAILS,OS_USER,OS_GROUP,RES
TART_MODE,FALLBACK_SNAPSHOT_CREATE_TIME
"SYSTEMDB","SystemDB-S08-00","YES","","","","DEFAULT",?
"S08","S08-00","NO","","","","DEFAULT",?
Two rows selected (overall time 89.048 msec; server time 385 usec)
```

Recovering the tenant database

After the system database is recovered and started, we can perform the tenant database recovery by using SAP HANA Cockpit. From the Database Directory, select **Database Management**, select the S08 line, and in the **Tenant Actions** drop-down menu, select **Recover Tenant**. A wizard starts for the tenant database recovery, where we provide input that is similar for a recovery of the system database. In this case, we can choose the option for PiT recovery where a specific PiT can be selected, or we can recover to the most recent state based on the existing complete, incremental, differential, and log backups that are available.

When we select a specific PiT from the latest complete (full) backup available, we are prompted to provide a time zone reference, which is Europe (Berlin) in our case, and the date and time for recovery, as shown in Figure 5-18.



1. Recovery Target

○ Recover to the most recent state

● Recover to a specific point in time

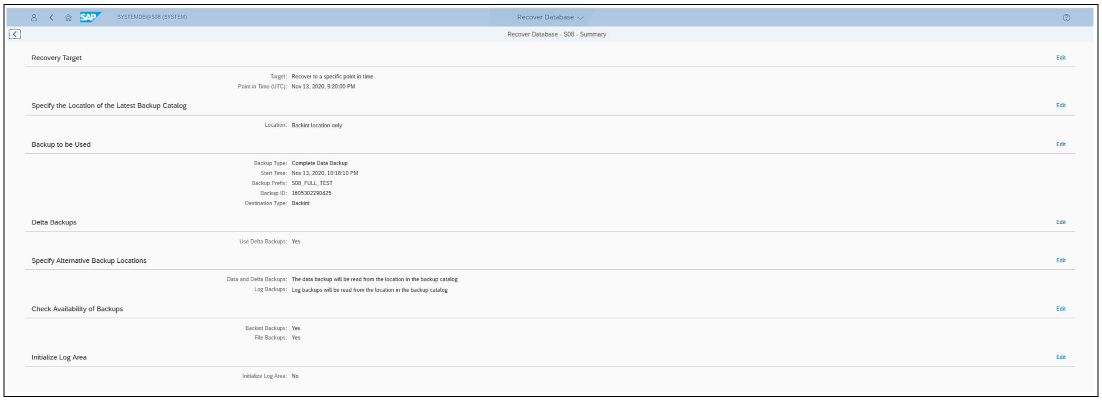
*Time Zone: Europe (Berlin)

*Time: Nov 13, 2020 22:20

Point in Time (UTC): Nov 13, 2020, 9:20:00 PM

Figure 5-18 Selecting the restore PiT

Follow the wizard and provide the appropriate inputs. Review the settings before you start the restore operation, as shown in Figure 5-19.



Recovery Target

Target: Recover to a specific point in time
Point in Time (UTC): Nov 13, 2020, 9:20:00 PM

Specify the Location of the Latest Backup Catalog

Location: Backint location only

Backup to be Used

Backup Type: Complete Data Backup
Start Time: Nov 13, 2020, 10:18:10 PM
Backup Prefix: S08_FULL_TEST
Backup ID: 1605302290425
Destination Type: Backint

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Log backups will be read from the location in the backup catalog

Check Availability of Backups

Backint Backups: Yes
File Backups: Yes

Initialize Log Area

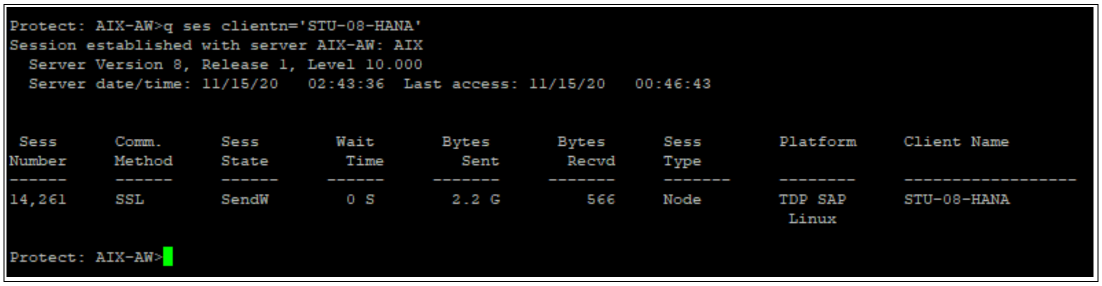
Initialize Log Area: No

Figure 5-19 Recovery summary options for the tenant database S08

Here is the SQL statement for the database recovery:

```
RECOVER DATABASE FOR S08 UNTIL TIMESTAMP '2020-11-13 21:20:00' USING CATALOG
BACKINT USING BACKUP_ID 1605302290425 CHECK ACCESS ALL
```

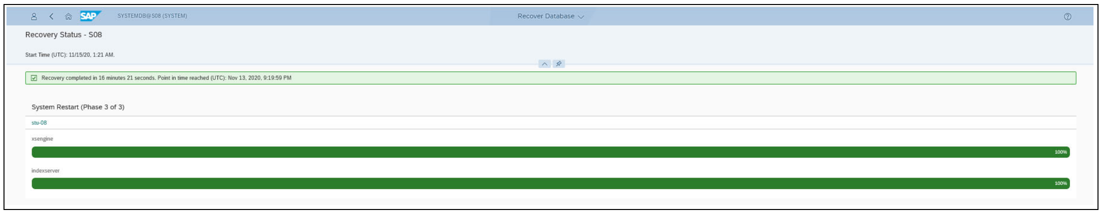
The recovery process starts. The data transfer sessions can be monitored on the IBM Spectrum Protect server, as shown in Figure 5-20.



```
Protect: AIX-AW>q ses clientn='STU-08-HANA'
Session established with server AIX-AW: AIX
  Server Version 8, Release 1, Level 10.000
  Server date/time: 11/15/20   02:43:36  Last access: 11/15/20   00:46:43


 Sess      Comm.      Sess        Wait       Bytes       Bytes      Sess        Platform     Client Name
Number     Method     State       Time        Sent       Recvd      Type
------     ------     ------     ------     --------    --------    -------     --------     ------------------
14,261     SSL        SendW        0 S        2.2 G        566      Node        TDP SAP      STU-08-HANA
                                                                                 Linux

Protect: AIX-AW>
```

Figure 5-20 IBM Spectrum Protect restore sessions during S08 database recovery

The final result is shown in Figure 5-21.



Recovery Status - S08

Start Time (UTC): 11/15/20, 1:21 AM.

☑ Recovery completed in 16 minutes 21 seconds. Point in time reached (UTC): Nov 13, 2020, 9:19:59 PM

System Restart (Phase 3 of 3)

stu-08

xsengine

indexserver

Figure 5-21 Complete restore of the S08 tenant database

You can check the database status by using SAP HANA Cockpit or by using the `hdbsql` SQL client, as shown in Example 5-9 on page 93.

Example 5-9 Checking the S08 database status by using a native SQL statement

```
hdbsql SYSTEMDB=> select * from M_DATABASES;
DATABASE_NAME,DESCRIPTION,ACTIVE_STATUS,ACTIVE_STATUS_DETAILS,OS_USER,OS_GROUP,RES
TART_MODE,FALLBACK_SNAPSHOT_CREATE_TIME
"SYSTEMDB","SystemDB-S08-00","YES","","","","DEFAULT",?
"S08","S08-00","YES","","","","DEFAULT",?
Two rows selected (overall time 59.547 msec; server time 330 usec)
```

5.3.3 Recovering an SAP HANA database from IBM Spectrum Protect without a backup catalog

In cases where a backup is not in the catalog but it is available for restore on the back-end device (file or Backint), the SAP HANA administrator can recover the database without the backup catalog.

Such cases can also be applied when performing specific reference full backups, for example, before applying a major change on the current system or for restoring to another system for test and cloning purposes. You must correctly tag such a backup so that it can be identified during the restore process by using the prefix. In this case, you need to specify the following items:

- The backup type (file or Backint).
- The location of the backup folder for file backup, or in the case of Backint, the path that starts with `'/usr/sap/<SID>/SYS/global/hdb/backint/'`.
- The backup prefix, which is a key parameter for correct identification of the backup files on the back-end device.

For our test case, we use a complete data backup that is generated with the prefix `‘S08_TEST_FULL_15NOV2020’` that was deleted from the catalog only, so no reference exists for this prefix in the current catalog (see Example 5-10, where we reuse the query from Example 5-3 on page 78).

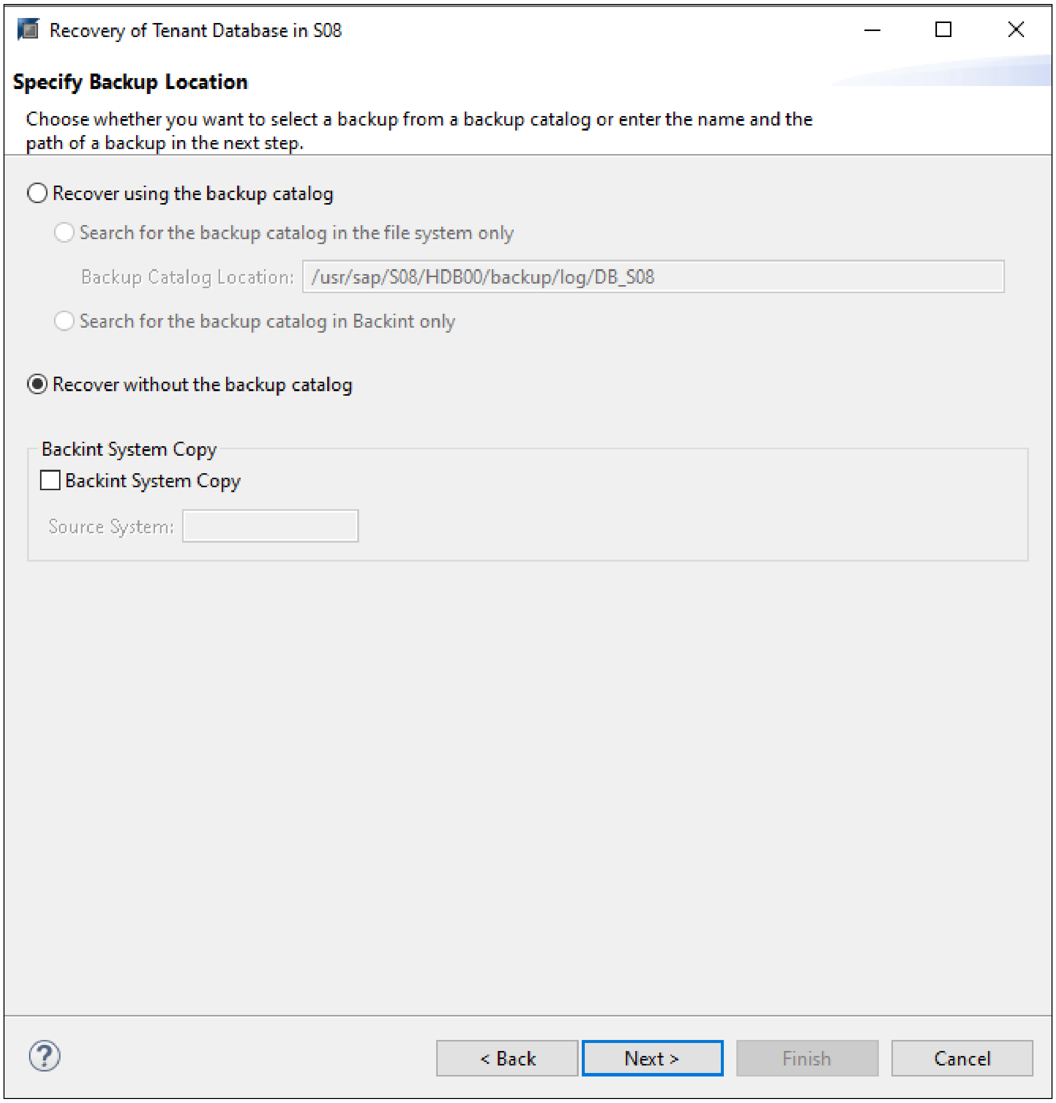
Example 5-10 Searching the backup catalog for a prefix

```
#Initial state after the full backup:
hdbsql S08=> SELECT A.BACKUP_ID, A.ENTRY_TYPE_NAME,
A.SYS_START_TIME,A.SYS_END_TIME,B.BACKUP_SIZE,B.DESTINATION_PATH,B.DESTINATION_TYP
E_NAME,B.EXTERNAL_BACKUP_ID FROM M_BACKUP_CATALOG A, M_BACKUP_CATALOG_FILES B
WHERE A.BACKUP_ID=B.BACKUP_ID and A.STATE_NAME = 'successful' AND
A.ENTRY_TYPE_NAME = 'complete data backup' and B.DESTINATION_PATH like
'%S08_TEST_FULL_15NOV2020%' ORDER BY A.UTC_START_TIME desc;

BACKUP_ID,ENTRY_TYPE_NAME,SYS_START_TIME,SYS_END_TIME,BACKUP_SIZE,DESTINATION_PATH
,DESTINATION_TYPE_NAME,EXTERNAL_BACKUP_ID
1605451342307,"complete data backup","2020-11-15 15:42:22.309000000","2020-11-15
15:47:55.936000000",83886080,"/usr/sap/S08/SYS/global/hdb/backint/DB_S08/S08_TEST_
FULL_15NOV2020_databackup_2_1","backint","S08___A0KHJ8A12Z"
1605451342307,"complete data backup","2020-11-15 15:42:22.309000000","2020-11-15
15:47:55.936000000",2634022912,"/usr/sap/S08/SYS/global/hdb/backint/DB_S08/S08_TES
T_FULL_15NOV2020_databackup_3_1","backint","S08___A0KHJ8A12Z"
1605451342307,"complete data backup","2020-11-15 15:42:22.309000000","2020-11-15
15:47:55.936000000",1614,"/usr/sap/S08/SYS/global/hdb/backint/DB_S08/S08_TEST_FULL
_15NOV2020_databackup_0_1","backint","S08___A0KHJ8A12Z"
3 rows selected (overall time 312.541 msec; server time 92.190 msec)
```

```
#After the backup has been deleted from catalog only:
hdbsql S08=> SELECT A.BACKUP_ID, A.ENTRY_TYPE_NAME,
A.SYS_START_TIME,A.SYS_END_TIME,B.BACKUP_SIZE,B.DESTINATION_PATH,B.DESTINATION_TYP
E_NAME,B.EXTERNAL_BACKUP_ID FROM M_BACKUP_CATALOG A, M_BACKUP_CATALOG_FILES B
WHERE A.BACKUP_ID=B.BACKUP_ID and A.STATE_NAME = 'successful' AND
A.ENTRY_TYPE_NAME = 'complete data backup' and B.DESTINATION_PATH like
'%S08_TEST_FULL_15NOV2020%' ORDER BY A.UTC_START_TIME desc;

