As IT managers realize the benefits of in-memory database technology, they are accelerating their plans to deploy existing SAP applications to SAP HANA, SAP’s in-memory analytics and computing platform. Although HANA’s standard savepoints and log writing protect against data loss during power failures, they do not help if the persistent storage is damaged. This white paper provides an overview of how Micro Focus® Data Protector, an SAP-certified solution, can help, and what to consider when planning or deploying it.
# Table of Contents

Backup and Restore for SAP HANA Databases ......................................................... 1
Why Back Up SAP HANA? .................................................................................. 1
Challenges of Deploying SAP HANA Backup and Recovery ............................... 2
Using SAP Backint as a Standalone Solution ..................................................... 3
Using SAP Backint with Storage System Snapshots .......................................... 3
Micro Focus Data Protector ................................................................................ 4
Making the Most of Backup Infrastructure ......................................................... 6
Infrastructure Examples .................................................................................... 7
Data Protector Monitoring and Analytics Capabilities for Predictive
  SLA Management ......................................................................................... 11
Conclusion ...................................................................................................... 13
Backup and Restore for SAP HANA Databases

SAP HANA’s standard savepoints and log writing protect against power failures, but they do not help if the persistent storage itself is damaged. Micro Focus Data Protector has a long track record of being a best-in-class solution in this context.

Why Back Up SAP HANA?

To ensure optimal performance, the bulk of SAP HANA’s database is stored in memory. However, it still uses persistent storage as a fallback in the event of a failure. During normal database operations, data is automatically saved from memory to disk at regular savepoints, and all data changes are recorded in the redo log—which is also saved from memory to disk with each committed database transaction. After a power failure, the SAP HANA database can be restarted like any disk-based database; it returns to its last consistent state by replaying the redo log recorded since the last savepoint.

SAP HANA comes with many high-availability features supported by fault-tolerant infrastructure designed to survive system node or storage system failures. But while savepoints and redo log archives do protect data against power failures, they cannot help if the persistent storage itself is damaged or when a logical error occurs. Backups are still necessary to protect against data loss caused by disk failures, human error, and due to legal requirements, for example. A backup saves the payload (the actual information) of the data area and log area to different locations, which are independent from the original source and cannot be harmed.

Regular backups:
- Protect against system and disk failures, logical damage, human error, and software bugs
- Help maintain compliance with legal requirements
- Make it possible to reset the database to a version captured at a much earlier point in time, if required
- Allow you to restore the underlying operating system and configuration.

Backups are also useful if you need to produce database copies; in this way they complement other availability strategies such as system replication or storage replication. However, SAP HANA does pose some challenges in backup environments.
Challenges of Deploying SAP HANA Backup and Recovery

SAP NetWeaver and HANA are designed for high availability; their multiple nodes and redundant copies make it easier to recover data. The main challenge is staying in sync with partner SAP nodes, especially since some recovery approaches are not designed to fully restore data in the same way. Backint, a part of BRTools, is the preferred method for restoring data, but HANA Studio and HANA Cockpit take over the scheduling and recovery in SAP HANA deployments, limiting the functionality of other third-party data protection solutions. Scripting is still available for backups, but it only prepares for storage system snapshots—it doesn’t create or manage them—so it relies on the know-how and experience of individual employees.

Bare-metal recovery of SAP HANA nodes is not a built-in feature of SAP HANA, so you would need to add it as an extra data protection solution. HANA Studio 1.0 also created hundreds of transaction log file backups per day, clogging essential backup processes.

Data Protector provides many advanced backup and recovery features to address these SAP HANA conflicts, including:

- Support for virtual and physical backup devices and appliances
- Support for storage system snapshots, mirroring, and replication technology
- Deduplication and the Storage Area Network (SAN) data transfer, to reduce the storage footprint and network load
- Support for small to large data centers, and remote offices
- Automatic use of all resources available, with multi-streaming and parallel workloads
- Support for bare-metal data recovery when using physical SAP HANA nodes
- Analysis and reporting on service-level agreements (SLAs), with information on current and past recovery point objectives (RPOs) and recovery time objectives (RTOs).

