CIO STORY™
The Enterprise Gateway
APRIL 2017
www.ciostory.com

SAP
Special Edition

REVEALING THE UN-USUAL SUSPECT
IN DIGITAL BUSINESS INTEGRATION

Improving Visibility of Application Usage

Unleash full business potential by implementing GRC

CIO STORY 25 Most Powerful SAP Tech Providers 2017

SAP HANA is the New Crown Jewel in the SAP Landscape Frequently it Goes Unprotected

It is hard to imagine the British Crown Jewels not properly protected from disaster or human attack. Every risk these legendary jewels face has been evaluated, and procedures are in place in case of disaster.

For many SAP landscapes, SAP HANA and S/4HANA are the new Crown Jewels. Entire digital transformation initiatives like smart stores or IoT are built around it. Yet, most SAP HANA implementations are not protected against disaster.

According to IDC, critical application failures can cost in the range of $500k-$1m per hour. Another study by DTI/PWC shows that 7 out of 10 small firms that experience a major data loss go out of business within a year! So why the blind spot when it comes to SAP HANA?

Disaster Recovery-as-a-Service for SAP: Affordable Business Insurance for the Digital World

Disaster Recovery (DR) used to require a fully redundant failover system at a far and undisclosed location. Setup, monitoring, and management were expensive – and often cost-prohibitive.

DRaaS has changed this. Companies can achieve infrastructure savings of up to 95% – not to mention the savings on labor and management. The reason: business data is streamed for backup into the cloud, stored at low cost, and is highly durable. When disaster strikes, this ongoing backup serves as the foundation for recovery. Critical business data can be quickly restored and provisioned in the cloud.

Key DRaaS Considerations for SAP HANA-Based Workloads (and others, too)

The DRaaS concept is universal and applies to many workloads and technologies. Our focus here, though, is on the Crown Jewels: SAP HANA. Mission critical, SAP HANA often holds highly valuable company information. Therefore, look for DRaaS solutions that fulfill the following five key considerations.

1. ***Secure data transmission and storage***

   Data encryption at rest and in motion is an absolute must for backing up your sensitive company data into the cloud. Look for solutions that fulfil this important requirement and others such as precise network definitions for network routes and ports, a strict authorization model with customer-defined policies, and an audit trail for all executed operations.

2. ***Optimized network traffic and light-weight processing***

   Network traffic volume is not only the most expensive cost element

Swen Conred,
CEO, Ocean9 Inc.

[1] *DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified, IDC Research, 2014.*

[2] *Contingency Planning, Strategic Research Corp. and DTI/ Price Waterhouse Coopers, 2004.*

for cloud backup and DR, but also affects the speed and duration of backups. This is where data compression comes into play. Depending on the actual business data, compression can reduce backup size by as much as 25–35% – which translates into cost and time savings of the same percentage.

3. ***A simple disaster recovery process***
   If disaster strikes, the last thing you'd need is a complex, error prone recovery procedure for your SAP system. Instead, you need extreme simplicity enabled by automation. This simplicity also enables frequent automated DR testing.

4. ***Production grade failover system – at the push of a button***
   Look for a DR provider that can give you fresh and clean SAP cloud installations with the ability to select the SAP HANA version, operating system version, and number of cluster sites for high availability – and the ability to again back up and protect the failover system as even the DR target site could become victim to yet another disaster.

5. ***Choice of DR cloud provider and region with the ability to switch***
   The mega clouds currently supporting SAP workloads are Microsoft Azure and Amazon Web Services, and now Google Cloud. Whichever you choose, remember things can change fast. Make sure you can re-locate your DR target location with ease and no cost from one cloud region to another – or from one cloud provider to the other.

The Ultimate Goal: Meeting Recovery Point and Recovery Time Objectives

The Recovery Point Objective (RPO) is the maximum period in which data might be lost from an IT service due to a major incident. The Recovery Time Objective (RTO) is the duration of time for a business process to be restored after a disaster or disruption. Make sure your vendor can meet the RTO and RPO goals you set.

For SAP workloads on SAP HANA, lowest RPO times are driven by the SAP HANA log backup frequency, which typically ranges from 5 to 15 minutes. The key driver of RPO is the time it takes to load the backup data back onto the failover machine. The shorter the time, the faster you're back in business. For SAP HANA DRaaS projects supported by recovery automation, aim for an RTO range of 1 to 2 hours.

Bonus: The On-Demand Sandbox

A bonus of cloud-based DR is the ability to create development and test systems on the fly. If it's easy to build a DR system, it's easy to build a development and test system in the cloud. Having such flexible system capacity at hand can unleash your development activities and drive more innovation at your company.

DRaaS for SAP: Not a Luxury, but a Necessity in Our Digital World

Just as the Crown Jewels never go unprotected, neither should your SAP system. With SAP DRaaS at a fraction of the cost of traditional DR solutions, there is no reason to wait and leave your SAP system vulnerable. Stop worrying and gain the peace of mind that comes with full protection for SAP systems. **CS**