By Rick (Arkadi) Litvin
IRNITU, Director, International R&D Department of Applied Cloud & Data Center Technologies

Cloud Backup and Storage Expert Tips: SAP Data Protection Considerations

SAP provides enterprise application software and software-related services worldwide. It operates through the On-Premise and Cloud segments. The company is the world's leading provider of business software, including SAP HANA, a subscription based enterprise cloud, SAP CRM, SAP ERP, SAP Product Lifecycle Management, SAP Supplier Relationship Management, SAP Supply Chain Management applications; mobile solutions comprising enterprise mobility management, mobile apps, and SAP Mobile Platform; database and technology solutions, including application development and integration, and database solutions; and cloud solutions.

Due to such broad spectrum of various SAP products and services, comes complexity and challenges for SAP customers to determine the best way to manage and protect critical enterprise data and information in SAP and non-SAP systems and to meet strict Service Level Agreements (SLAs).

A brief history lesson in SAP data protection area of the product:
SAP created Backint as a backup application in the days when Oracle was the most popular Database in the industry. At that time, SAP had no real internal backup application yet, and Oracle RMAN was not created. SAP maintained Backint as a backup application, but it only supported SAP running on Oracle, HANA, and MaxDB. Rather than coding Backint to support other database products that already had established internal backup applications, such as MS-SQL or DB2, SAP just recommended the use of those internal backup applications.

The SAP backup tool quiesced the database for data consistency, copied all necessary files to the backup devices, including all database logs, and recovered it when necessary. At a later time, SAP backup application (Backint) was transitioned to SAP BR-tools. Despite the fact that 'SAP BR-tools' package is fully integrated into SAP's NetWeaver application server and management stack, it required a lot of scripting and customization to leverage complete and fully functional BR-tool integration.

To develop and implement robust data protection strategy for SAP products, one should have a good understanding of various SAP-related components and required SLA, RPO & RTO.

The following SAP components should be considered as an integral part of data protection scenario:

SAP Database objects (files) - Tablespace files, Database control files, Online redo logs & Offline redo logs

SAP Database objects are located within SAP database server. As indicated above, the database objects protection requires backup of database data files [tablespace backup is a backup of the database files that constitute the tablespace], database control files, online or offline redo logs.

SAP Non-database files - SAP binary, Database Binary (e.g., Oracle binary), SAP Configuration files

SAP non-database files are database executable, SAP executable and SAP configuration files. These data, predominately, only changes when profile parameter changes or after an upgrade/patch of system. Indeed, all these files do require data protection as well, but data protection approach for these files will be different from data protection approach for SAP Database objects (files).

Based on your company's objectives, required SLA, RPO & RTO etc., various data protection scenarios can be designed and implemented, e.g., traditional (streaming) backups, snapshot-based backups or combination of both traditional backups and snapshot-based backups.

There are a number of commercial backup/data protection products that do offer fairly tight integration with various SAP products. One of the key backup/data protection products with the focus on SAP are Symantec NetBackup, CommVault Simpana and HP Data Protector. There are comparative newcomer companies such as Actifio, Catalogic etc. that do offer their own, unique way of data protection.

In case of SAP backups, one should pay a close attention to supportability by corresponding backup vendor(s) of various permutations of different SAP database types, OS types and corresponding DB/OS version / patch numbers. Below, please see an example of supportability matrix by one of the backup' vendors (this example is provided only for the purpose of demonstration; as to what are different variations one should consider to make sure that their solution will be supported by specific backup vendor).