BACKUP_ID,ENTRY_TYPE_NAME,SYS_START_TIME,SYS_END_TIME,BACKUP_SIZE,DESTINATION_PATH
,DESTINATION_TYPE_NAME,EXTERNAL_BACKUP_ID
0 rows selected (overall time 255.738 msec; server time 91.644 msec)
```

For the recovery of a specific backup, we use SAP HANA Studio and access the task menu **Recover Tenant Database from the System Database**. A recovery wizard starts where you complete the following steps:

1. Select S08 SAP HANA database for recovery.
2. In the next window, select **Recover the database to a specific data backup**.
3. In the next window, select **Recover without the backup catalog** (see Figure 5-22 on page 95).



Recovery of Tenant Database in S08

Specify Backup Location

Choose whether you want to select a backup from a backup catalog or enter the name and the path of a backup in the next step.

○ Recover using the backup catalog

○ Search for the backup catalog in the file system only

Backup Catalog Location: /usr/sap/S08/HDB00/backup/log/DB_S08

○ Search for the backup catalog in Backint only

● Recover without the backup catalog

Backint System Copy

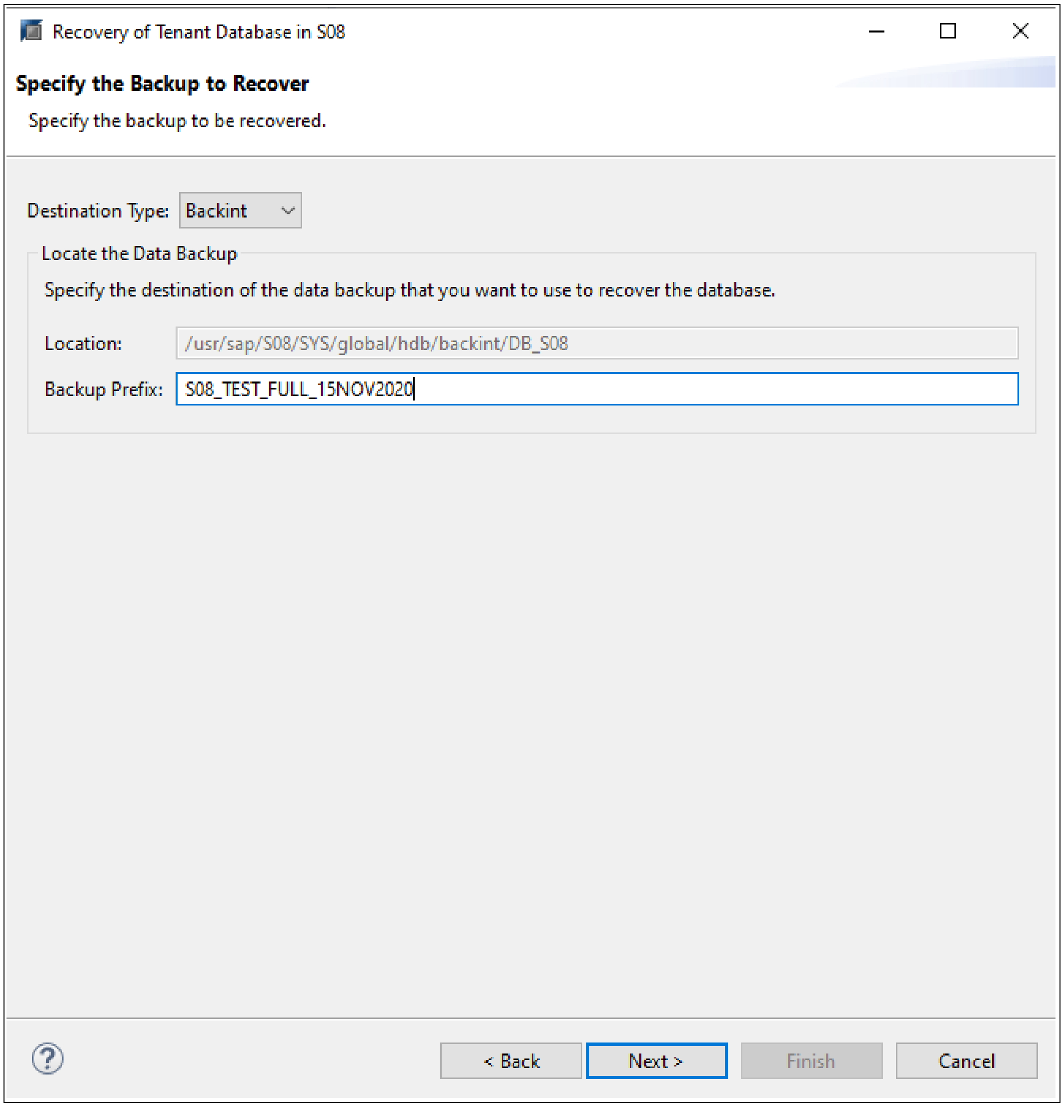
□ Backint System Copy

Source System:

Figure 5-22 Specifying that the backup recovery is performed without the catalog

Note: At this step, there is also an option to provide a source SAP HANA database that can be used for cloning a database to another SAP HANA system (a different system ID (SID)) that is based on Backint and uses a complete (full) database backup). The syntax for a multitenant environment is `<Database>@<SID>`, for example `S08@S08`.

4. Specify the destination type as `backint` and provide the prefix to be used for searching the backup on the back-end device (Figure 5-23).



Specify the Backup to Recover

Specify the backup to be recovered.

Destination Type: Backint

Locate the Data Backup

Specify the destination of the data backup that you want to use to recover the database.

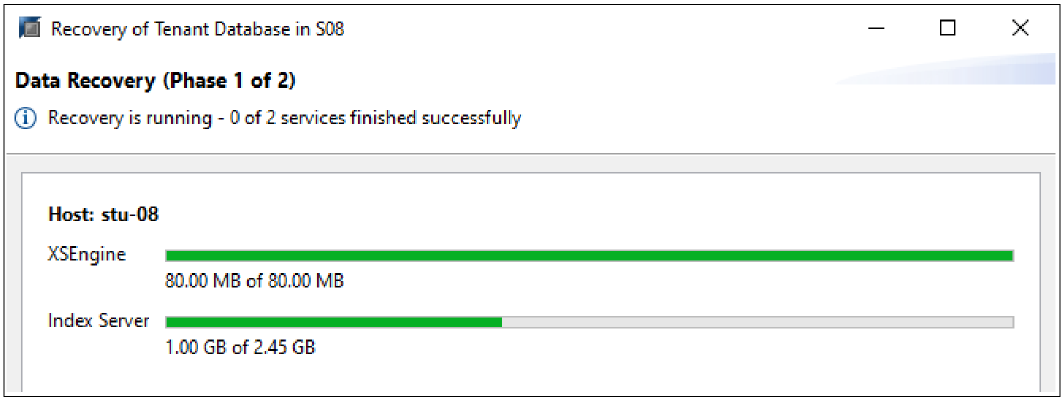
Location: /usr/sap/S08/SYS/global/hdb/backint/DB_S08

Backup Prefix: S08_TEST_FULL_15NOV2020

Figure 5-23 Specifying the destination type and prefix for recovery

> **Note:** If there are multiple backups that are performed under the same prefix, the latest one is selected for restore. There is no option to restore previous versions in this restore scenario, so be sure to use distinct prefix names.

5. There are no more options to be provided. Based on previous selections, the recovery process enforces “Initialize Log Area”, and this type of backup (without catalog) does not allow for applying any delta or log backups.
6. Review the final options and start the recovery process. Wait for the operation to complete. To see the progress of the recovery operation, see Figure 5-24 on page 97.


Recovery of Tenant Database in S08

Data Recovery (Phase 1 of 2)

Recovery is running - 0 of 2 services finished successfully

Host: stu-08

XSEngine 80.00 MB of 80.00 MB

Index Server 1.00 GB of 2.45 GB

Figure 5-24 Recovery of tenant database S08@S08 without backup catalog

For more information about the recovery of a specific data backup, see Recover a Database from a Data Backup (SAP HANA Studio).

A similar restore process can be done by using the database copy wizard in SAP HANA Cockpit by selecting the source and destination of the copy to the same database and not using a backup catalog for restore. The next section details a database copy process where a PiT recovery that is based on the Backint backup catalog is performed by using SAP HANA Cockpit.

5.3.4 Copying an SAP HANA database by using backup and restore with IBM Spectrum Protect

This operation can be applied for cloning a database by using Backint restore from IBM Spectrum Protect to a different SAP HANA system or to a different database on the same system. Our scenario creates a tenant database that is named S08CLONE for target restore within the same S08 SAP HSID with a distinct IBM Spectrum Protect backup profile:

- There are backup options in the database `global.ini` configuration file that is generated from Data Protection for SAP HANA configuration by using the **`setup.sh`** tool with more configuration of log and database backups by using distinct `utl` files (see Example 5-11).

Example 5-11 The global.ini configuration file of the S08CLONE tenant database

```
s08adm@stu-08:/hana/shared/S08/global/hdb/opt/hdbconfig> cat
/hana/shared/S08/global/hdb/custom/config/DB_S08CLONE/global.ini

# global.ini last modified 2020-11-15 20:51:36.846227 by hdbindexserver -port
30040
[backup]
log_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(DBNAME)_log.utl
catalog_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(DBNAME)_log.utl
parallel_data_backup_backint_channels = 4
data_backup_parameter_file =
/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/init$(DBNAME).utl
catalog_backup_using_backint = true
log_backup_using_backint = true
```

- The `utl` files for the database, log, and backup catalog for the new tenant database point to the IBM Spectrum Protect server instance:

```
SERVER         AIX-AW-HANA-CLONE     # Servername, as defined in dsm.sys
SESSIONS              4
  PASSWORDREQUIRED    NO             # Use a password
  BRBACKUPMGTCLASS    DATABASE       # Mgmt-Classes for database backup
  BRARCHIVEMGTCLASS   LOG            # Mgmt-Classes for redo log backup
```

- The system options file `dsm.sys` for the IBM Spectrum Protect application programming interface (API) contains the server stanza that is associated with the server name:

```
SErvername AIX-AW-HANA-CLONE
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   10.0.240.164
   Nodename STU-08-HANA1
   PASSWORDACCESS GENERATE
   ERRORLOGName /tsm/S08CLONE/dsmerror.log
   PASSWORDDIR /tsm/S08CLONE
   SCHEDLOGName /tsm/S08CLONE/dsmsched.log
   SCHEDLOGRetention 30 D
```

The database copy operation from the S08 database backup to the new tenant database S08CLONE is performed by using the SAP HANA Cockpit interface. Before running the restore operation, ensure that the following configuration elements are accomplished:

- The `utl` and `bki` files of the source database exist on the target restore system. In the case of a different SAP HANA system, the files must be copied on to the target restore SAP HANA system. In our environment, the folder of the `utl` file is `/usr/sap/S08/SYS/global/hdb/opt/hdbconfig/`. Example 5-12 shows the content of the folder in our environment.

Example 5-12 The utl and bki files are present on the target restore system

```
s08adm@stu-08:/usr/sap/S08/SYS/global/hdb/opt/hdbconfig> ls -l
total 60
-rw-r--r--. 1 s08adm sapsys    33 Nov 15 20:35 agent.lic
-rw-r-----. 1 s08adm sapsys   347 Nov  5 22:46 initS08.bki
-rw-r-----. 1 s08adm sapsys   353 Nov 15 20:37 initS08CLONE.bki
-rw-r-----. 1 s08adm sapsys 12021 Nov 15 22:00 initS08CLONE_log.utl
-rw-r-----. 1 s08adm sapsys 12020 Nov 15 21:59 initS08CLONE.utl
-rw-r-----. 1 s08adm sapsys 11838 Nov  5 22:45 initS08_log.utl
-rw-r-----. 1 s08adm sapsys 11838 Nov  5 22:52 initS08.utl
```

Example 5-12 shows that there is a single `init<DBNAME>.bki` file for each database, which is pointed at by the `CONFIG_FILE` parameter in both the data and redo log/catalog `utl` profile files.

Note: Ensure that the original `init<SID>.utl` files for data and log backups have the `CONFIG_FILE` parameter pointing the valid path to the `bki` file. If you use another SAP HANA target system with a different SID, update the path.

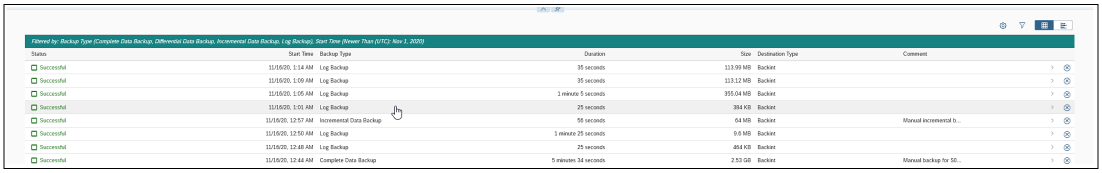
- The IBM Spectrum Protect API system options file `dsm.sys` on the target system contains the server stanzas that are associated with the original S08 database and log/catalog backups. In our environment, the source IBM Spectrum Protect server profile is displayed as follows:

```
SErvername AIX-AW-HANA
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   10.0.240.164
   Nodename STU-08-HANA
   PASSWORDACCESS GENERATE
   ERRORLOGName /tsm/S08/dsmerror.log
   PASSWORDDIR /tsm/S08
   SCHEDLOGName /tsm/S08/dsmsched.log
```

- The access to the IBM Spectrum Protect server by using the source database S08 backup profile can be done on the target system without providing a password interactively. This password is stored in the `initSID.bki` file and in the IBM Spectrum Protect API folder, which in our case is pointed to the `PASSWORDIR` parameter in the system options file (`dsm.sys`). If an update is required, use the following command:

```
hdbbackint -p <initSID.utl> -f password
```

The backup catalog entries for the source database S08 at the time of the copy operation are displayed in Figure 5-25. We set our PiT objective to 16-Nov, 01:02 AM CET.

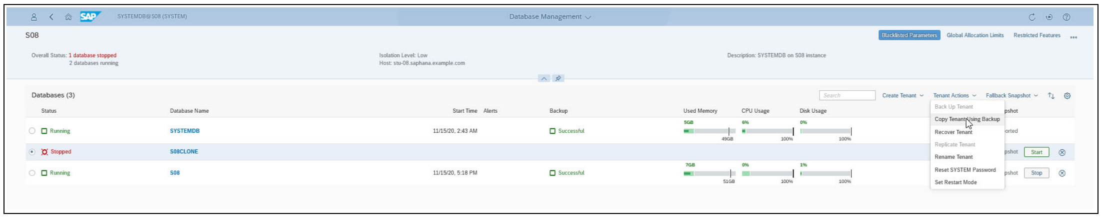


Filtered by: Backup Type (Complete Data Backup, Differential Data Backup, Incremental Data Backup, Log Backup), Start Time (Newer Than (UTC): Nov 1, 2020)

Status	Start Time	Backup Type	Duration	Size	Destination Type	Comment
☐ Successful	11/16/20, 1:14 AM	Log Backup	35 seconds	113.99 MB	Backint	
☐ Successful	11/16/20, 1:09 AM	Log Backup	35 seconds	113.12 MB	Backint	
☐ Successful	11/16/20, 1:05 AM	Log Backup	1 minute 5 seconds	355.04 MB	Backint	
☐ Successful	11/16/20, 1:01 AM	Log Backup	25 seconds	384 KB	Backint	
☐ Successful	11/16/20, 12:57 AM	Incremental Data Backup	56 seconds	64 MB	Backint	Manual incremental b...
☐ Successful	11/16/20, 12:50 AM	Log Backup	1 minute 25 seconds	9.6 MB	Backint	
☐ Successful	11/16/20, 12:48 AM	Log Backup	25 seconds	464 KB	Backint	
☐ Successful	11/16/20, 12:44 AM	Complete Data Backup	5 minutes 34 seconds	2.53 GB	Backint	Manual backup for S0...

Figure 5-25 Available backup entries on the S08 backup catalog

The database S08CLONE stopped before the database copy operation ran. Using SAP HANA Cockpit, start the copy process from the **Database Management** window of the system database by selecting the target restore database S08CLONE and then selecting **Tenant Actions** → **Copy Tenant Using Backup**, as shown in Figure 5-26.



S08

Overall Status: 1 database stopped
2 databases running

Isolation Level: Low
Host: stu-08.saphana.example.com

Description: SYSTEMDB on S08 instance

Databases (3)

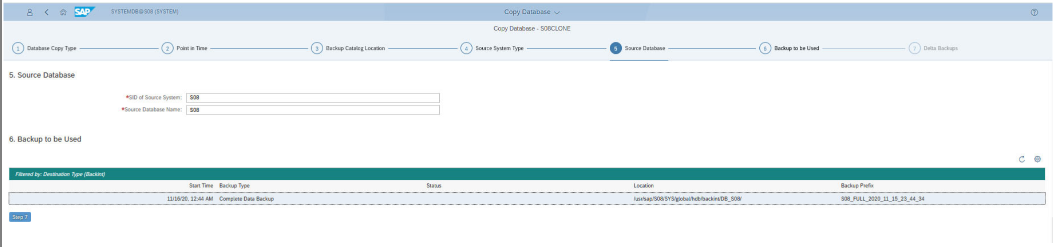
	Status	Database Name	Start Time	Alerts	Backup	Used Memory	CPU Usage	Disk Usage
○	☐ Running	SYSTEMDB	11/15/20, 2:43 AM		☐ Successful	5GB 49GB	6% 100%	0% 100%
●	Stopped	S08CLONE						
○	☐ Running	S08	11/15/20, 5:18 PM		☐ Successful	7GB 51GB	0% 100%	1% 100%

Figure 5-26 Starting the operation: Copy Tenant Using Backup

The copy database wizard starts. For our environment, we select the following options:

1. For database copy type: Data and logs backups for copying a PiT of the database.
2. PiT options: Specify the time zone and the date and time for restore. In our test case, we use CET for time zone and 16 Nov 01:02 AM for the Time.
3. Backup catalog location: Backint.
4. Source system type: Multi container.

5. Source database:
   - SID of source system: S08.
   - Source database name: S08.
6. Now, the backups of the source database S08 are accessed and displayed for selection. We select the latest available complete data backup to the specified PiT recovery, as shown in Figure 5-27.



5. Source Database

*SID of Source System: S08
*Source Database Name: S08

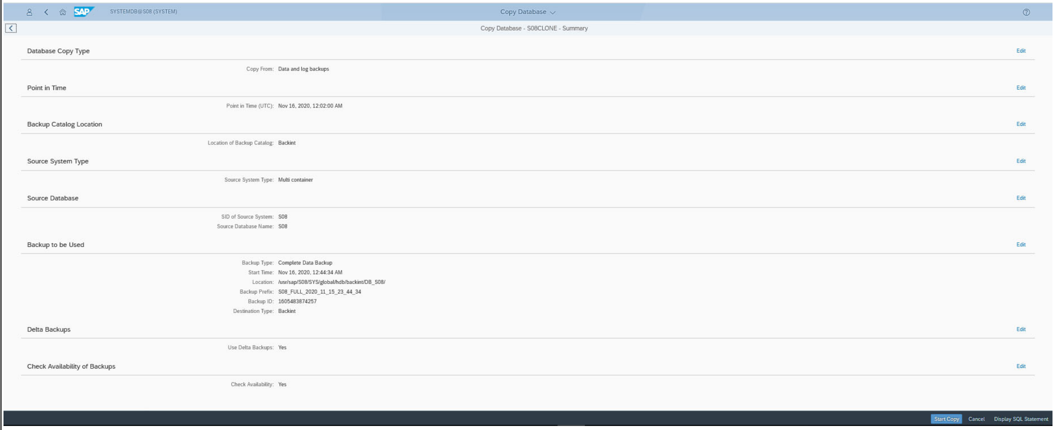
6. Backup to be Used

Filtered by: Destination Type (Backint)

Start Time	Backup Type	Status	Location	Backup Prefix
11/16/20, 12:44 AM	Complete Data Backup		/usr/sap/S08/SYS/global/hdb/backint/DB_S08/	S08_FULL_2020_11_15_23_44_34

Figure 5-27 Selecting the complete data backup reference for restore

7. Specify the use of delta backups: Yes (recommended).
8. Check the availability of the backups at the beginning of the copy operation: Yes.
9. Review the copy wizard option that is provided, as shown in Figure 5-28.



Database Copy Type

Copy From: Data and log backups

Point in Time

Point in Time (UTC): Nov 16, 2020, 12:02:00 AM

Backup Catalog Location

Location of Backup Catalog: Backint

Source System Type

Source System Type: Multi container

Source Database

SID of Source System: S08
Source Database Name: S08

Backup to be Used

Backup Type: Complete Data Backup
Start Time: Nov 16, 2020, 12:44:34 AM
Location: /usr/sap/S08/SYS/global/hdb/backint/DB_S08/
Backup Prefix: S08_FULL_2020_11_15_23_44_34
Backup ID: 1605483874257
Destination Type: Backint

Delta Backups

Use Delta Backups: Yes

Check Availability of Backups

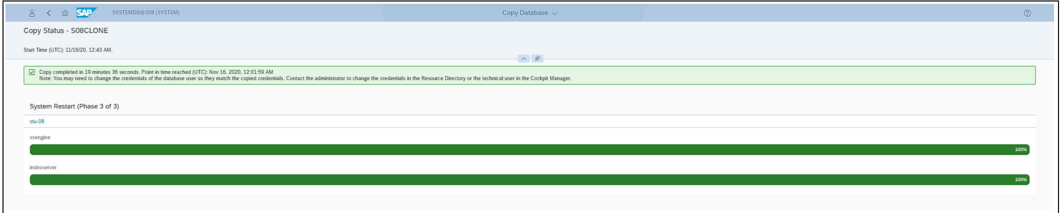
Check Availability: Yes

Figure 5-28 Summary of database copy options

The SQL statement is as follows:

