These days the world operates in real-time all the time. Whether in making ticket purchases or getting the best deal from online retailers, data is expected to be up to date with the best information at your fingertips. Businesses are expected to meet this requirement, whether they sell products or services. Having this real-time, actionable information can dictate whether a business survives or dies. In-memory databases have become popular in these environments. The world’s 24X7 real-time demands cannot wait for legacy ERP and CRM application rewrites. Companies such as SAP devised ways to integrate disparate databases by building a single, super-fast uber-database that could operate with legacy infrastructure while simultaneously creating a new environment where real-time analytics and applications can flourish.

SAP HANA is a growing and very popular example of an application environment that uses in-memory database technology and allows the processing of massive amounts of real-time data in a short time. The in-memory computing engine allows HANA to process data stored in RAM as opposed to reading it from a disk. At the heart of SAP HANA is a database that operates on both OLAP and OLTP database workloads simultaneously. To overcome the volatility of server DRAM, the HANA architecture requires persistent shared storage to enable greater scalability, disaster tolerance, and data protection.

SAP HANA is available on-premises as a dedicated appliance and/or via best-in-class components through the SAP Tailored Datacenter Integration (TDI) program. The TDI environment has become the more popular HANA option as it provides the flexibility to leverage legacy resources such as data protection infrastructure and enables a greater level of scalability that was lacking in the appliance approach. Hewlett Packard Enterprise (HPE) has long been the leader in providing mission-critical infrastructure for SAP environments. SUSE has long been the leader in providing the mission-critical Linux operating system for SAP environments. Micro Focus has long been a strategic partner of HPE, and together they have leveraged unique hardware and software integrations that enable a complete end-to-end, robust data protection environment for SAP. One of the key value propositions of SAP HANA is its ability to integrate with legacy databases. Therefore, it makes the most sense to leverage a flexible data protection solution from Micro Focus and HPE to cover both legacy database environments and modern in-memory HANA environments.

In this solution brief, Taneja Group will explore the data protection requirements for HANA TDI environments. Then we’ll briefly examine what makes Micro Focus Data Protector combined with HPE storage an ideal solution for protecting mission-critical SAP environments.

STORAGE AND DATA PROTECTION REQUIREMENTS FOR SAP HANA

Real-time data access and analysis drives faster, better decision-making. SAP HANA performs real-time analysis on data from multiple sources including SAP HANA, legacy systems, big data repositories, and external sources. Because SAP HANA solutions often coexist with other on-premises infrastructure, SAP TDI has become a popular approach for HANA deployment. TDI environments allow businesses the flexibility to leverage existing infrastructure, and data protection is one area where this leverage makes sense. SAP HANA has unique persistent storage and data protection requirements even though the primary database is in-memory. We will briefly describe the overall TDI environment with the focus of
the paper being on the data protection elements. Figure 1 shows the basic architecture of the scale-out HANA environment with the storage tier highlighted. SAP HANA can be deployed both in a single node environment (scale-up) or multi-node environment (scale-out). The scale-out TDI environment requires a more robust enterprise storage capability and will be the focus of this paper.

In multi-host environments, the database tables are distributed across RAM on multiple servers. Multi-host environments are configured in an N + 1 topology where active hosts accept and process database requests. A standby host is a passive component with all database services running, but no data in RAM. The standby host waits for a failure of an active host then takes over its role.

**All-flash Arrays are Ideal for SAP HANA Environments**

The in-memory capacity of each host dictates the shared storage capacity requirements. The total number of active hosts in the environment dictates the performance requirement of the storage. All-flash Arrays (AFAs) are ideal for both in-memory environments and OLTP/OLAP databases since they create the highest overall performance within a relatively small SSD footprint. HPE positions their flagship 3PAR AFA storage as an ideal shared storage device for SAP HANA environments. Micro Focus Data Protector automates the HPE 3PAR Virtual Copy feature to enable advanced data protection in HANA environments. Figure 2 outlines how each node will structure the data within a 2 + 1 configuration for a shared storage device such as HPE 3PAR.

The data protection advantages of AFAs in HANA environments extend even further, as the following benefits illustrate.

**Key benefits of all-flash deployments for Data Protection:**

- **Reduced HANA backup times:** Best practice is to backup to another external shared storage device. However, this operation puts a heavy read load on the system. An AFA with snapshots can handle this workload more efficiently and faster than spinning media on an active system. It is still recommended to use a secondary device in the case of a DR situation.
• **Reduced host auto-failover times:** A standby host is configured into the system and will take over an active host that fails. Flash enables this process to happen faster since the DB load from disk to memory along with the replaying of logs happens much faster.

• **Reduced HANA startup times:** During boot up, each HANA node must read from a centrally shared storage repository. The resulting boot storm puts a heavy read burden on the array, increasing startup times. Flash helps to minimize startup times, and also enables database logs to be replayed much faster than with spinning media in the event that hosts power off unexpectedly.