A single approach to data protection may be sufficient in homogenous environments, but most IT systems are heterogeneous; they combine physical and virtual systems, devices and vendors, as well as local and remote locations—including the cloud. Most IT specialists like the idea of standardization and consolidation. Optimizing SAP HANA protection is a good place to start, but it is just the beginning of the journey.

The two best-known approaches involve using SAP Backint—the application programming interface (API) that enables third-party tool vendors to directly connect their backup agents to the SAP HANA database—either as a standalone solution or combined with storage system snapshots. Both have their own advantages and restrictions.
Using SAP Backint as a Standalone Solution

As a baseline procedure and a key element of SAP certification, deploying SAP Backint as a standalone solution is the most common method of data protection. SAP Backint ensures that backup and recovery procedures are universally independent from the backup software vendor, while APIs that enable third-party tool vendors can give you a direct connection between backup agents and the SAP HANA database. Backint will also be familiar to any SAP administrator.

There are many advantages to using SAP Backint. For example, it:

■ Has a known and standardized interface
■ Works with every physical or virtual system platform
■ Is compatible with every underlying storage system
■ Can be part of any SAP HANA deployment.

However, SAP Backint as a standalone solution:

■ Requires streaming all full and transaction log data (traditional backup data)
■ Has a long restore time and RTO, especially for large systems.

Using SAP Backint with Storage System Snapshots

A storage system snapshot functionality can speed up your backups and shorten RTO. A snapshot is taken at the beginning of the process and later mounted to a dedicated media server, from which it can stream to any backup device. SAP Backint is fully aware of this activity and lists completed backups.

Combining SAP Backint with storage system snapshots can:

■ Speed up the snapshot procedure when backing up and restoring
■ Improve your overall RTO.

However, this approach:

■ Relies on a disk-based system, which slows down over time
■ Is more expensive, because you need to acquire snapshot licenses and additional disk capacity
■ May only work with single-tenant databases.

“Data Protector is a comprehensive, SAP HANA-certified solution for maintaining business continuity in your SAP HANA environment.”
Although snapshots are no substitute for a full backup, they can assist you in the backup process. If the database is very large and long-term retention is not necessary (assuming you only need the last runtime minutes or hours) you may not require “traditional” backups that use SAP Backint alone.

With this in mind, the decision comes down to the following questions:

- Do you want to run a separate solution for snapshot management and general data protection, and another for virtual machines (VMs)?
- Many of today’s IT specialists still rely on physical tape as last line of defense. Who in your organization will support the existing tape and platform with barcodes and import/export functionality?
- How will the media migration from any source format to any destination format—and replication between data centers—be handled?

All of these questions arise when you consider how SAP HANA can protect data, making it relevant to consider a dedicated enterprise-level data protection software suite.

**Micro Focus Data Protector**

As an enterprise-class backup and recovery solution, Data Protector provides reliable, comprehensive data protection and high availability for fast-growing business data. It offers an extensive backup and restore functionality, specifically tailored for enterprise-wide, distributed environments. Its features include:

- Comprehensive enterprise data protection
- A single, scalable, federated deduplication solution
Centralized management for backup and recovery, media management, replication, and disaster recovery

A high-performance backup solution that orchestrates hundreds of backup devices and data streams in parallel using SAN, iSCSI, and LAN

Automated backup and recovery driven by the application owner

An SAP-certified backup solution that supports BRTOOLS, Backint and so on

Automated, cost-effective disaster recovery.

Data Protector offers predictive analytics which monitor and track Service Level Agreements to provide valuable insights to forecast and avoid outages. SAP HANA environments are typically mission critical, hence require management and real-time monitoring of service levels agreement (SLAs).”

Data Protector addresses hybrid IT requirements by bridging the gap between physical, virtual, and cloud systems. Due to its scalability and capacity, Data Protector can protect SAP HANA as well as all other enterprise applications. Performance tuning is built in and covers all known storage industry standards. For databases that can be read with many streams in parallel and that use the appropriate number of backup devices, Data Protector auto-tunes for multistreaming and/or multiplexing. It also organizes backup replication using appliances such as HPE StoreOnce and EMC Data Domain, incorporating deduplicated data payloads.
Making the Most of Backup Infrastructure

Data Protector handles multiple tasks involving physical and virtual backup devices, including deduplication, replication, and media migration. Sometimes those tasks are predefined by the fact that you already have certain backup devices or have made certain strategic decisions.