```
RECOVER DATABASE FOR S08CLONE UNTIL TIMESTAMP '2020-11-16 00:02:00' CLEAR LOG
USING SOURCE 'S08@S08' USING CATALOG BACKINT USING BACKUP_ID 1605483874257
CHECK ACCESS ALL
```

10. Start the database copy operation and monitor for completion. The operation processes all require full, differential, and incremental backups and log backups for recovery to the PiT objective. The operation can be also monitored in the `backup.log` and `backint.log` files for the target tenant database S08CLONE. The results are shown in Figure 5-29.



Copy Status - S08CLONE

Start Time (UTC): 11/16/20, 12:43 AM.

☑ Copy completed in 19 minutes 36 seconds. Point in time reached (UTC): Nov 16, 2020, 12:01:59 AM
Note: You may need to change the credentials of the database user so they match the copied credentials. Contact the administrator to change the credentials in the Resource Directory or the technical user in the Cockpit Manager.

System Restart (Phase 3 of 3)

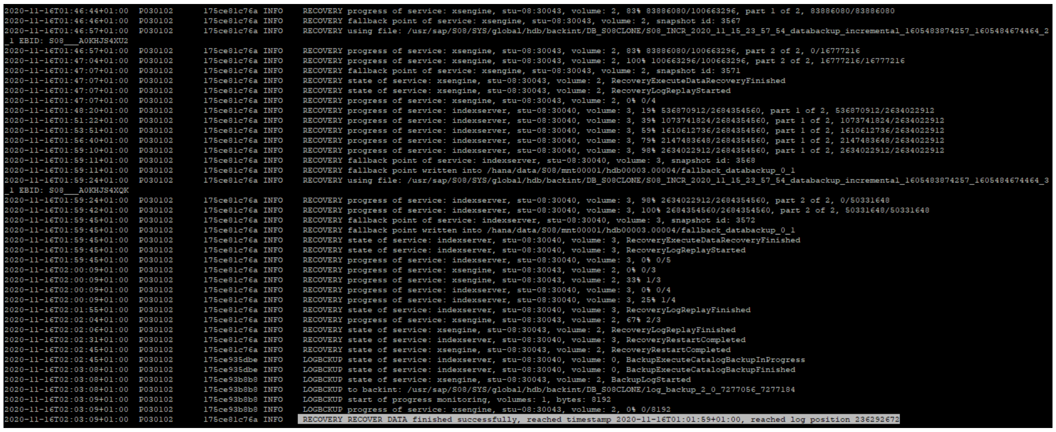
stu-08

xsengine 100%

indexserver 100%

Figure 5-29 Copy operation completed

A snapshot of the restore activity from the `backup.log` file is shown in Figure 5-30.



```
2020-11-16T01:46:44+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 83% 83886080/100663296, part 1 of 2, 83886080/83886080
2020-11-16T01:46:46+01:00  P030102      175ce81c76a INFO    RECOVERY fallback point of service: xsengine, stu-08:30043, volume: 2, snapshot id: 3567
2020-11-16T01:46:57+01:00  P030102      175ce81c76a INFO    RECOVERY using file: /usr/sap/S08/SYS/global/hdb/backint/DB_S08CLONE/S08_INCR_2020_11_15_23_57_54_databackup_incremental_1605483874257_1605484674464_2
_1 EBID: S08___A0KHJS4XU2
2020-11-16T01:46:57+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 83% 83886080/100663296, part 2 of 2, 0/16777216
2020-11-16T01:47:04+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 100% 100663296/100663296, part 2 of 2, 16777216/16777216
2020-11-16T01:47:07+01:00  P030102      175ce81c76a INFO    RECOVERY fallback point of service: xsengine, stu-08:30043, volume: 2, snapshot id: 3571
2020-11-16T01:47:07+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: xsengine, stu-08:30043, volume: 2, RecoveryExecuteDataRecoveryFinished
2020-11-16T01:47:07+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: xsengine, stu-08:30043, volume: 2, RecoveryLogReplayStarted
2020-11-16T01:47:07+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 0% 0/4
2020-11-16T01:48:20+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 19% 536870912/2684354560, part 1 of 2, 536870912/2634022912
2020-11-16T01:51:22+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 39% 1073741824/2684354560, part 1 of 2, 1073741824/2634022912
2020-11-16T01:53:51+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 59% 1610612736/2684354560, part 1 of 2, 1610612736/2634022912
2020-11-16T01:56:40+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 79% 2147483648/2684354560, part 1 of 2, 2147483648/2634022912
2020-11-16T01:59:10+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 98% 2634022912/2684354560, part 1 of 2, 2634022912/2634022912
2020-11-16T01:59:11+01:00  P030102      175ce81c76a INFO    RECOVERY fallback point of service: indexserver, stu-08:30040, volume: 3, snapshot id: 3568
2020-11-16T01:59:11+01:00  P030102      175ce81c76a INFO    RECOVERY fallback point written into /hana/data/S08/mnt00001/hdb00003.00004/fallback_databackup_0_1
2020-11-16T01:59:24+01:00  P030102      175ce81c76a INFO    RECOVERY using file: /usr/sap/S08/SYS/global/hdb/backint/DB_S08CLONE/S08_INCR_2020_11_15_23_57_54_databackup_incremental_1605483874257_1605484674464_3
_1 EBID: S08___A0KHJS4XQK
2020-11-16T01:59:24+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 98% 2634022912/2684354560, part 2 of 2, 0/50331648
2020-11-16T01:59:42+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 100% 2684354560/2684354560, part 2 of 2, 50331648/50331648
2020-11-16T01:59:45+01:00  P030102      175ce81c76a INFO    RECOVERY fallback point of service: indexserver, stu-08:30040, volume: 3, snapshot id: 3572
2020-11-16T01:59:45+01:00  P030102      175ce81c76a INFO    RECOVERY fallback point written into /hana/data/S08/mnt00001/hdb00003.00004/fallback_databackup_0_1
2020-11-16T01:59:45+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: indexserver, stu-08:30040, volume: 3, RecoveryExecuteDataRecoveryFinished
2020-11-16T01:59:45+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: indexserver, stu-08:30040, volume: 3, RecoveryLogReplayStarted
2020-11-16T01:59:45+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 0% 0/5
2020-11-16T02:00:09+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 0% 0/3
2020-11-16T02:00:09+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 33% 1/3
2020-11-16T02:00:09+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 0% 0/4
2020-11-16T02:00:09+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: indexserver, stu-08:30040, volume: 3, 25% 1/4
2020-11-16T02:01:55+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: indexserver, stu-08:30040, volume: 3, RecoveryLogReplayFinished
2020-11-16T02:02:04+01:00  P030102      175ce81c76a INFO    RECOVERY progress of service: xsengine, stu-08:30043, volume: 2, 67% 2/3
2020-11-16T02:02:06+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: xsengine, stu-08:30043, volume: 2, RecoveryLogReplayFinished
2020-11-16T02:02:31+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: indexserver, stu-08:30040, volume: 3, RecoveryRestartCompleted
2020-11-16T02:02:45+01:00  P030102      175ce81c76a INFO    RECOVERY state of service: xsengine, stu-08:30043, volume: 2, RecoveryRestartCompleted
2020-11-16T02:02:45+01:00  P030102      175ce935dbe INFO    LOGBCKUP state of service: indexserver, stu-08:30040, volume: 0, BackupExecuteCatalogBackupInProgress
2020-11-16T02:03:08+01:00  P030102      175ce935dbe INFO    LOGBCKUP state of service: indexserver, stu-08:30040, volume: 0, BackupExecuteCatalogBackupFinished
2020-11-16T02:03:08+01:00  P030102      175ce93b8b8 INFO    LOGBCKUP state of service: xsengine, stu-08:30043, volume: 2, BackupLogStarted
2020-11-16T02:03:08+01:00  P030102      175ce93b8b8 INFO    LOGBCKUP to backint: /usr/sap/S08/SYS/global/hdb/backint/DB_S08CLONE/log_backup_2_0_7277056_7277184
2020-11-16T02:03:09+01:00  P030102      175ce93b8b8 INFO    LOGBCKUP start of progress monitoring, volumes: 1, bytes: 8192
2020-11-16T02:03:09+01:00  P030102      175ce93b8b8 INFO    LOGBCKUP progress of service: xsengine, stu-08:30043, volume: 2, 0% 0/8192
2020-11-16T02:03:09+01:00  P030102      175ce81c76a INFO    RECOVERY RECOVER DATA finished successfully, reached timestamp 2020-11-16T01:01:59+01:00, reached log position 236292672
```

Figure 5-30 Restore operation activity in the backup.log file for the S08CLONE database

5.3.5 Restoring SAP HANA database snapshot backups by using IBM Spectrum Copy Data Management

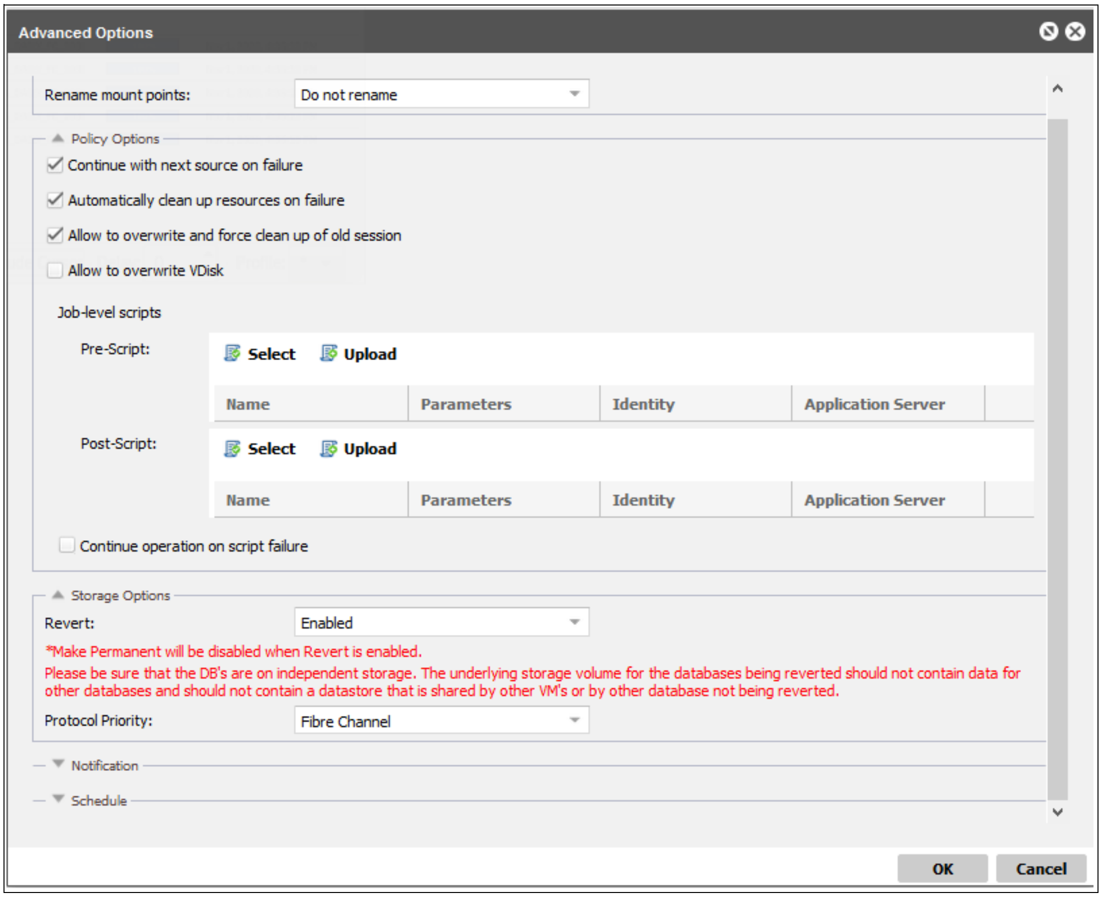
This scenario assumes an environment where the SAP HANA backup is performed only by using the snapshot backup that is based on IBM Spectrum Copy Data Management. When restoring the SAP HANA database from the IBM Spectrum Copy Data Management based snapshot, a restore job must be created. There are two available templates for the SAP HANA restore job:

- Instant database restore, which provides a direct restore mechanism from the data snapshot that is selected with an automatic start of the database but without the possibility to apply more logs.
- Instant disk restore, where IBM Spectrum Copy Data Management performs the mount of the data and log backup snapshot (if the log backup is enabled on the IBM Spectrum Copy Data Management job) and allows for more checks on the snapshot data, test recovery of the snapshot backup, and more log roll-forward. In this case, the recovery operation is required in addition to the snapshot restore operation, and it is performed by using the SAP HANA backup and recovery features that are based on native SQL or GUI (SAP HANA Cockpit or SAP HANA Studio interfaces).

Performing a database recovery by using Instant Database Restore

This scenario restores the latest snapshot backup version that was performed with IBM Spectrum Copy Data Management by using the Instant Database Restore template. In IBM Spectrum Copy Data Management, restore the job with the **`revert`** option on the storage system to overwrite the existing image of the SAP HANA data storage volumes with the snapshot volumes. The source and destination of the snapshot backup and restore are the same SAP HANA system S08. In the Advanced Options window for the restore job options, we select the following items (Figure 5-31):

- Application options: For **Rename mount points**, select **Do not rename**, which is required to use the original SAP HANA data mount point as part of the automated recovery and database startup.
- Storage options:
  - **Revert**: Enabled
  - **Protocol Priority**: FC



Rename mount points: Do not rename

Policy Options

☑ Continue with next source on failure

☑ Automatically clean up resources on failure

☑ Allow to overwrite and force clean up of old session

☐ Allow to overwrite VDisk

Job-level scripts

Pre-Script:

Name	Parameters	Identity	Application Server

Post-Script:

Name	Parameters	Identity	Application Server

☐ Continue operation on script failure

Storage Options

Revert: Enabled

*Make Permanent will be disabled when Revert is enabled.

Please be sure that the DB's are on independent storage. The underlying storage volume for the databases being reverted should not contain data for other databases and should not contain a datastore that is shared by other VM's or by other database not being reverted.

Protocol Priority: Fibre Channel

Figure 5-31 Advanced options for the Instant Database Recovery use case

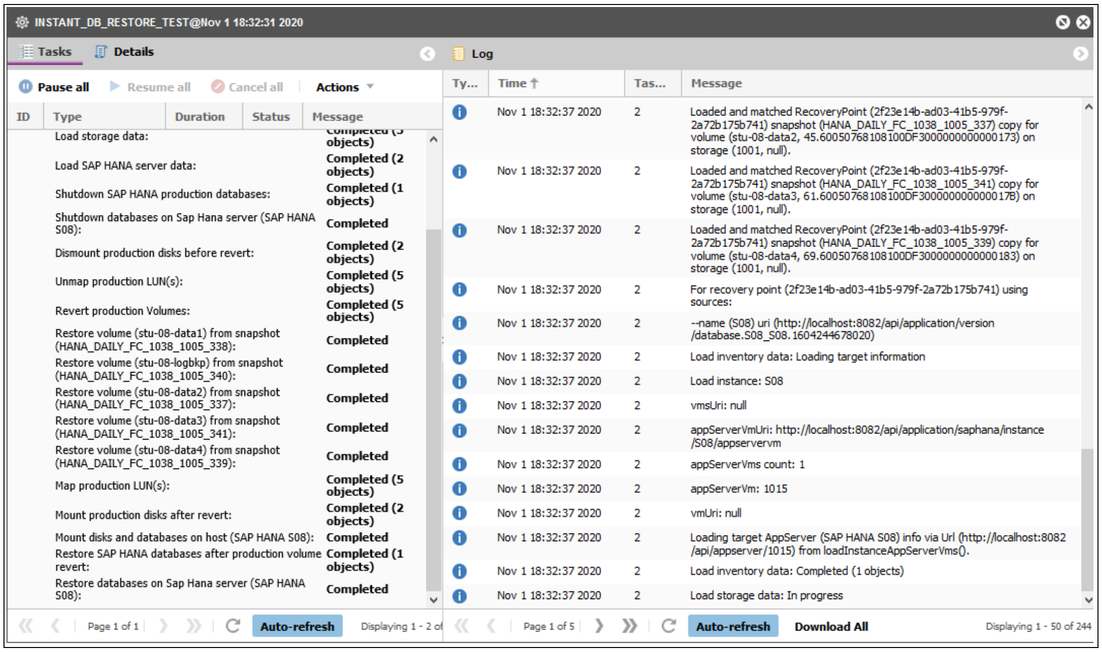
> **Note:** Before starting the restore job, stop the SAP HANA database and deactivate the data and log backup volumes that were included during the backup job.

In our scenario, we run **`umount`** on `/hana/data/S08` and `/hana/logbackup` and also deactivate their volume groups by running the following command:

```
vgchange -a n <volume_group>
```

The database recovery operation requires only the SAP HANA data snapshot to be mounted on the target system for recovery of the data to the snapshot PiT. Due to various scenarios for the backup snapshots being generated with or without log backup enabled, ensure that the parameters `basepath_catalogbackup` and `basepath_logbackup` are not set in the `global.ini` configuration files for the system and tenant databases before starting the restore job.

The restore process performs a reverse FlashCopy operation from the target snapshot volumes in the storage device to the original volumes, so the original volumes are remounted with the image of the snapshot data. The SAP HANA database is recovered and started at the end of the process. The recovery result is shown in Figure 5-32.



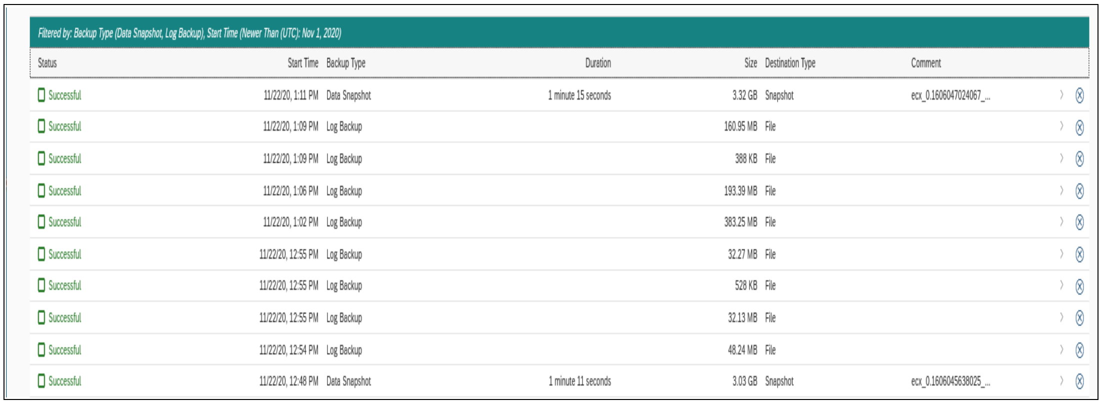
ID	Type	Duration	Status	Message
	Load storage data:			Completed (5 objects)
	Load SAP HANA server data:			Completed (2 objects)
	Shutdown SAP HANA production databases:			Completed (1 objects)
	Shutdown databases on Sap Hana server (SAP HANA S08):			Completed
	Dismount production disks before revert:			Completed (2 objects)
	Unmap production LUN(s):			Completed (5 objects)
	Revert production Volumes:			Completed (5 objects)
	Restore volume (stu-08-data1) from snapshot (HANA_DAILY_FC_1038_1005_338):			Completed
	Restore volume (stu-08-logbkp) from snapshot (HANA_DAILY_FC_1038_1005_340):			Completed
	Restore volume (stu-08-data2) from snapshot (HANA_DAILY_FC_1038_1005_337):			Completed
	Restore volume (stu-08-data3) from snapshot (HANA_DAILY_FC_1038_1005_341):			Completed
	Restore volume (stu-08-data4) from snapshot (HANA_DAILY_FC_1038_1005_339):			Completed
	Map production LUN(s):			Completed (5 objects)
	Mount production disks after revert:			Completed (2 objects)
	Mount disks and databases on host (SAP HANA S08):			Completed
	Restore SAP HANA databases after production volume revert:			Completed (1 objects)
	Restore databases on Sap Hana server (SAP HANA S08):			Completed

Ty...	Time	Tas...	Message
ℹ	Nov 1 18:32:37 2020	2	Loaded and matched RecoveryPoint (2f23e14b-ad03-41b5-979f-2a72b175b741) snapshot (HANA_DAILY_FC_1038_1005_337) copy for volume (stu-08-data2, 45.60050768108100DF3000000000000173) on storage (1001, null).
ℹ	Nov 1 18:32:37 2020	2	Loaded and matched RecoveryPoint (2f23e14b-ad03-41b5-979f-2a72b175b741) snapshot (HANA_DAILY_FC_1038_1005_341) copy for volume (stu-08-data3, 61.60050768108100DF300000000000017B) on storage (1001, null).
ℹ	Nov 1 18:32:37 2020	2	Loaded and matched RecoveryPoint (2f23e14b-ad03-41b5-979f-2a72b175b741) snapshot (HANA_DAILY_FC_1038_1005_339) copy for volume (stu-08-data4, 69.60050768108100DF3000000000000183) on storage (1001, null).
ℹ	Nov 1 18:32:37 2020	2	For recovery point (2f23e14b-ad03-41b5-979f-2a72b175b741) using sources:
ℹ	Nov 1 18:32:37 2020	2	--name (S08) uri (http://localhost:8082/api/application/version /database.S08_S08.1604244678020)
ℹ	Nov 1 18:32:37 2020	2	Load inventory data: Loading target information
ℹ	Nov 1 18:32:37 2020	2	Load instance: S08
ℹ	Nov 1 18:32:37 2020	2	vmsUri: null
ℹ	Nov 1 18:32:37 2020	2	appServerVmUri: http://localhost:8082/api/application/saphana/instance /S08/appservervm
ℹ	Nov 1 18:32:37 2020	2	appServerVms count: 1
ℹ	Nov 1 18:32:37 2020	2	appServerVm: 1015
ℹ	Nov 1 18:32:37 2020	2	vmUri: null
ℹ	Nov 1 18:32:37 2020	2	Loading target AppServer (SAP HANA S08) info via Url (http://localhost:8082 /api/appserver/1015) from loadInstanceAppServerVms().
ℹ	Nov 1 18:32:37 2020	2	Load inventory data: Completed (1 objects)
ℹ	Nov 1 18:32:37 2020	2	Load storage data: In progress

Figure 5-32 Instant Database Restore job activity

Point-in-time recovery by using Instant Disk Restore

This scenario restores the database to a specific PiT between two consecutive snapshots. The recovery scenario is applicable for backups that are created by an IBM Spectrum Copy Data Management backup job with the log backups enabled. The state of the latest two snapshots for the S08 database and the log backups in the SAP HANA backup catalog is shown in Figure 5-33.


Filtered by: Backup Type (Data Snapshot, Log Backup), Start Time (Newer Than (UTC): Nov 1, 2020)

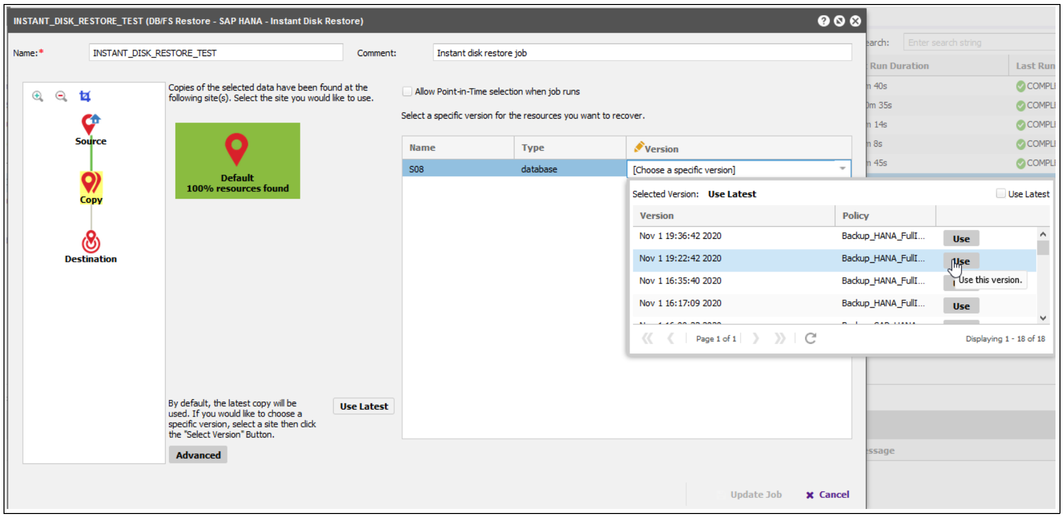
Status	Start Time	Backup Type	Duration	Size	Destination Type	Comment
▢ Successful	11/22/20, 1:11 PM	Data Snapshot	1 minute 15 seconds	3.32 GB	Snapshot	ecx_0.1606047024067_...
▢ Successful	11/22/20, 1:09 PM	Log Backup		160.95 MB	File	
▢ Successful	11/22/20, 1:09 PM	Log Backup		388 KB	File	
▢ Successful	11/22/20, 1:06 PM	Log Backup		193.39 MB	File	
▢ Successful	11/22/20, 1:02 PM	Log Backup		383.25 MB	File	
▢ Successful	11/22/20, 12:55 PM	Log Backup		32.27 MB	File	
▢ Successful	11/22/20, 12:55 PM	Log Backup		528 KB	File	
▢ Successful	11/22/20, 12:55 PM	Log Backup		32.13 MB	File	
▢ Successful	11/22/20, 12:54 PM	Log Backup		48.24 MB	File	
▢ Successful	11/22/20, 12:48 PM	Data Snapshot	1 minute 11 seconds	3.03 GB	Snapshot	ecx_0.1606045638025_...

Figure 5-33 SAP HANA backup catalog with the latest two snapshots and the log backups

The PiT restore for the IBM Spectrum Copy Data Management job is 11/22/20, 1:03 PM.

The following options are used on the restore job:

- Source and target systems are the same SAP HANA system (S08 SAP HANA database instance on the stu-08 host).
- On the copy version, we select **Allow Point-in-Time selection when job runs**, as shown in Figure 5-34.



INSTANT_DISK_RESTORE_TEST (DB/FS Restore - SAP HANA - Instant Disk Restore)

Name:* INSTANT_DISK_RESTORE_TEST Comment: Instant disk restore job

Copies of the selected data have been found at the following site(s). Select the site you would like to use.

☐ Allow Point-in-Time selection when job runs

Select a specific version for the resources you want to recover.

Name	Type	Version
S08	database	[Choose a specific version]

Selected Version: **Use Latest** ☐ Use Latest

Version	Policy	
Nov 1 19:36:42 2020	Backup_HANA_FullI...	Use
Nov 1 19:22:42 2020	Backup_HANA_FullI...	Use
Nov 1 16:35:40 2020	Backup_HANA_FullI...	Use this version.
Nov 1 16:17:09 2020	Backup_HANA_FullI...	Use

Page 1 of 1 Displaying 1 - 18 of 18

By default, the latest copy will be used. If you would like to choose a specific version, select a site then click the "Select Version" Button.

Figure 5-34 Selecting the snapshot version to be restored

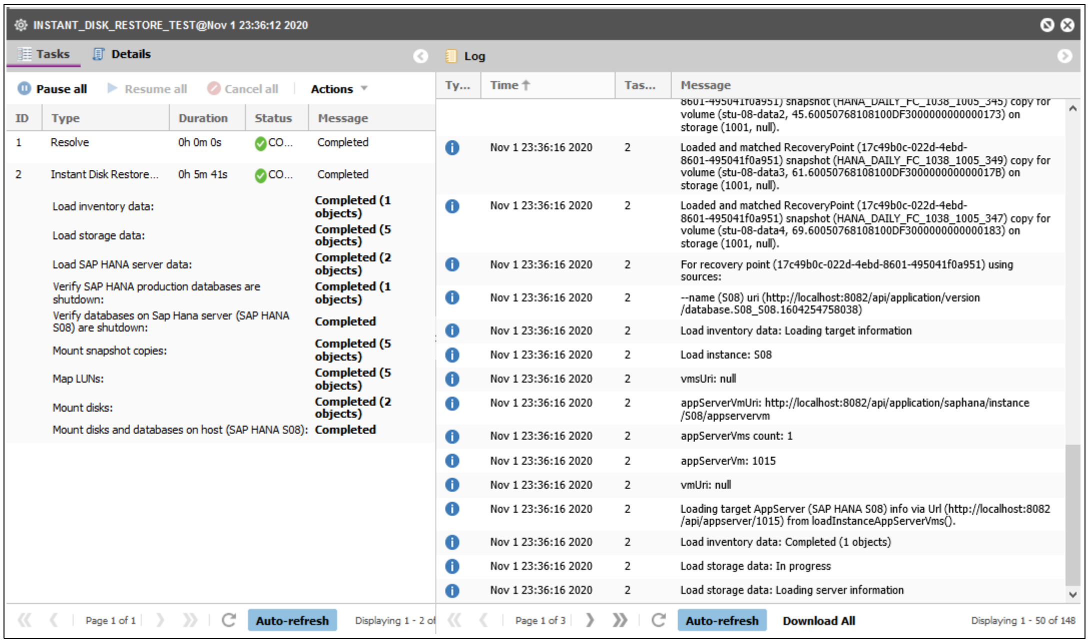
- Application options: Rename `mount points=Add a custom suffix`, where the suffix is `_TEST`.
- Storage options: The following options ensure mounting only the file systems (data+logbackup) on the SAP HANA server, with the possibility to decide later on the storage copy that is tested, such as cancel the copy, revert it, or make permanent volumes out of it:
  - Make Permanent: **User Selection**
  - Revert: **User Selection**
  - Protocol Priority: **FC**

Before starting the restore job, check that the SAP HANA database is shut down but that the original data (`/hana/data/S08`) and log backup (`/hana/logbackup`) volumes can still be mounted (see Example 5-13). The new snapshot image is mounted on different mount points.

Example 5-13 Initial SAP HANA data and log backup file systems

```
Filesystem                            Size  Used Avail Use% Mounted on
/dev/mapper/VG_S08_LOG-LV_S08_LOG     256G  4.4G  252G   2% /hana/log/S08
/dev/mapper/VG_S08_SHARED-LV_S08_SHARED  64G   44G   21G  69% /hana/shared
/dev/mapper/VG_S08_DATA-LV_S08_DATA   512G  6.0G  506G   2% /hana/data/S08
/dev/mapper/VG_S08_LOGBKP-LV_S08_LOGBKP 500G  6.1G  494G   2% /hana/logbackup
```

At the start of the restore job, we are prompted to provide a PiT for restore, so we provide `Nov 22 13:03:00 2020` for our test objective. When running a PiT restore job between two consecutive snapshots, IBM Spectrum Copy Data Management mounts the SAP HANA data volume from the older snapshot image and the logbackup volume from the later snapshot. In our case, the selected version for the SAP HANA data is the data snapshot@12:48 PM and for the SAP HANA log backups the snapshot @1:11 PM (see the backup catalog entries in Figure 5-33 on page 103). The result of the restore job is shown in Figure 5-35.



ID	Type	Duration	Status	Message
1	Resolve	0h 0m 0s	✓ CO...	Completed
2	Instant Disk Restore...	0h 5m 41s	✓ CO...	Completed
	Load inventory data:			**Completed (1 objects)**
	Load storage data:			**Completed (5 objects)**
	Load SAP HANA server data:			**Completed (2 objects)**
	Verify SAP HANA production databases are shutdown:			**Completed (1 objects)**
	Verify databases on Sap Hana server (SAP HANA S08) are shutdown:			**Completed**
	Mount snapshot copies:			**Completed (5 objects)**
	Map LUNs:			**Completed (5 objects)**
	Mount disks:			**Completed (2 objects)**
	Mount disks and databases on host (SAP HANA S08):			**Completed**

Ty...	Time ↑	Tas...	Message
			8601-495041f0a951) snapshot (HANA_DAILY_FC_1038_1005_345) copy for volume (stu-08-data2, 45.60050768108100DF3000000000000173) on storage (1001, null).
ⓘ	Nov 1 23:36:16 2020	2	Loaded and matched RecoveryPoint (17c49b0c-022d-4ebd-8601-495041f0a951) snapshot (HANA_DAILY_FC_1038_1005_349) copy for volume (stu-08-data3, 61.60050768108100DF300000000000017B) on storage (1001, null).
ⓘ	Nov 1 23:36:16 2020	2	Loaded and matched RecoveryPoint (17c49b0c-022d-4ebd-8601-495041f0a951) snapshot (HANA_DAILY_FC_1038_1005_347) copy for volume (stu-08-data4, 69.60050768108100DF3000000000000183) on storage (1001, null).
ⓘ	Nov 1 23:36:16 2020	2	For recovery point (17c49b0c-022d-4ebd-8601-495041f0a951) using sources:
ⓘ	Nov 1 23:36:16 2020	2	--name (S08) uri (http://localhost:8082/api/application/version/database.S08_S08.1604254758038)
ⓘ	Nov 1 23:36:16 2020	2	Load inventory data: Loading target information
ⓘ	Nov 1 23:36:16 2020	2	Load instance: S08
ⓘ	Nov 1 23:36:16 2020	2	vmsUri: null
ⓘ	Nov 1 23:36:16 2020	2	appServerVmUri: http://localhost:8082/api/application/saphana/instance/S08/appservervm
ⓘ	Nov 1 23:36:16 2020	2	appServerVms count: 1
ⓘ	Nov 1 23:36:16 2020	2	appServerVm: 1015
ⓘ	Nov 1 23:36:16 2020	2	vmUri: null
ⓘ	Nov 1 23:36:16 2020	2	Loading target AppServer (SAP HANA S08) info via Url (http://localhost:8082/api/appserver/1015) from loadInstanceAppServerVms().
ⓘ	Nov 1 23:36:16 2020	2	Load inventory data: Completed (1 objects)
ⓘ	Nov 1 23:36:16 2020	2	Load storage data: In progress
ⓘ	Nov 1 23:36:16 2020	2	Load storage data: Loading server information

Figure 5-35 Instant Disk Restore job result - phase 1 (mounting the snapshot on target server)

The mounted file systems are also shown in Example 5-14. The new file systems are mounted from different LVM devices and on different mount points: `/hana/data/S08_TEST` and `/hana/logbackup_TEST`. They correspond to the temporary clones that are generated by the restore job on the storage device from the selected snapshot data and log backup versions.

Example 5-14 Mounted file systems as a result of restore job phase one