**Capacity Requirements for SAP HANA**

SAP provides a very prescriptive minimum capacity allocation needed to build an SAP HANA scale-out configuration. The following table outlines the capacity requirements for each of these directories on a per-host basis. RAM refers to the entire amount of memory required to host HANA in memory. Different HANA application requirements may dictate different RAM requirements per host. Some vendors simplify RAM to be the total system memory installed in the host so storage capacity will never be depleted.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Minimum Requirement (single node)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>60 GB</td>
<td>Operating system plus SAP files</td>
</tr>
<tr>
<td>/hana/data</td>
<td>1.2x net disk space for data</td>
<td>Net disk space is calculated using SAP tools across all the nodes. Some vendors simplify this requirement by using 1.2 x RAM per node.</td>
</tr>
<tr>
<td>/hana/log</td>
<td>[systems ≤ 512 GB] = 1/2 x RAM</td>
<td>Typically simplified to system memory size.</td>
</tr>
<tr>
<td></td>
<td>[systems &gt; 512 GB] = 512 GB</td>
<td></td>
</tr>
<tr>
<td>/hana/shared</td>
<td>1 x RAM per 4 nodes</td>
<td>For 12 nodes, this would be 3 x RAM</td>
</tr>
<tr>
<td>Backup</td>
<td>Sum of data and log directories</td>
<td>Backups should be stored on a separate storage device. SAP recommends 7x RAM to cover this.</td>
</tr>
</tbody>
</table>

A good rule of thumb for SAP HANA capacity would be 2.5 times RAM per host for primary shared storage and another seven times RAM for secondary backup storage.

**Options for SAP Backup and Recovery**

Protecting the SAP HANA environment in the event of corrupted data, hardware failure, or other natural disaster is an important part of the overall storage design. SAP HANA offers a variety of ways to accomplish this task depending on the business-criticality of the environment. In this section of the paper, we take a closer look at some of the data protection schemes offered by SAP HANA.

SAP HANA provides three primary ways to backup the multi-node environment (described below). Data backups can be scheduled or triggered manually. The goal of a backup is to copy the database savepoint plus the associated log segments to a physically separate storage device. The speed of the backup process and speed of the recovery time are dictated by the organization’s Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

**External Shared Filesystem:** In this scenario, all nodes will copy their database savepoints and redo logs to a centralized shared filesystem over NFS. This approach is the simplest of the backup options. However, the more nodes you have, the more RTO and RPO can be impacted by the performance of the shared filesystem when processing multiple backup streams in parallel. The benefit of this approach is
that it is simple to configure, does not require the purchase of additional backup software to implement, and is controlled by SAP HANA.

**BACKINT Interface:** In this scenario, the backup process is handled by third-party backup tools such as Micro Focus Data Protector. Through BACKINT integration, the third-party software is responsible for transferring the data savepoints and log segments over to another backup device. The benefit of this solution is that it enables advanced backup techniques such as array-based snapshots with separate data movement to tape or deduplication-based appliances. If done properly, the impact of backup is minimized on the primary SAP HANA nodes, and array-based snapshots can reduce RPO and RTO.

**Native Array-based Snapshots:** In this scenario, SAP HANA supports a storage array's native snapshot to recover the previous versions of the database. Integration can be accomplished through scripting provided by the array vendors or, if supported, through native SAP integration. The benefit of this solution is that RTO is reduced due to the inherent speed of mounting an older version of the data and replaying the redo logs. We recommend an approach combining array-based snapshots controlled by BACKINT integrated backup software with an offload to a second storage device as the best way to cover the broadest range of potential hardware and software failures.

Figure 7 from SAP gives a high-level view of the backup process.

---

**Figure 7: Overview of the backup flow for SAP HANA**

---

**HPE and Micro Focus Approach to SAP HANA Data Protection**

The goal of SAP HANA TDI is to leverage existing best-in-class, on-premises components, and our research indicates SAP HANA instances will coexist with other on-premises mission-critical applications. We recommend that customers integrate SAP HANA data protection into existing enterprise-grade data recovery solutions. HPE combined with Micro Focus Data Protector provides an ideal data protection solution due to the broad compatibility and unique value-added integrations these companies have brought together with their respective hardware and software capabilities. Micro Focus Data Protector provides an enterprise-grade data recovery solution and has a rich history of supporting a wide variety of mission-critical application environments. A companion product called Micro Focus Backup Navigator provides IT staff with a global-wide interactive dashboard that enables analytical insight and adaptive intelligence, helping IT staff to maintain SLA compliance of backup and recovery operations. Micro Focus data protection solutions enable unique SAP HANA backup requirements to fit seamlessly into existing operations.

HPE and Micro Focus have partnered together to provide the solutions that support each of the SAP HANA data protection schemes. Micro Focus and HPE also provide extensive integration into the SAP management console itself to allow backups and restores to be triggered automatically from the SAP HANA Studio interface. At the center of HPE data protection solutions is HPE Recovery Manager Central (RMC). This software is capable of interacting with multiple HPE 3PAR StoreServ arrays and HPE
StoreOnce backup devices through a rich set of APIs. Micro Focus Data Protector integrates with these APIs to take advantage of advanced HPE storage features. The following table summarizes the currently recommended approach for each of the main data protection approaches described previously.