The following are some best practices we have learned from previous customer installations:

- Despite what some industry experts have predicted, tape is not dead. In cases requiring fast single-stream performance, tape (Linear Tape Open, or LTO) can easily outperform virtual backup tools. It is not always possible to force an application to create multiple streams; even SAP HANA needs a certain database size before parallel streams are available. So, for pure database backups, tape is still a very good option.

- Virtual tape appliances are best for smaller chunks of data like log backups, and backups with a high number of incoming streams. Most of these virtual tools offer deduplication so they may be sufficient where only backup appliances are in use, although it is important to make sure there are enough spindles to take the constant load of incoming data.

- You can replicate backup data to another data center using the “Object Copy” feature in Data Protector. Data Protector can control appliance-based replication (using HPE StoreOnce or EMC Data Domain) where the data stays deduplicated, or it can make a full copy of any other backup object to another location.

- Data Protector can stream SAP HANA data directly from a HANA node to a fiber channel–connected backup device. This ensures LAN-less backup and recovery, and full-bandwidth availability for users connected to SAP HANA.

- Data Protector allows backup infrastructure to be shared with any other platform and backup tool, using Network Data Management Protocol (NDMP) and other protocols. There is no need to assign dedicated resources to support SAP HANA data protection.
Infrastructure Examples

A typical infrastructure setup could look like this, with a physical or virtual HANA node backed up by Backint and the Data Protector integration agents.

Figure 3. A typical SAP HANA backup infrastructure setup

The data flow starts by reading from SAP HANA and is either streamed directly to a backup device via fiber channel or SAS (if a physical HANA node is used), or via a backup media server using LAN (if a virtual HANA node is used, or for general consolidation purposes).

Storage snapshots help reduce the backup duration and RTO with help from the underlying disk system infrastructure. SAP Backint can set up SAP HANA for this procedure—preparing and tracking the snapshot creation, rather than executing the activity itself. The actual workflow depends on the infrastructure in place. The examples below show a physical deployment on the left (for completely local performance) and a more virtual deployment on the right, where the nodes are deployed as VMs or containers and there is no storage system directly attached.
Snapshot procedures follow the same workflow, to a certain extent. With physical volumes attached, a snapshot is taken at the storage system level and is delivered to a dedicated backup host. You can then retain multiple snapshots for restore purposes.

In a virtual or cloud-based scenario, the disk volumes are not directly presented to a VM or container; instead, the general storage capacity is shown to the underlying cloud or hypervisor component. Then, instead of creating storage system snapshots, the hypervisors create software snapshots of virtual disks or cinder volumes. These “soft snaps” are mounted to a dedicated backup VM or container, and data flows from here. Potential backup targets include an open source object storage Swift store, or a cloud-based or VM backup appliance. Additional OpenStack tools like Freezer or Karbor can facilitate API access to cloud-based data protection.

“In the event of dual data center deployments, Data Protector makes it easy to run and organize the replication process between data centers.”

Now that we’ve talked about attaching disks—either physically or virtually—we need to discuss how to reach a backup device’s full potential. If you have backup hardware already, you can use it here. In the event of dual data center deployments, Data Protector makes it easy to run and organize the replication process between data centers, and to confirm that a direct recovery can be performed using available copies or replicas. It can be a good idea to offload some data to tape for compliance reasons, or just to clear backup disk capacity and boost performance.
The diagram above also demonstrates the multiple levels of protection available. SAP HANA, the servers, and the disk storage generally represent current data availability; if one goes down, another will take over. But as mentioned above, if a logical issue occurs, the damaged data may be replicated to all elements in the system. SAP savepoint recovery can help to some extent, but in some cases this process may stall too. This is when your backup and recovery solution kicks in. And since Data Protector manages backup objects independent of the operating system platform, device type, and connection, you will be able to recover your data even if the infrastructure has changed over time and the restore path differs from the backup path.