```
Filesystem                            Size  Used Avail Use% Mounted on
/dev/mapper/VG_S08_LOG-LV_S08_LOG     256G  4.4G  252G   2% /hana/log/S08
/dev/mapper/VG_S08_SHARED-LV_S08_SHARED 64G  44G   21G  69% /hana/shared
/dev/mapper/VG_S08_DATA-LV_S08_DATA   512G  6.0G  506G   2% /hana/data/S08
/dev/mapper/VG_S08_LOGBKP-LV_S08_LOGBKP 500G 6.1G 494G   2% /hana/logbackup
/dev/mapper/VG_S08_DATAhCX-LV_S08_DATA 512G 4.6G  508G   1% /hana/data/S08_TEST
/dev/mapper/VG_S08_LOGBKPBNm-LV_S08_LOGBKP 500G 5.8G 495G 2% /hana/logbackup_TEST
/dev/mapper/VG_S08_BACKUP-LV_S08_BACKUP 1000G 23G 978G   3% /hana/log/S08_TEST
```

For isolating the original SAP HANA database from the new PiT restored database environment, we use the file system `/hana/log/S08_TEST` on a spare volume as an uninitialized area. At this stage, inspect the mounted file systems, check the logs in the log recovery area, and start the database on the new database image. After confirming the restored image, activate the newly cloned volumes on the S08 instance on the original server and promote them to permanent volumes.

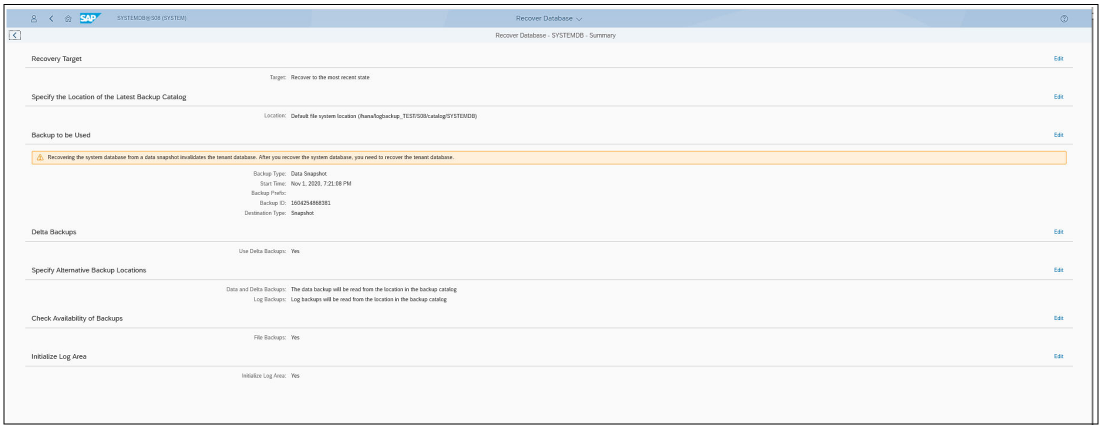
For this purpose, we save the original `global.ini` files of the system and tenant databases and modify the configuration to point to the new locations (`_TEST`), as shown in Example 5-15.

Example 5-15 Modifying the SAP HANA global configuration for the new log and catalog backup location

```
*******************system database global configuration file**********************
[root@stu-08 ~]# cat /hana/shared/S08/global/hdb/custom/config/global.ini
# global.ini last modified 2020-11-21 16:31:24.637323 by hdbnameserver
[communication]
ssl = systempki

[multidb]
mode = multidb
database_isolation = low

[persistence]
basepath_catalogbackup = /hana/logbackup_TEST/S08/catalog
basepath_logbackup = /hana/logbackup_TEST/S08
basepath_datavolumes = /hana/data/S08_TEST
basepath_logvolumes = /hana/log/S08_TEST

[system_information]
xsa_sizing = M
*******************system database global configuration file**********************

*******************S08 tenant database global configuration
file*******************
[root@stu-08 ~]# cat /hana/shared/S08/global/hdb/custom/config/DB_S08/global.ini
# global.ini last modified 2020-11-21 16:31:24.128549 by hdbindexserver -port
30003
[persistence]
basepath_catalogbackup = /hana/logbackup_TEST/S08/catalog
basepath_logbackup = /hana/logbackup_TEST/S08
[root@stu-08 ~]#
*******************S08 tenant database global configuration file*****************
```

Now, we continue with the SAP HANA database recovery process by using SAP HANA Cockpit, starting with SYSTEMDB and then with the S08 tenant database from the Database Overview of the system database in the access recovery wizard. In the recovery wizard, the data snapshot @12:48 PM is outlined as Available (green) and used during the recovery process. When performing the system database recovery, only recovery to most recent state is possible by using SAP HANA Cockpit. We also select to initialize the log recovery area because we are generating a cloned database with an uninitialized SAP HANA log volume in our test case.

A review of all settings that were selected for the recovery wizard is shown in Figure 5-36 on page 107.



Recover Database - SYSTEMDB - Summary

Recovery Target

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog

Location: Default file system location (/hana/logbackup_TEST/S08/catalog/SYSTEMDB)

Backup to be Used

⚠ Recovering the system database from a data snapshot invalidates the tenant database. After you recover the system database, you need to recover the tenant database.

Backup Type: Data Snapshot
Start Time: Nov 1, 2020, 7:21:08 PM
Backup Prefix:
Backup ID: 1604254868381
Destination Type: Snapshot

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Log backups will be read from the location in the backup catalog

Check Availability of Backups

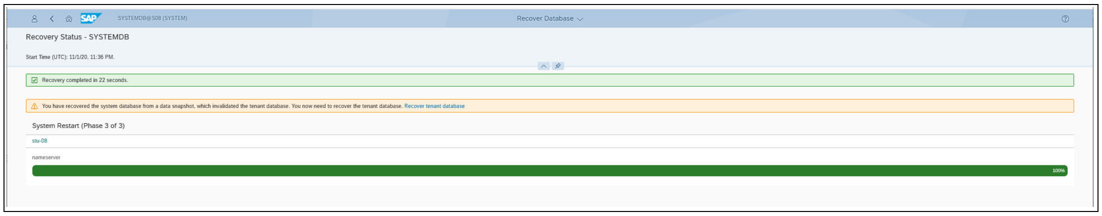
File Backups: Yes

Initialize Log Area

Initialize Log Area: Yes

Figure 5-36 Summary of the recovery options for the system database

The system database recovery completed successfully, as shown in Figure 5-37.



Recovery Status - SYSTEMDB

Start Time (UTC): 11/1/20, 11:36 PM.

☑ Recovery completed in 22 seconds.

⚠ You have recovered the system database from a data snapshot, which invalidated the tenant database. You now need to recover the tenant database. Recover tenant database

System Restart (Phase 3 of 3)

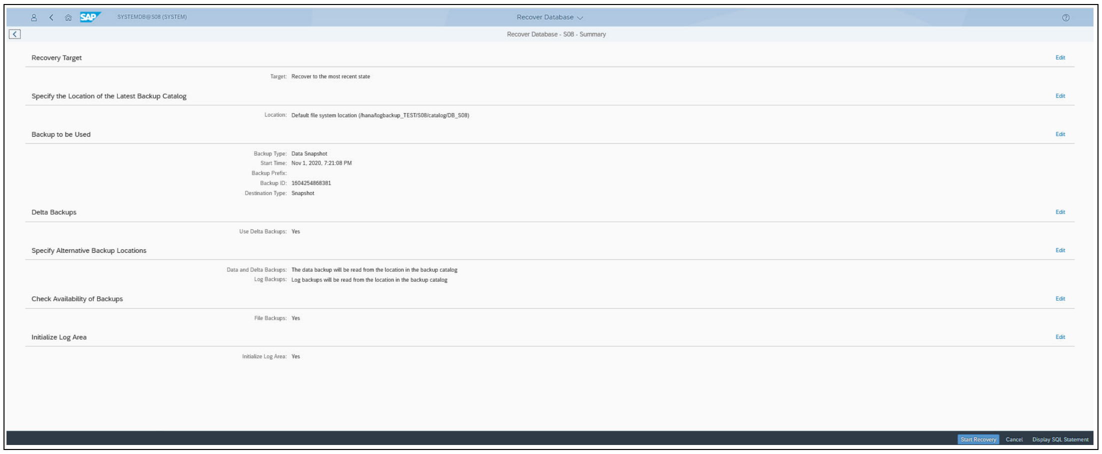
stu-08

nameserver

100%

Figure 5-37 System database complete recovery

After the recovery of the system database completes, the tenant database must be recovered by using a similar process. Start the wizard by going to the Database Management window for SYSTEMDB@S08 by selecting **Tenant Actions** → **Recover Tenant**. We specify the recovery objective point for 13:03:00 CET time (12:03:00 Coordinated Universal Time). A summary of recovery options is illustrated in Figure 5-38.



Recover Database - S08 - Summary

Recovery Target

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog

Location: Default file system location (/hana/logbackup_TEST/S08/catalog/DB_S08)

Backup to be Used

Backup Type: Data Snapshot
Start Time: Nov 1, 2020, 7:21:08 PM
Backup Prefix:
Backup ID: 1604254868381
Destination Type: Snapshot

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Log backups will be read from the location in the backup catalog

Check Availability of Backups

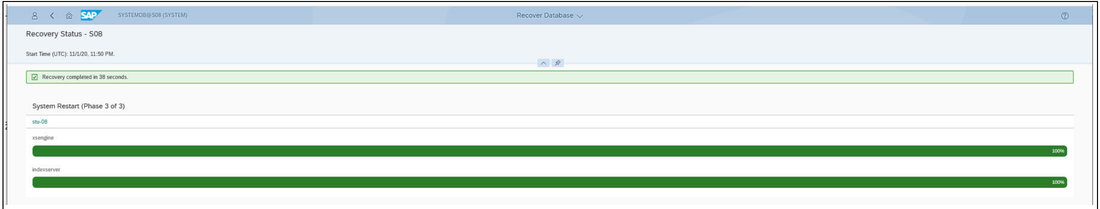
File Backups: Yes

Initialize Log Area

Initialize Log Area: Yes

Figure 5-38 Summary of the S08 tenant database recovery options

The result of the recovery operation for the tenant database S08 is shown in Figure 5-39. The recovery point is 12:02:45 PM (Coordinated Universal Time), which is the nearest log backup that is available for the 12:03 PM (Coordinated Universal Time) PiT that is set for recovery (also see the initial backup catalog entries that are shown in Figure 5-33 on page 103).



Recovery Status - S08

Start Time (UTC): 11/1/20, 11:50 PM.

☑ Recovery completed in 38 seconds.

System Restart (Phase 3 of 3)

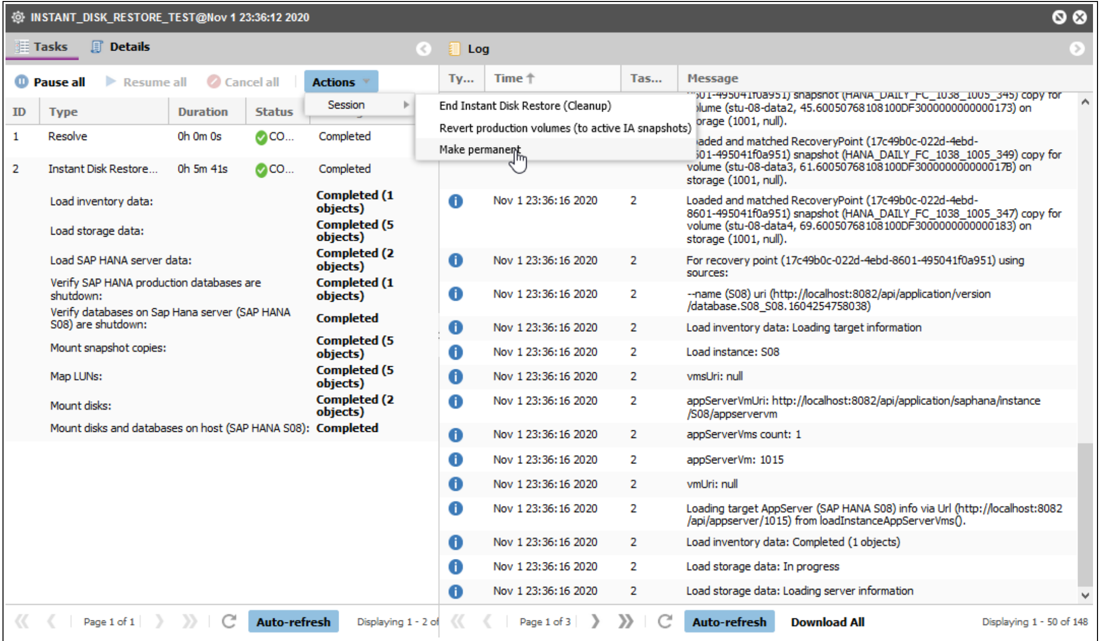
stu-08

xsengine 100%

indexserver 100%

Figure 5-39 Recovery completed for the S08 tenant database

After confirming the entire snapshot recovery operation, the cloned volumes on storage can be dropped if the database that is recovered is no longer needed, reverted, or promoted to permanent volumes. In our case, we promote them to full data copies on the storage device. In this case, go to the IBM Spectrum Copy Data Management restore job window, and in the Activity Detail window, select **Actions** → **Make permanent production volume**, as shown in Figure 5-40. In this phase, the volumes that are initially mounted as FlashCopy targets to the host are converted to full copies of independent volumes.



ID	Type	Duration	Status	
1	Resolve	0h 0m 0s	✓ CO...	Completed
2	Instant Disk Restore...	0h 5m 41s	✓ CO...	Completed
	Load inventory data:			Completed (1 objects)
	Load storage data:			Completed (5 objects)
	Load SAP HANA server data:			Completed (2 objects)
	Verify SAP HANA production databases are shutdown:			Completed (1 objects)
	Verify databases on Sap Hana server (SAP HANA S08) are shutdown:			Completed
	Mount snapshot copies:			Completed (5 objects)
	Map LUNs:			Completed (5 objects)
	Mount disks:			Completed (2 objects)
	Mount disks and databases on host (SAP HANA S08):			Completed

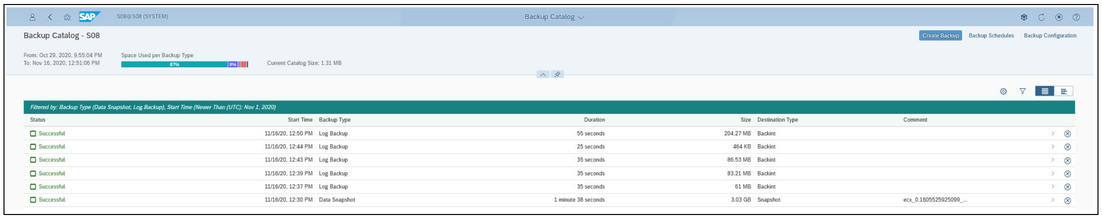
Ty...	Time ↑	Tas...	Message
			501-495041f0a951) snapshot (HANA_DAILY_FC_1038_1005_345) copy for olume (stu-08-data2, 45.60050768108100DF3000000000000173) on orage (1001, null).
			aded and matched RecoveryPoint (17c49b0c-022d-4ebd-501-495041f0a951) snapshot (HANA_DAILY_FC_1038_1005_349) copy for volume (stu-08-data3, 61.60050768108100DF300000000000017B) on storage (1001, null).
ℹ	Nov 1 23:36:16 2020	2	Loaded and matched RecoveryPoint (17c49b0c-022d-4ebd-8601-495041f0a951) snapshot (HANA_DAILY_FC_1038_1005_347) copy for volume (stu-08-data4, 69.60050768108100DF3000000000000183) on storage (1001, null).
ℹ	Nov 1 23:36:16 2020	2	For recovery point (17c49b0c-022d-4ebd-8601-495041f0a951) using sources:
ℹ	Nov 1 23:36:16 2020	2	--name (S08) uri (http://localhost:8082/api/application/version /database.S08_S08.1604254758038)
ℹ	Nov 1 23:36:16 2020	2	Load inventory data: Loading target information
ℹ	Nov 1 23:36:16 2020	2	Load instance: S08
ℹ	Nov 1 23:36:16 2020	2	vmsUri: null
ℹ	Nov 1 23:36:16 2020	2	appServerVmUri: http://localhost:8082/api/application/saphana/instance /S08/appservervm
ℹ	Nov 1 23:36:16 2020	2	appServerVms count: 1
ℹ	Nov 1 23:36:16 2020	2	appServerVm: 1015
ℹ	Nov 1 23:36:16 2020	2	vmUri: null
ℹ	Nov 1 23:36:16 2020	2	Loading target AppServer (SAP HANA S08) info via Url (http://localhost:8082 /api/appserver/1015) from loadInstanceAppServerVms().
ℹ	Nov 1 23:36:16 2020	2	Load inventory data: Completed (1 objects)
ℹ	Nov 1 23:36:16 2020	2	Load storage data: In progress
ℹ	Nov 1 23:36:16 2020	2	Load storage data: Loading server information

Figure 5-40 Making the cloned volumes permanent (phase 2)

The “Make permanent” operation is running transparently in the background as a non-disruptive operation for the SAP HANA host (stu-08). When the operation completes, the cloned volumes that are copied from the storage snapshot image that is selected during the recovery operation are detached from the FlashCopy mapping, and they are running as independent disks that are attached to the SAP HANA host.

5.3.6 Snapshot backup recovery by using IBM Spectrum Copy Data Management with log recovery from IBM Spectrum Protect

For this scenario, consider the backup context of the S08 database, as shown in Figure 5-41, where a snapshot backup was generated by using IBM Spectrum Copy Data Management (for more information, see 5.2.2, “Performing a database snapshot backup by using IBM Spectrum Copy Data Management” on page 81) with a job that does not have the log backup enabled, and the log backup is automatically performed by using the IBM Spectrum Protect Data Protection for SAP HANA Backint agent (for more information, see “Automatic log back up to IBM Spectrum Protect” on page 76). We perform a recovery up to the most recent state by using the latest version of the snapshot backup and applying the redo logs backup that is saved on the IBM Spectrum Protect server.



Backup Catalog - S08

From: Oct 29, 2020, 9:55:04 PM
To: Nov 16, 2020, 12:51:06 PM

Current Catalog Size: 1.31 MB

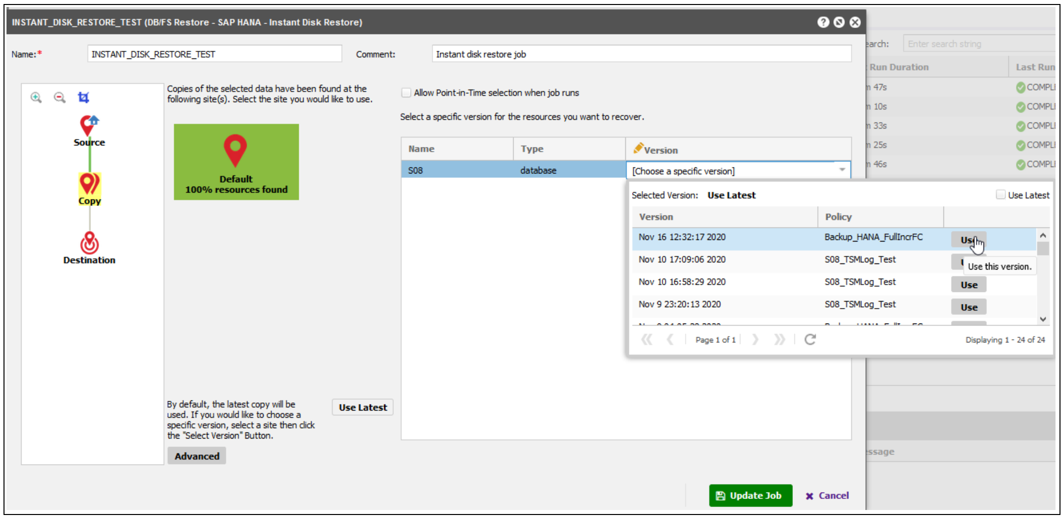
Filtered by: Backup Type (Data Snapshot, Log Backup), Start Time (Newer Than (UTC): Nov 1, 2020)

Status	Start Time	Backup Type	Duration	Size	Destination Type	Comment
Successful	11/16/20, 12:50 PM	Log Backup	55 seconds	204.27 MB	Backint	
Successful	11/16/20, 12:44 PM	Log Backup	25 seconds	464 KB	Backint	
Successful	11/16/20, 12:43 PM	Log Backup	35 seconds	86.53 MB	Backint	
Successful	11/16/20, 12:39 PM	Log Backup	35 seconds	83.21 MB	Backint	
Successful	11/16/20, 12:37 PM	Log Backup	35 seconds	61 MB	Backint	
Successful	11/16/20, 12:30 PM	Data Snapshot	1 minute 38 seconds	3.03 GB	Snapshot	ecx_0.1605525925099_...

Figure 5-41 S08 backup catalog entries

We check that the S08 database is stopped and the file systems `/hana/data/S08` and `/hana/logbackup` are unmounted from the SAP HANA system before starting the recovery operation. We use a IBM Spectrum Copy Data Management Instant Disk Restore job with the following configuration:

- The source and target systems are the same SAP HANA system (S08 SAP HANA database instance on stu-08 host).
- The snapshot version is the latest, as shown in Figure 5-42.



INSTANT_DISK_RESTORE_TEST (DB/FS Restore - SAP HANA - Instant Disk Restore)

Name:* INSTANT_DISK_RESTORE_TEST

Comment: Instant disk restore job

Copies of the selected data have been found at the following site(s). Select the site you would like to use.

By default, the latest copy will be used. If you would like to choose a specific version, select a site then click the "Select Version" Button.

□ Allow Point-in-Time selection when job runs

Select a specific version for the resources you want to recover.

Name	Type	Version
S08	database	[Choose a specific version]

Selected Version: **Use Latest** □ Use Latest

Version	Policy	
Nov 16 12:32:17 2020	Backup_HANA_FullIncrFC	Use
Nov 10 17:09:06 2020	S08_TSMLog_Test	Use
Nov 10 16:58:29 2020	S08_TSMLog_Test	Use
Nov 9 23:20:13 2020	S08_TSMLog_Test	Use

Use this version.

Page 1 of 1 Displaying 1 - 24 of 24

Figure 5-42 Selecting the snapshot version to be restored

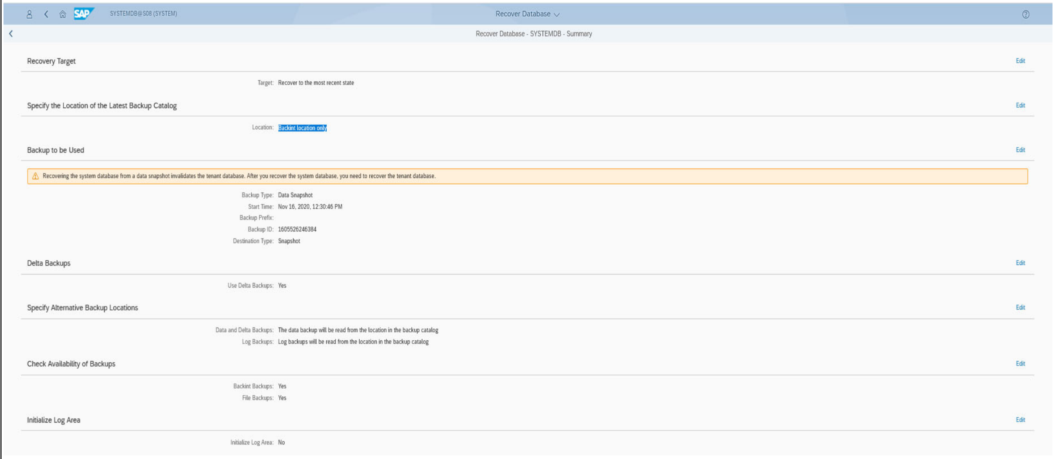
- Application options: Rename mount points to ”Do not rename”.

- Storage options: The following options perform a FlashCopy revert operation on the IBM Spectrum Virtualize device, and mounts the SAP HANA data file system on the server:
  - Make permanent: N/A
  - Revert: **Enabled**
  - Protocol priority: **FC**

The restore job runs and finishes with a "COMPLETED" state after restoring the content of the snapshot on the original volumes and mounting the SAP HANA data volume `/hana/data/S08`.

We continue the recovery process for the S08 tenant database by using SAP HANA Cockpit and specifying the Backint option for log recovery. The backup catalog and redo log backups that are used for recovery are restored from the IBM Spectrum Protect server, and the snapshot image to be restored is made available in the data area by an IBM Spectrum Copy Data Management restore job. The recovery is using the same SAP HANA Cockpit flow that is described in "Point-in-time recovery by using Instant Disk Restore" on page 103:

1. Recovery of the system database is performed first by using the Backint location for the logs. The recovery is performed to the most recent state. A summary of the recovery options that are used are shown in Figure 5-43.



Recovery Target

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog

Location: Backint location only

Backup to be Used

⚠ Recovering the system database from a data snapshot invalidates the tenant database. After you recover the system database, you need to recover the tenant database.

Backup Type: Data Snapshot
Start Time: Nov 16, 2020, 12:30:46 PM
Backup Prefix:
Backup ID: 1605526246384
Destination Type: Snapshot

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Log backups will be read from the location in the backup catalog

Check Availability of Backups

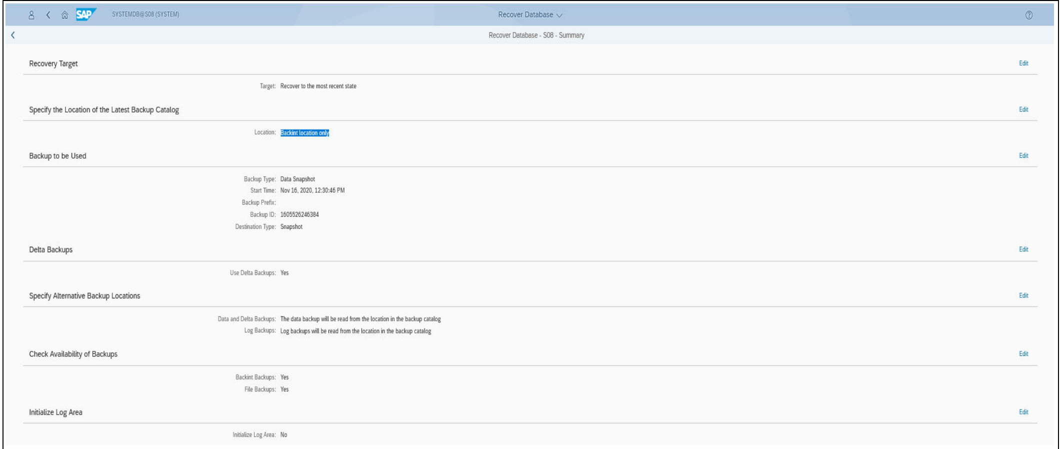
Backint Backups: Yes
File Backups: Yes

Initialize Log Area

Initialize Log Area: No

Figure 5-43 Summary of recovery options for the system database

2. After a complete recovery and start of the system database from the snapshot backup, perform the recovery of the tenant database S08. The RPO is also the most recent state. A similar recovery wizard as in the system database case is followed and the summary options are displayed in Figure 5-44.



Recover Database - S08 - Summary

Recovery Target — Edit

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog — Edit

Location: Backint location only

Backup to be Used — Edit

Backup Type: Data Snapshot
Start Time: Nov 16, 2020, 12:30:46 PM
Backup Prefix:
Backup ID: 1605526246384
Destination Type: Snapshot

Delta Backups — Edit

Use Delta Backups: Yes

Specify Alternative Backup Locations — Edit

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Log backups will be read from the location in the backup catalog

Check Availability of Backups — Edit

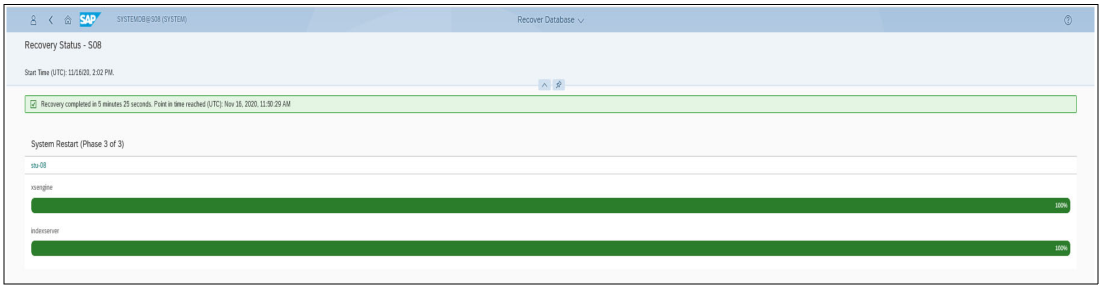
Backint Backups: Yes
File Backups: Yes

Initialize Log Area — Edit

Initialize Log Area: No

Figure 5-44 Summary of the recovery options for tenant database S08

The final result of the recovery operation is shown in Figure 5-45. The PiT recovery is 12:50:29 CET (Coordinated Universal Time+1), which can be correlated to the available logs in the backup catalog at the time the S08 database stopped for recovery from the snapshot (also see the initial backup catalog entries for S08 database in Figure 5-41 on page 109).



Recovery Status - S08

Start Time (UTC): 11/16/20, 2:02 PM.

☑ Recovery completed in 5 minutes 25 seconds. Point in time reached (UTC): Nov 16, 2020, 11:50:29 AM

System Restart (Phase 3 of 3)

stu-08

xsengine 100%

indexserver 100%

Figure 5-45 S08 tenant database: Recovery complete

A

Scheduling an SAP HANA backup by using IBM Spectrum Protect

This appendix provides a sample script to be used for an SAP High-performance Analytic Appliance (HANA) full backup by using the Backint agent that is provided by IBM Spectrum Protect Data Protection for SAP HANA, and how to configure the automation of the backup by using the scheduling services of IBM Spectrum Protect.

This appendix contains the following topics:

- “Sample script for a full backup of an SAP HANA database” on page 114.
- “Configuring the IBM Spectrum Protect scheduler” on page 115.
- “Configuring the scheduler on IBM Spectrum Protect server” on page 115.
- “Configuring the client scheduler service” on page 116.

Sample script for a full backup of an SAP HANA database

The following script performs a full backup of an SAP HANA database. It uses two input parameters: The SAP HANA SID (SAP HSID) and SAP HANA database for backup (HDB) to set the appropriate context and connect to the database in single or multitenant environments. The following prerequisites and considerations apply for running the script:

- Data Protection of SAP HANA agent is configured and the TSM key is set in the SAP HANA secure user store. Check that the key is present by running the **hdbuserstore** command, as shown in Example 5-2 on page 78.
- The script has execution permission. The script is run as root and switches to the `<sid>adm` user to start the SAP HANA database by running a native SQL command on the **hdbsql** client.
- The client scheduler service is configured and running on the SAP HANA system. The script uses the environment variables *$HSID* for HANA SID and *$HDB* for the SAP HANA target database name for backup, which are set by using systemd environment variables in Red Hat Enterprise Linux 7. For another configuration example, see "Managing the scheduler service by using systemd on Red Hat Enterprise Linux 7" on page 117. The variables can also be statically defined in the script for a specific SAP HANA target database environment.
- The script provides more output to the `/tsm/$HSID` folder, as shown in Example A-1, which must exist and contain the `dsm_$HDB.opt` IBM Spectrum Protect application programming interface (API) options file for the definition of the connectivity to the IBM Spectrum Protect server.

Example A-1 SAP HANA full backup script: HANA_full_bkp.sh