<table>
<thead>
<tr>
<th>Data Protection Approach</th>
<th>HPE and Micro Focus Solution(s)</th>
<th>Benefits/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple Backup to an External FileSystem</td>
<td>Backup to HPE StoreOnce deduplicating backup appliance using NFS</td>
<td>Low-cost disk-based backup appliance with deduplication and a broad range of capacity and price points available.</td>
</tr>
<tr>
<td>BACKINT: Micro Focus Data Protector</td>
<td>Data Protector provides plug-ins that fully support the SAP HANA Studio environment.</td>
<td>Enables integration into enterprise-wide data protection management solutions. HPE Tape support is also available through Micro Focus.</td>
</tr>
<tr>
<td>BACKINT: HPE StoreOnce Catalyst Plug-in</td>
<td>HPE integrates StoreOnce Catalyst for use by Micro Focus Data Protector and other third-party software.</td>
<td>Enables source-based dedupe on each HANA node for higher performance and lower network bandwidth utilization in conjunction with StoreOnce appliances.</td>
</tr>
<tr>
<td>BACKINT: HPE Recovery Manager Central Plug-in</td>
<td>HPE RMC manages native snapshot integration of arrays and native direct backup between 3PAR and StoreOnce. RMC also enables snapshot management for integration with Micro Focus Data Protector.</td>
<td>Enables many advanced data protection techniques to be coordinated for the multiple HPE storage products.</td>
</tr>
<tr>
<td>Array-based Snapshots</td>
<td>HPE 3PAR Virtual Copy</td>
<td>Enables array-based protection and is supported natively in SAP HANA using HPE RMC.</td>
</tr>
<tr>
<td>Array-based Replication</td>
<td>HPE 3PAR Remote Copy</td>
<td>Enables array-based replication and is managed in SAP HANA using HPE RMC.</td>
</tr>
</tbody>
</table>

The following attributes make Micro Focus Data Protector with Backup Navigator an ideal solution for HPE SAP HANA environments.

- **SAP HANA Application-consistent Recovery**: Micro Focus supports online application-consistent backups and point-in-time restore for SAP HANA environments. Also, Micro Focus supports SAP/R3 environments and single-node HANA appliances.

- **Protects the entire environment**: Micro Focus Data Protector backs up the SAP HANA system elements overlooked by the native backup tool. Missing elements not backed up by native tools include the database config files and the entire host OS environment. This capability enables Data Protector to support bare metal recovery of HANA nodes, which will greatly improve RTO and reduce exposure to multi-node hardware failures.

- **Heterogenous Flexibility**: Micro Focus Data Protector has a rich history of supporting multiple enterprise backup environments. By seamlessly fitting into an SAP HANA environment, Micro Focus Data Protector enables SAP HANA to fit into an existing customer's backup infrastructure. This
flexibility allows SAP HANA customers to benefit from other backup infrastructure already on-premises, such as backup appliances, media servers, and even tape-based systems.

- **Enterprise-wide monitoring and analytics:** Micro Focus Backup Navigator provides an interactive dashboard that gives analytical insight and adaptive intelligence to maintain backup and recovery operations. IT staff can immediately identify inefficiencies within the backup operations such as the unbalanced use of backup resources and uncover failures before they are exposed in the recovery process. With adaptive intelligence, the highest priority backup jobs are ensured completion to meet given service level agreements.

- **Storage Network Bandwidth Optimization:** Micro Focus Data Protector, when combined with HPE StoreOnce, provides options to minimize storage network bandwidth, such as through the use of source-side deduplication. Since multi-node HANA is a scale-out architecture, this enables the backup administrator to balance storage area network usage versus CPU usage to optimize the system overall. Micro Focus Data Protector can also control low-bandwidth HPE 3PAR snapshot direct offload copy to a StoreOnce system.

**TANEJA GROUP OPINION**

The world’s 24X7 real-time demands are fueling the popularity of super-fast in-memory databases such as SAP HANA. Often overlooked in such environments, though, is the critical role of data protection solutions. Host and system failover techniques are very important but not sufficient to protect these mission-critical environments. There are many other needs for maintaining point-in-time copies of the environment. Viruses, ransomware, software defects, and human errors are just some of the reasons for continuously backing up these mission-critical environments. Additionally, data protection solutions are a great way to keep long-term archives for compliance related reasons or maintain copies for test and development purposes. We believe Micro Focus Data Protector combined with HPE infrastructure provides an ideal data protection solution due to the broad compatibility and unique value-added integrations these companies have brought together for SAP environments.

Micro Focus and HPE are working together on numerous mission-critical data protection solutions such as those we have highlighted in this Solution Brief. While the solutions highlighted here work on any SAP HANA environment, it’s noteworthy that over 90% of all SAP HANA workloads worldwide run on SUSE Linux, which SAP uses to run their business and recommends for SAP HANA. We expect these strategic partnerships to remain strong in the future as the companies continue to work together on a broad range of solutions.

---

**NOTICE:** The information and product recommendations made by Taneja Group are based upon public information and sources and may also include personal opinions both of Taneja Group and others, all of which we believe to be accurate and reliable. However, as market conditions change and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. Taneja Group, Inc. assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors that may appear in this document.