You may want to avoid LAN-based (especially user LAN) backup I/O, which can be slow to complete, impacting productivity. Data Protector allows you to set up a “Media Agent” on the SAP HANA node, which allows the node to write directly to any supported backup device. If you have SAN infrastructure available, it can read the backup I/O from the disk and stream it to a backup device via SAN, iSCSI, SAS, or similar. This setup also allows for redirected restores following a failure, if you want to restore data to a temporary location while the node is being repaired.

Figure 5. Examples of backup and recovery workflows

“Since Data Protector manages backup objects independent of the operating system platform, device type, and connection, you will be able to recover your data even if the infrastructure has changed over time and the restore path differs from the backup path.”
Sometimes there is no option but to move a backup over LAN. As with cloud-based transfer, there is no need for direct SAN access, as long as you have access to block or object storage in the form of Cinder, Swift, and other OpenStack modules. Alternatively, you may be using a Hypervisor for VMs that doesn’t offer direct SAN access.

In these situations, you can use source-side deduplication to transfer only unknown blocks to a target like HPE StoreOnce (Catalyst) or Dell EMC Data Domain (DD Boost). Data Protector also offers a software-only version of a StoreOnce appliance with full compatibility, for smaller implementations such as at remote office sites.
“Data Protector offers predictive analytics which monitor and track Service Level Agreements to provide valuable insights to forecast and avoid outages.”

Data Protector Monitoring and Analytics Capabilities for Predictive SLA Management

Data Protector offers predictive analytics which monitor and track Service Level Agreements to provide valuable insights to forecast and avoid outages. SAP HANA environments are typically mission critical, hence require management and real-time monitoring of service levels agreement (SLAs). Data Protector’s monitoring dashboard allows SAP HANA admins to define and manage and track application recovery point and time objectives (RPOs and RTOs) with alerts and intelligent recommendations to ensure that availability needs can be met consistently.

This combination scenario also requires more specific storage design, as some storage systems lack the capacity or horsepower to keep or manage such a large number of snapshots.

Figure 7. Deduplication data paths

Data Protector is certified by SAP and you’ll find all the individual statements on the SAP website.

SAP® Certified Integration with SAP HANA®

Note that HPE Software recently became part of Micro Focus. SAP certifications do not yet reflect this change.
For most enterprises, tracking, managing, and meeting SLAs is a key requirement, so any data protection solution must include the tools required to measure overall backup and restore quality and success. Data Protector displays live backup data on summary dashboards, drawing on analytics and office format output. You can also set up monitors that check on SLAs and other key metrics, so administrators can keep track of performance using standardized or customized reports.

Data Protector can also help identify bottlenecks and optimize your backup operations. If you are running hundreds of backup jobs each day—or more—it can be difficult to ascertain which backup jobs failed and why. A backup job failing to complete within the required timeframes also counts as a failure. And since SAP is all about enterprise resource planning, you also need to be able to predict your future storage capacity needs, backup performance results and backup runtimes. Data Protector can provide this information on demand, or as a regular output sent by email or other convenient formats. The results can be filtered according to backup system, tenants, devices, applications, and other factors, giving you real-time information not only about what has actually happened, but also what has been planned, so you have an accurate audit trail if needed.
Conclusion

Data Protector is a comprehensive solution for maintaining business continuity in your SAP HANA environment. If you have been tasked with protecting your SAP HANA applications, this may be a good opportunity to think about protecting other applications and VMs on your business continuity to-do list. While many enterprises have multiple solutions for individual data protection processes, this may be your chance to boost efficiency and productivity by standardizing and consolidating your data protection tasks. The cost savings start with minimizing the number of tools deployed, which also simplifies and streamlines administration tasks.

SAP HANA users can deploy Data Protector as a universal backup solution simplifying and standardizing backup and recovery for filesystems and applications across heterogeneous environments—physical, virtual, and cloud, and storage platforms, and operating systems. Data Protector is designed to seamlessly scale from a small, single system deployment to thousands of systems across core data centers and remote sites, and backup to disk, tape, and cloud targets. Built on an adaptive architecture that combines analytics, automation, and built-in security, Data Protector allows you to reach across applications and infrastructure silos and automate the full range of business continuity processes, eliminating multiple products and manual error-prone actions.

Learn More At
Micro Focus Data Protector
Micro Focus Monitoring and Analytics