```
#!/bin/sh

###############################################################################
##
#for static setup of HSID and HDB uncomment the bellow lines and
#set them to the appropriate values
#for Red Hat Enterprise Linux 7.x the variables can be passed through systemd
environment variables
#HSID=S08
#HDB=S08
###############################################################################
##
LOG=/tsm/${HSID}/HANA_full_${HDB}.log
export DSMI_CONFIG=/tsm/${HSID}/dsm_${HDB}.opt
export DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
export DSMI_LOG=/tsm/${HSID}
inst=`echo $HSID | tr '[:upper:]' '[:lower:]'`
echo "Starting backup of ${HDB}@${HSID} ...." >> $LOG
echo "Date: `date`" >> $LOG
su - ${inst}adm -c "hdbsql -U TSM -d $HDB \"backup data using backint
('FULL_${HDB}_$(date +'%Y_%m_%d:%H:%M')')\"" >> $LOG 2>&1
RC=$?

if [ $RC -eq 0 ]
then
echo "Backup of database ${HDB}@${HSID} successful !" >> $LOG
else
echo "Backup of instance ${HDB}@${HSID} unsuccessful !" >> $LOG
```

```
fi

echo "Date: `date`"
exit $RC
```

Configuring the IBM Spectrum Protect scheduler

Enabling the backup script to run by using the IBM Spectrum Protect centralized scheduler services requires a two-sided configuration:

- Server-side configuration: The scheduler is defined in the policy domain of the SAP HANA node that is associated with the target database for backup, and the node is associated with the scheduler.
- Client-side configuration: The client scheduler service is configured for Data Protection for SAP HANA agent connectivity to the IBM Spectrum Protect server.

Configuring the scheduler on IBM Spectrum Protect server

The following steps are used for defining a scheduler for an SAP HANA full backup by using a weekly frequency. We use the following configuration parameters for this scenario, which are defined on the IBM Spectrum Protect server as part of the Data Protection for SAP HANA agent configuration:

- Policy domain: `HANA_DOM`
- Node name for HANA database S08 backup: `STU-08-HANA`

Complete the following steps:

1. From the administrative command-line interface (CLI) (`dsmadmc`), create the scheduler `HANA_WEEKLY_FULL` in the domain `HANA_DOM` with a weekly frequency that runs Sunday at 08:00 PM:

   ```
   define schedule HANA_DOM HANA_WEEKLY_FULL Description='HANA Weekly Full Backup
   to IBM Spectrum Protect' action=command object='/tsm/scripts/HANA_full_bkp.sh'
   period=1 perunit=week dayofWeek=Sunday startt=20:00:00
   ```

   Check the scheduler definition by running the **`q schedule`** command, as shown in Example A-2.

   Example A-2 Defining the weekly backup scheduler for an SAP HANA full database backup

   ```
   Protect: AIX-AW>q sched HANA_DOM HANA_WEEKLY_FULL f=d

               Policy Domain Name: HANA_DOM
                    Schedule Name: HANA_WEEKLY_FULL
                      Description: HANA Weekly Full Backup to IBM Spectrum Protect
                           Action: Command
                        Subaction:
                          Options:
                          Objects: /tsm/scripts/HANA_full_bkp.sh
                         Priority: 5
                  Start Date/Time: 11/14/20   20:00:00
                         Duration: 1 Hour
       Maximum Run Time (Minutes): 0
   ```

```
                Schedule Style: Classic
                        Period: 1 Week
                   Day of Week: Sunday
                         Month:
                  Day of Month:
                 Week of Month:
                    Expiration:
Last Update by (administrator): ADMIN
         Last Update Date/Time: 11/14/20   00:40:44
              Managing profile:
```

The scheduler runs the script **/tsm/scripts/HANA_full_bkp.sh** on the SAP HANA server to perform the full database backup.

2. Associate the scheduler with the SAP HANA node by running the following command:

```
define assoc HANA_DOM HANA_WEEKLY_FULL STU-08-HANA
```

Configuring the client scheduler service

In our example, we use the folder `/tsm/S08` that is owned by the SAP HANA instance user s08adm, where we keep the configuration files for IBM Spectrum Protect API, errorlog files, password-generated files, scheduler, and SAP HANA backup script outputs. The target database has the system instance name of S08, and the tenant database is S08.

The options file that is used for the IBM Spectrum Protect API configuration with Data Protection for SAP HANA agent and the client scheduler service is shown in Example A-3.

Example A-3 Client option file for the IBM Spectrum Protect API and client scheduler service