DB Version	Windows	SUSE	AIX	HP-UX	RHEL	Solaris
SAP on ORACLE [Kernel version of SAP (7.2)]	2008 R2, 2008, 2003	11	7.1, 6.x	11.31	5.x, 6.0, 6.1, 6.2, 6.3	11, 10, 9
SAP on ORACLE [Kernel version of SAP (6.x)]	no longer supported	no longer supported	no longer supported	no longer supported	no longer supported	no longer supported
Oracle 12c	2012 R2, 2012, 2008 R2, 2008	not supported	not supported	not supported	6.4	not supported
Oracle 11g R2	2008 R2, 2008, 2003	11, 10	7.1, 6.x	11.31	5.x, 6.0, 6.1, 6.2, 6.3, 6.4	11, 10
SAP on MaxDB [Kernel version of SAP (7.6)]	2003	10, 9	6.1	11.31, 11.23	5.x	not supported
SAP on MaxDB [Kernel version of SAP (7.7)]	2008, 2003	11, 10, 9	7.1, 6.1	11.31, 11.23	5.x	not supported
DB2 (10.5)	2008 R2	11, 10	7.1	11.31	6.0, 6.1, 6.2, 6.3, 6.4	not supported
SQL 2012	2012 R2, 2012, 2008 R2, 2008	n/a	n/a	n/a	n/a	n/a
Sybase (15.7)	2008 R2, 2003 R2	11	7.1	11.31	6.0, 6.1, 6.2, 6.3, 6.4, 6.5	10
HANA	n/a	11.1, 11.2	n/a	n/a	n/a	n/a

SAP-Support-Matrix-by-Backup-Vendors

Click to download

When considering incorporating snapshot-based backups in overall data protection scenario, additional supportability metrics from storage vendor(s) should be taken into consideration, such as storage array type, OS type/version # of specific storage system etc. E.g., for Catalogic product, it doesn't matter what mix of primary storage is in place, but secondary storage was based on NetApp technology until recently. A few months ago, IBM Storage was introduced as secondary storage target as well, but only for VMware environments.

Catalogic can protect SAN- and NAS-based primary storage data residing on any disk vendor array (NetApp, EMC, Hitachi, IBM, Dell, HP, etc.), direct-attached storage and internal drives, such as boot disks, but secondary storage should be based on NetApp and IBM (VMware environment only) storage.

Snapshots-based backup approach enables significantly faster backups than any traditional streaming backup approach can provide. Traditional backup system cannot provide aggressive Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) as snapshots-based backup.

The key functionalities of snapshot-based backups one should consider are:

- Scheduling storage-based snapshots across multiple storage arrays, applications and VM virtual servers
- Ability to catalogue these snapshots for full volume or granular file recovery
- Quick search and recovery of individual files across collection of indexed snapshots
- Quickly create and retain application aware snapshots

It's important to note SNIA's [Storage Networking Industry Association] definition of snapshot-based backup. Per SNIA … a snapshot is not really a backup until it has been replicated to another storage

system. Since a snapshot is a virtual copy of the data, if something happens to the volume this snapshot is associated with, the snapshot of the volume will be of no use unless it is copied to another volume via replication.

Today, key enterprise backup vendors (e.g., Symantec NetBackup, CommVault Simpana and HP Data Protector) with good integration for SAP solutions do offer within their products an ability to enable both traditional streaming backup and snapshots-based backups. However, not all snapshot-based backup systems (along with other backup functionalities) from different vendors are alike and should be closely examined / tested to ensure the best fit for your company's objectives in data protection for SAP-based products.

The key backup requirements for SAP production systems should be:
- Frequent backups via a scheduled backup
- Online database data backup
- Database transaction log backup
- Point-in-time database recovery
- Closely synchronized file system and database backups

For SAP production systems, a regular restore of backups to a separate system is strongly recommended, so that:
- Restore and recovery procedures and Service Level Agreement (SLA) objectives can be validated
- Restored data can be checked for consistency

About the Author: Rick Litvin is Director, International R&D Department of Applied Cloud & Data Center Technologies at IRNITU. For more than a decade, Rick was Storage Architect / Manager, Data Center Services at NTT America, where he designed NTT's storage & recovery solutions. Rick led Virtustream as VP, Global Storage Architecture and Engineering and also held a number of senior positions at a number of companies, including EMC. He has been awarded a number of US patents for data storage systems technologies. Rick can be reached via email: alitvin@sanasventures.com and his LinkedIn profile can be viewed at **https://www.linkedin.com/in/arkadilitvin**