```
[root@stu-08 ~]# cat /tsm/S08/dsm_S08.opt
SErvername AIX-AW-HANA
```

The associated stanza in the system options file `dsm.sys` (`$DSMI_DIR/dsm.sys`) is shown in Example A-4.

Example A-4 The dsm.sys stanza for the server name that is used in the client option file

```
SErvername AIX-AW-HANA
   COMMMethod         TCPip
   TCPPort            1500
   TCPServeraddress   10.0.240.164
   Nodename STU-08-HANA
   PASSWORDACCESS GENERATE
   ERRORLOGName /tsm/S08/dsmerror_s08.log
   PASSWORDDIR /tsm/S08
   SCHEDLOGName /tsm/S08/dsmsched_s08.log
   SCHEDLOGRetention 30 D
```

Our example case uses the node name `STU-08-HANA` for backing up the tenant database S08 to the IBM Spectrum Protect server. We use the CAD default option to manage only the web client. If the CAD service is configured to also manage the scheduler, the following option is added to the `dsm.sys` stanza:

```
managedservices webclient schedule
```

To run the backup script for the database backup that is defined with the IBM Spectrum Protect scheduler, the client scheduler must be started. It can be started manually for verification purposes. In the context of the backup script that is presented in “Sample script for a full backup of an SAP HANA database” on page 114, you must run the script as root by running the following command:

```
/bin/dsmc schedule -optfile=/tsm/S08/dsm_S08.opt
```

Managing the scheduler service by using systemd on Red Hat Enterprise Linux 7

In Red Hat Enterprise Linux 7, you can configure systemd units to manage the IBM Spectrum Protect client scheduler services and automate the service start. In our scenario, we create a systemd unit for the client service and configure it for passing the variables SAP HANA system ID (*HSID*) and *HDB* to the backup script at the time of execution. The flexibility of the systemd resource configuration allows deploying multiple services that are customized for each database and SAP HANA system, and the backup script can be reused without changes.

To define the client scheduler service, complete the following steps:

1. Create a unit file that is specific to the database that is targeted for backup. In our environment, we use the SAP HANA instance S08 with the tenant database S08, as shown in Example A-5.

   Example A-5 Unit file for the S08 database client scheduler service

   ```
   [root@stu-08 ~]# cat /etc/systemd/system/dsmcsched_s08.service
   [Unit]
   Description="IBM Spectrum Protect client scheduler for SAP HANA S08"
   After=local-fs.target network-online.target

   [Service]
   Type=simple
   GuessMainPID=no
   Environment="DSM_LOG=/tsm/S08"
   Environment="HSID=S08"
   Environment="HDB=S08"
   ExecStart=/bin/sh -c '/usr/bin/dsmc sched -optfile=/tsm/S08/dsm_S08.opt'
   ExecStopPost=/bin/bash -c 'let i=0; while [[ (-n "$(ps -ef | grep 'dsmc sched'
   | grep S08)") && ($i -le 10) ]]; do let i++; sleep 1; done'
   Restart=on-failure

   [Install]
   WantedBy=multi-user.target
   ```

   In Example A-5, the variables *HSID* and *HDB* are defined in the systemd environment and used by the backup script at run time.

2. Refresh the systemd unit list by running the following command:

   ```
   systemctl daemon-reload
   ```

3. Enable the client scheduler service at start time by running the following command:

   ```
   systemctl enable dsmcsched_s08.service
   ```

4. Start the service by using the following command:

   ```
   systemctl start dsmcsched_s08.service
   ```

You can manage the service by using star, stop, and status commands for **systemctl**. Example A-6 shows an example of checking the status of the service after it starts.

Example A-6 Checking the status of the client scheduler service for the S08 HANA database

```
[root@stu-08 ~]# systemctl status dsmcsched_s08.service
? dsmcsched_s08.service - "IBM Spectrum Protect client scheduler for SAP HANA
S08"
   Loaded: loaded (/etc/systemd/system/dsmcsched_s08.service; enabled; vendor
preset: disabled)
   Active: active (running) since Fri 2020-11-20 06:07:08 +04; 8s ago
 Main PID: 116338 (dsmc)
   CGroup: /system.slice/dsmcsched_s08.service
           ··116338 /usr/bin/dsmc sched -optfile=/tsm/S08/dsm_S08.opt

Nov 20 06:07:08 stu-08.saphana.example.com systemd[1]: Started "IBM Spectrum
Protect client scheduler for SAP HANA S08".
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: IBM Spectrum Protect
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: Command Line
Backup-Archive Client Interface
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: Client Version 8,
Release 1, Level 11.0
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: Client date/time:
11/20/2020 06:07:08
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: (c) Copyright by IBM
Corporation and other(s) 1990, 2018. All Rights Reserved.
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: IBM Spectrum Protect
Backup-Archive Client Version 8, Release 1, Level 11.0
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: Querying server for next
scheduled event.
Nov 20 06:07:08 stu-08.saphana.example.com sh[116338]: Node Name: STU-08-HANA
```

After the service starts, monitor the activity of the scheduler in the log file that is defined in the system options file by using the parameter `SCHEDLOGName` in `dsm.sys`, which is shown in Example A-4 on page 116.

B

Configuring IBM Spectrum Protect with IBM Cloud Object Storage

This appendix provides a configuration example for IBM Spectrum Protect with IBM Cloud Object Storage. This scenario can be applied to an SAP High-performance Analytic Appliance (HANA) database backup that uses Data Protection for SAP HANA agent to store data on cloud storage that is attached to the IBM Spectrum Protect server.

This appendix provides an example about provisioning IBM Cloud Object Storage and how to configure the IBM Spectrum Protect server cloud container storage pool.

This appendix contains the following topics:

- “IBM Cloud Object Storage” on page 120.
- “Provisioning IBM Cloud Object Storage” on page 120.
- “Defining the cloud container pool for SAP HANA backup” on page 124.

IBM Cloud Object Storage

IBM Cloud Object Storage provides durable, security-rich, and cost-effective cloud storage for various backup needs. It helps replace tape, streamlines backup operations, and simplifies archival processes.

IBM Cloud Object Storage offers various storage classes to meet high capacity demands and various access pattern needs. For our configuration example, we selected the cold vault option. Use this option for data that must be stored on cloud but accessed for read operations only a few times a year. Common use cases include long-term backup, large data set preservation, or older media content.

For more information, see IBM Cloud Object Storage.

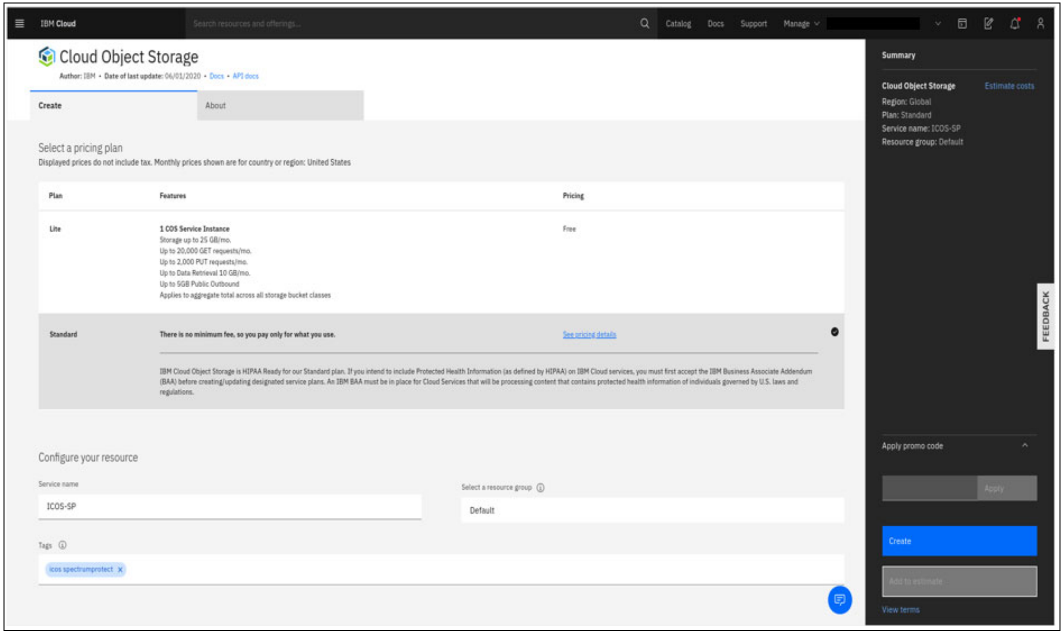
Provisioning IBM Cloud Object Storage

To provision the IBM Cloud Object Storage cold vault class storage for use with IBM Spectrum Protect, complete the following steps:

1. Log in to IBM Cloud by using an account with IBM Cloud Object Storage administrative privileges.

   For more information about access control policies for IBM Cloud Object Storage, see Setting Access Control Policies for IBM Cloud Object Storage.

2. Create an IBM Cloud Object Storage resource instance by selecting **Catalog** → **Object Storage**, and selecting the pricing plan (Lite or Standard) and a name for the IBM Cloud Object Storage service. Tags are optional, but in this case we use `icos spectrumprotect`, as shown in Figure B-1.



Cloud Object Storage

Author: IBM • Date of last update: 06/01/2020 • Docs • API docs

Select a pricing plan

Displayed prices do not include tax. Monthly prices shown are for country or region: United States

Plan	Features	Pricing
Lite	1 COS Service Instance Storage up to 25 GB/mo. Up to 20,000 GET requests/mo. Up to 2,000 PUT requests/mo. Up to Data Retrieval 10 GB/mo. Up to 5GB Public Outbound Applies to aggregate total across all storage bucket classes	Free
Standard	There is no minimum fee, so you pay only for what you use. IBM Cloud Object Storage is HIPAA Ready for our Standard plan. If you intend to include Protected Health Information (as defined by HIPAA) on IBM Cloud services, you must first accept the IBM Business Associate Addendum (BAA) before creating/updating designated service plans. An IBM BAA must be in place for Cloud Services that will be processing content that contains protected health information of individuals governed by U.S. laws and regulations.	See pricing details

Configure your resource

Service name: ICOS-SP

Select a resource group: Default

Tags: icos spectrumprotect

Summary

Cloud Object Storage

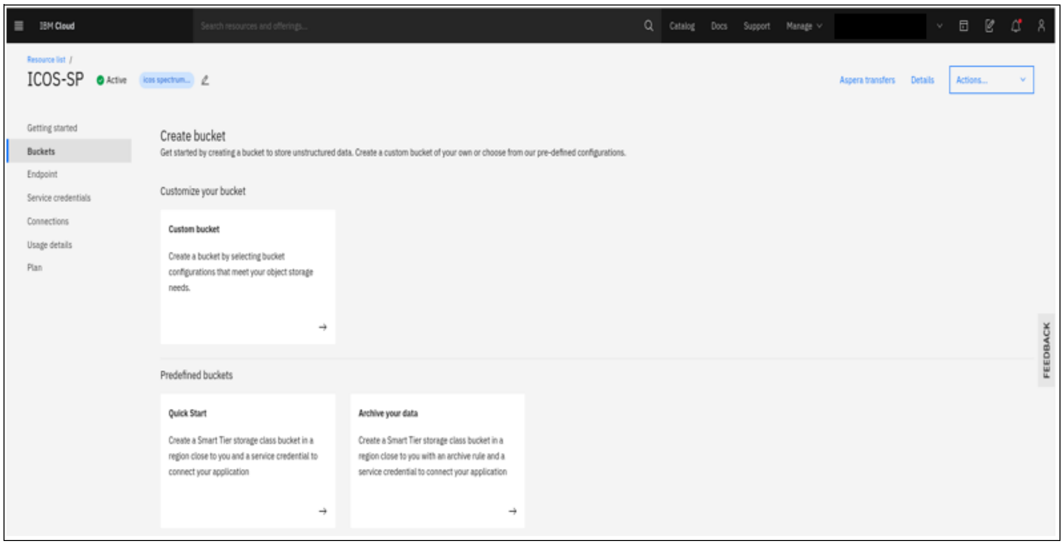
Region: Global
Plan: Standard
Service name: ICOS-SP
Resource group: Default

Figure B-1 Plan selection for IBM Cloud Object Storage

Click **Create**. The resource instance with the name ICOS-SP is created. You are redirected to the IBM Cloud Object Storage window.

3. Create a bucket in the new resource instance ICOS-SP. A bucket is a way to organize the data, where you can choose the resiliency levels and storage class options. There are also advanced optional features for setting rules and policy and extra services such as security and monitoring.

4. Select **Custom Bucket**, as shown in Figure B-2.



Create bucket

Get started by creating a bucket to store unstructured data. Create a custom bucket of your own or choose from our pre-defined configurations.

Customize your bucket

Custom bucket

Create a bucket by selecting bucket configurations that meet your object storage needs.

Predefined buckets

Quick Start

Create a Smart Tier storage class bucket in a region close to you and a service credential to connect your application

Archive your data

Create a Smart Tier storage class bucket in a region close to you with an archive rule and a service credential to connect your application

Figure B-2 Create Custom Bucket options

5. Provide the bucket parameter details. The following parameters are only for example. Provide the appropriate parameters according to your environment:

   – Unique bucket name: `icos-sp-b00001`. The name must be unique across the whole IBM Cloud Object Storage system. All buckets in all regions share a single namespace. When you create buckets or add objects, avoid using personally identifiable information (PII).

   – Resiliency: Regional (best performance). The following options are available:

     - **Cross-region resiliency**: Data is spread across several metropolitan areas.
     - **Regional resiliency**: Data is spread across a single metropolitan area.
     - **Single data center resiliency**: Data is spread across multiple appliances within a single data center.

     > **Note:** Regional and cross region buckets can maintain availability during a site outage.

   – Location: As applicable for your location.

   – Storage Class=Cold Vault. You can choose from four storage classes:

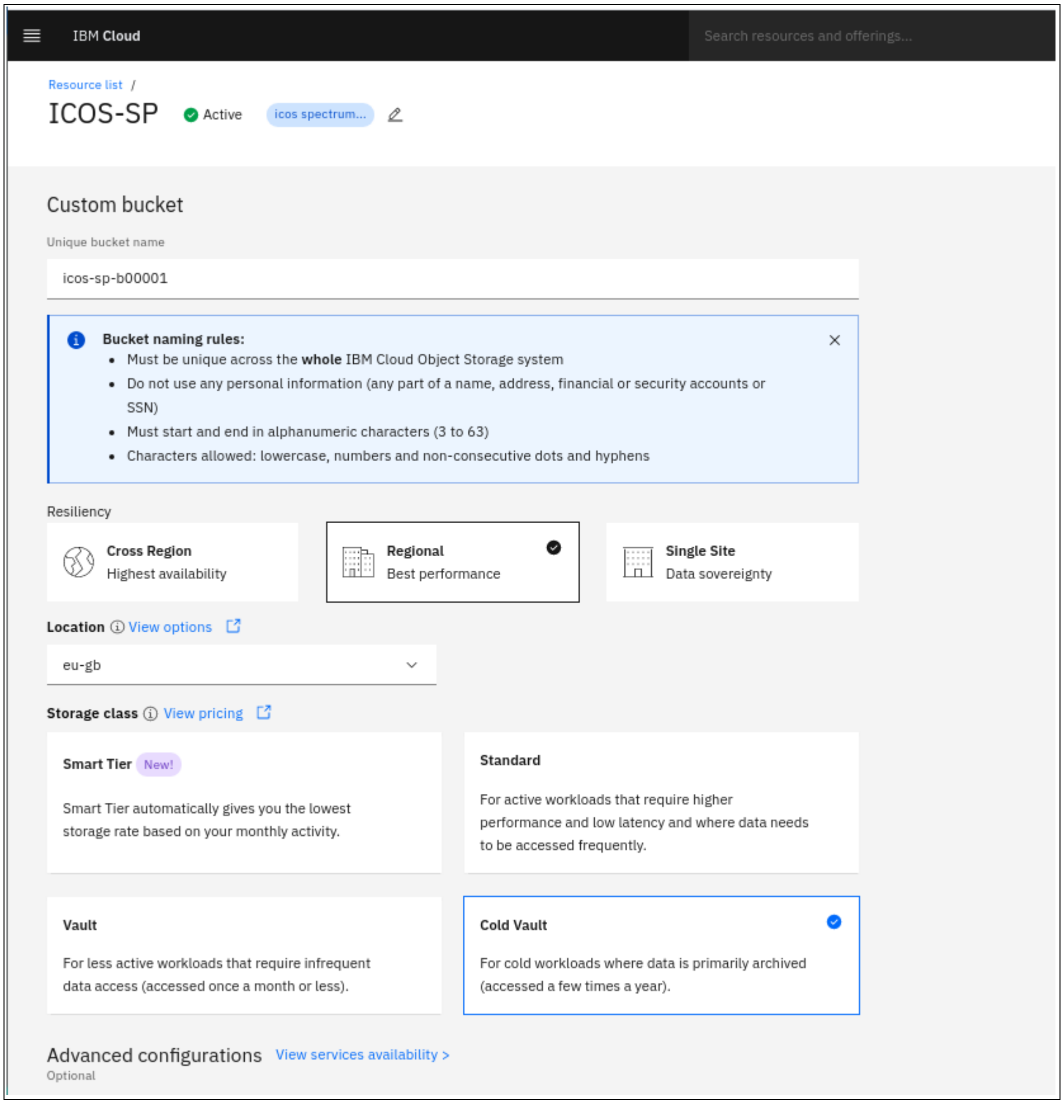
     - **Smart Tier** can be used for any workload, especially dynamic workloads where access patterns are unknown or difficult to predict.
     - **Standard** is used for active workloads, with no charge for data that is retrieved (other than the cost of the operational request itself).

- **Vault** is used for cool workloads where data is accessed less than once a month. An extra retrieval charge is applied each time that data is read. The service includes a minimum threshold for object size and storage period that is consistent with the intended use of this service for cooler, less-active data.
- **Cold Vault** is used for cold workloads where data is accessed every 90 days or less. A larger extra retrieval charge is applied each time data is read. The service includes a longer minimum threshold for object size and storage period that is consistent with the intended use of this service for cold, inactive data.

For more information about the storage classes for IBM Cloud Object Storage, see Storage classes and archive.

– Advanced services: No other extra services are selected now. If needed, they can be activated later.

Figure B-3 shows the create bucket options.



ICOS-SP ✓ Active icos spectrum...

Custom bucket

Unique bucket name

icos-sp-b00001

Bucket naming rules:
- Must be unique across the **whole** IBM Cloud Object Storage system
- Do not use any personal information (any part of a name, address, financial or security accounts or SSN)
- Must start and end in alphanumeric characters (3 to 63)
- Characters allowed: lowercase, numbers and non-consecutive dots and hyphens

Resiliency

Cross Region Highest availability	● Regional Best performance	Single Site Data sovereignty

Location View options

eu-gb

Storage class View pricing

Smart Tier New!
Smart Tier automatically gives you the lowest storage rate based on your monthly activity.

Standard
For active workloads that require higher performance and low latency and where data needs to be accessed frequently.

Vault
For less active workloads that require infrequent data access (accessed once a month or less).

● **Cold Vault**
For cold workloads where data is primarily archived (accessed a few times a year).

Advanced configurations View services availability >
Optional

Figure B-3 Create bucket options

6. Create bucket credentials for IBM Spectrum Protect connectivity to IBM Cloud Object Storage.

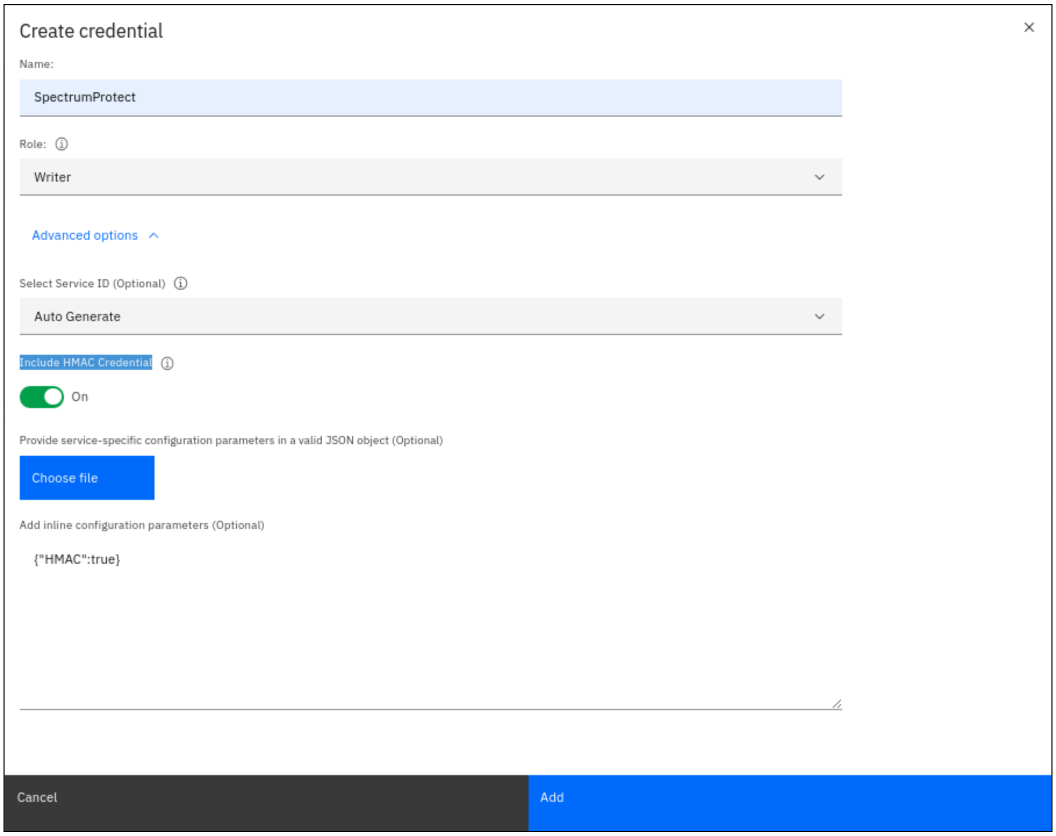
From the dashboard, go to the Resource List, select the ICOS-SP resource instance, and select **Service Credentials** → **New Credential**. Provide the required parameters (the name parameter is for example):

– Name: SpectrumProtect.

– Role: Writer.

Click **Advanced options** and enable **Include HMAC Credential**, as shown in Figure B-4.

> **Note:** HMAC Credential is a mandatory option that must be enabled to provide the required access keys that are needed for integration with IBM Spectrum Protect.



Create credential

Name: SpectrumProtect

Role: Writer

Advanced options

Select Service ID (Optional): Auto Generate

Include HMAC Credential: On

Provide service-specific configuration parameters in a valid JSON object (Optional)

Choose file

Add inline configuration parameters (Optional)

{"HMAC":true}

Cancel

Add

Figure B-4 Creating bucket credentials

7. Click **Add** (in blue as shown in Figure B-4) and the new credentials are created. Capture the details that are related to the application programming interface (API) keys that are generated. In the **Buckets** menu, go to the newly created bucket (icos-sp-b00001) under the **Configuration** menu and visualize the details. Focus on the CloudURL address, which can be either on a private or direct VPC network if your IBM Spectrum Protect server is deployed in IBM Cloud or in a public network when the IBM Spectrum Protect server is outside the IBM Cloud.

8. Write down the details for the IBM Spectrum Protect integration:

   – CloudURL.

   – bucket name.

   – access_key_id.

   – secret_access_key.

Defining the cloud container pool for SAP HANA backup

After activating the IBM Cloud Object Storage resource instance and defining the bucket and associated credentials, create the storage pool and associate a local cache directory for staging the backup data before storing it to IBM Cloud Object Storage by completing the following steps:

1. Review the IBM Cloud Object Storage provisioned resources details and credentials. Define a storage pool that is named `CLOUD_IBMS3_POOL1` for SAP HANA backup data to IBM Cloud Object Storage by using the IBM Spectrum Protect administrative client to run the following command:

   ```
   DEFine STGpool CLOUD_IBMS3_POOL1 STGType=CLOUD DESCription='Stgpool Cloud
   Container on IBM Cloud Object Storage S3' CLOUDType=S3 CLOUDUrl=<cloudURL>
   IDentity='<access_key_id>'  PAssword='<secret_access_key>'
   CLOUDLocation=OFfpremise BUCKETName='icos-sp-b00001'
   ```

2. Associate a local cache directory by defining a `stgpool` directory to the previously defined `stgpool CLOUD_IBMS3_POOL1` by running the following command:

   ```
   DEFine STGPOOLDIRectory CLOUD_IBMS3_POOL1 /tsmclouddisk1/CLOUDCACHE
   ```

   Using a local disk buffer is a best practice for optimizing the transfer of the data to cloud. For more information, see Optimizing performance for IBM Cloud Object Storage.

3. Check the `stgpool` settings by using `query stgpool` while focusing on the dedup, compression, and encryption (`default=YES`) settings, as shown in Example B-1.

Example B-1 Detailed view of cloud container stgpool

```
Protect: TSMCLOUD>q stgpool CLOUD_IBMS3_POOL1 f=d

                     Storage Pool Name: CLOUD_IBMS3_POOL1
                     Storage Pool Type: Primary
                     Device Class Name:
                          Storage Type: CLOUD
                            Cloud Type: S3
                             Cloud URL: <cloudURL>
                        Cloud Identity: <access_key_id>
                        Cloud Location: OFFPREMISE
                    Estimated Capacity:
                    Space Trigger Util:
                              Pct Util:
                              Pct Migr:
                           Pct Logical:
                          High Mig Pct:
                           Low Mig Pct:
                       Migration Delay:
                    Migration Continue:
                   Migration Processes:
                 Reclamation Processes:
                     Next Storage Pool:
                  Reclaim Storage Pool:
                Maximum Size Threshold: No Limit
                                Access: Read/Write
                           Description: Stgpool Cloud Container on IBM Cloud
Object Storage S3
                     Overflow Location:
                 Cache Migrated Files?:
```

```
                            Collocate?:
                  Reclamation Threshold:
              Offsite Reclamation Limit:
        Maximum Scratch Volumes Allowed:
         Number of Scratch Volumes Used:
           Delay Period for Cloud Reuse: 1
                 Migration in Progress?:
                   Amount Migrated (MB):
      Elapsed Migration Time (seconds):
              Reclamation in Progress?:
        Last Update by (administrator): ADMIN
                  Last Update Date/Time: 10/20/2020 03:08:34
              Storage Pool Data Format: Native
                  Copy Storage Pool(s):
                   Active Data Pool(s):
                Continue Copy on Error?:
                               CRC Data: No
                       Reclamation Type:
            Overwrite Data when Deleted:
                     Deduplicate Data?: Yes
  Processes For Identifying Duplicates:
                            Compressed: Yes
         Space Used for Protected Data:
                   Total Pending Space:
                  Deduplication Savings: 0 (0%)
                   Compression Savings: 0 (0%)
                     Total Space Saved: 0 (0%)
                        Auto-copy Mode:
 Contains Data Deduplicated by Client?:
          Maximum Simultaneous Writers: No Limit
                     Protect Processes:
               Protection Storage Pool:
         Protect Local Storage Pool(s):
              Reclamation Volume Limit:
Date of Last Protection to Remote Pool:
 Date of Last Protection to Local Pool:
          Deduplicate Requires Backup?:
                             Encrypted: Yes
                         Pct Encrypted: 0%
            Cloud Space Allocated (MB): 0
             Cloud Space Utilized (MB): 0
                           Bucket Name: icos-sp-b00001
              Local Estimated Capacity: 8,422 G
                        Local Pct Util: 0.0
                     Local Pct Logical: 0.0
                   Cloud Storage Class: Default
Remove Restored Cpy Before End of Life:
```

The local cache directory configuration for the cloud container pool can be verified by running the **query stgpooldirectory** command, as shown in Example B-2.

Example B-2 The query stgpooldirectory command

```
Protect: TSMCLOUD>q stgpooldir

Storage Pool Name     Directory                                             Access
-----------------     ---------------------------------------------         ------------
CLOUD_IBMS3_POOL1     /tsmclouddisk1/CLOUDCACHE                             Read/Write
```

4. Associate the SAP HANA backup policy domain with the destination pool in IBM Cloud Object Storage. In our case, we consider only full database backups to cloud for longer term retention on IBM Cloud Object Storage storage class Cold Vault, and the regular backups are maintained on local pools. We consider a distinct node for each type of backup that is associated with the same policy domain HANA_DOM, which contains all management classes for both profiles. The management class DATABASE_LT is used for long-term retention, and we set the destination for the cloud storage pool:

   ```
   update copy HANA_DOM STANDARD DATABASE_LT STANDARD type=archive
   destination=CLOUD_IBMS3_POOL1
   ```

   The SAP HANA database backups are bound to the archive copy group in the IBM Spectrum Protect policy domain.

5. Configure the Backint profile to use for SAP HANA long-term backup. The following example provides the stanzas that are used in the initSID.utl file for regular backup and for long-term backups. The backup of redo logs backups are not considered for long-term storage and do not change the management class.

   ```
   SERVER         TSMCOULD-HANA         # Servername, as defined in dsm.sys
   SESSIONS              4
   PASSWORDREQUIRED    NO               # Use a password
   BRBACKUPMGTCLASS    DATABASE         # Mgmt-Classes for database backup
   BRARCHIVEMGTCLASS   LOG              # Mgmt-Classes for redo log backup

   SERVER         TSMCOULD-HANA-LT      # Servername, as defined in dsm.sys
     SESSIONS              4
     PASSWORDREQUIRED    NO             # Use a password
     BRBACKUPMGTCLASS    DATABASE_LT    # Mgmt-Classes for database backup
     BRARCHIVEMGTCLASS   LOG            # Mgmt-Classes for redo log backup
   ```

   The order of the stanzas in the initSID.utl file is important. By default, the first stanza is used, which is our case reflects the regular backup profile being maintained on the IBM Spectrum Protect server local pools.

   Each server stanza from initSID.utl must have an associated Servername stanza in the IBM Spectrum Protect API system options file dsm.sys. The following stanzas provide an example where we can observe distinct node names that are used for each backup profile:

   ```
   SErvername TSMCOULD-HANA
      COMMMethod         TCPip
      TCPPort            1500
      TCPServeraddress   <IP address of the TSM Server>
      Nodename STU-S08-HANA
      PASSWORDACCESS GENERATE

   SErvername TSMCLOUD-HANA-LT
      COMMMethod         TCPip
      TCPPort            1500
   ```

```
TCPServeraddress <IP address of the TSM Server>
Nodename STU-S08-HANA-LT
PASSWORDACCESS GENERATE
```

More considerations are applied when taking different types of backups with different retentions. For more information, see “Create SAP HANA backups with different retention times” in IBM Spectrum Protect Data Protection for Enterprise Resource Planning V8.1 Documentation Updates.

6. You can perform a backup to the cloud storage profile by using the native SQL client or SAP HANA Cockpit. To run the backup by using the CLI, use the **hdbsql** client with the **tooloption** parameter as follows:

```
hdbsql -U TSM -d S08 "backup data using backint ('monthly_Nov_2020') tooloption
'stanza=TSMCLOUD-HANA-LT'"
```

C

Additional material

This paper refers to additional material that can be downloaded from the internet as described in the following sections.

Locating the web material

The web material that is associated with this paper is available in softcopy on the internet from the IBM Redbooks web server:

`ftp://www.redbooks.ibm.com/redbooks/REDP5618`

Alternatively, you can go to the IBM Redbooks website:

`ibm.com/redbooks`

Search for REDP5618, select the title, and then click **Additional materials** to open the directory that corresponds with the IBM Redpaper form number, REDP5618.

Using the web material

The additional web material that accompanies this paper includes the following files:

File name	*Description*
NISTTable.zip	Compressed spreadsheet and PDF file of National Institute of Standards and Technology table.

Downloading and extracting the web material

Create a subdirectory (folder) on your workstation, and extract the contents of the web material compressed file into this folder.

Abbreviations and acronyms

API	application programming interface
BE	Big Endian
CVE	Common Vulnerabilites and Exposures
ERP	Enterprise Resource Planning
FC	Fibre Channel
GDE	IBM Guardium Data Encryption
GRO	geographic redundancy objective
HANA	High-performance Analytic Appliance
IBM	International Business Machines Corporation
ISICC	IBM SAP International Competence Center
KMIP	Key Management Interoperability Protocol
LE	Little Endian
LPAR	logical partition
MDC	Multitenant Database Container
NIST	National Institute of Standards and Technology
NPIV	N_Port ID Virtualization.
OS	operating system
OVF	Open Virtualization Format
PII	personally identifiable information
PiT	point-in-time
ReAR	Relax And Recover
RPO	recovery point objective
RTO	recovery time objective
SAP HDB	HANA database
SAP HSID	HANA system ID
SAP HSR	SAP HANA System Replication
SAPS	SAP Application Performance Standard
SEP	Symantec Endpoint Protection
SID	system ID
SLA	service-level agreement.
TBMR	System Recovery for IBM Spectrum Protect
TCO	total cost of ownership
VM	virtual machine
VRO	version retention objective
WORM	Write Once Read Many

Related publications

The publications that are listed in this section are considered suitable for a more detailed description of the topics that are covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide more information about the topics in this document. Some publications that are referenced in this list might be available in softcopy only.

- *Deploying SAP Software in Red Hat OpenShift on IBM Power Systems*, REDP-5619
- *Red Hat OpenShift V4.3 on IBM Power Systems Reference Guide*, REDP-5599
- *Red Hat OpenShift V4.X and IBM Cloud Pak on IBM Power Systems Volume 2*, SG24-8486
- *SAP HANA Data Management and Performance on IBM Power Systems*, REDP-5570
- *SAP HANA on IBM Power Systems Architectural Summary*, REDP-5569
- *SAP HANA on IBM Power Systems: High Availability and Disaster Recovery Implementation Updates*, SG24-8432
- *SAP HANA Platform Migration*, REDP-5571
- *Software Defined Data Center with Red Hat Cloud and Open Source IT Operations Management*, SG24-8473

You can search for, view, download, or order these documents and other Redbooks, Redpapers, web docs, drafts, and additional materials at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- IBM Spectrum Copy Data Management User’s Guide

  https://www.ibm.com/support/knowledgecenter/en/SS57AN_2.2.11/com.ibm.spectrum.cdm.doc/welcome.html

- IBM Spectrum Protect Blueprints and Sizing

  https://www.ibm.com/support/pages/ibm-spectrum-protect-blueprints

- IBM Spectrum Protect Snapshot for Custom Applications

  https://www.ibm.com/support/knowledgecenter/en/SSERFV_8.1.4/fcm.unx/c_fcmu_ca_ovr_overview.html

- IBM Spectrum Protect UNIX and Linux Backup-Archive clients Installation and User's Guide

  https://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.9/client/b_ba_guide_unx_lnx.pdf?view=kc

- SAP Certified and Supported SAP HANA Hardware Directory - IBM Power Systems

  https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/power-systems.html
- SAP HANA Administration Guide

  http://help.sap.com/hana/SAP_HANA_Administration_Guide_en.pdf
- SAP HANA System Replication Guide

  https://help.sap.com/doc/c81e9406d08046c0a118c8bef71f6bdc/2.0.05/en-US/SAP_HANA_System_Replication_Guide_en.pdf
- Supported Linux distributions and virtualization options for POWER8 and POWER9 Linux on Power Systems

  https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

REDP-5618-00

ISBN 0738459690

Printed in U.S.A.