White Paper

EMC RecoverPoint for Virtual Machines Gives Administrators More Agility and Control

By Jason Buffington, Senior Analyst

August 2014

This ESG White Paper was commissioned by EMC and is distributed under license from ESG.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.
Contents

Introduction ........................................................................................................................................3
Virtualization Administrators Are Taking Control .................................................................4
  The Times Are Changing ...........................................................................................................4
Agile Data Protection Is More than Just Backups ..................................................................5
  Snapshots ..................................................................................................................................6
  Replication ..................................................................................................................................6
EMC RecoverPoint for Virtual Machines ..................................................................................6
  Why Virtualization Administrators Should Look at RecoverPoint for VMs ......................8
The Bigger Truth .......................................................................................................................9

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.
Introduction

Protecting a modern data center has never been more important, as advances in server virtualization spur the creation of software-defined data centers (SDDCs) with dense arrays of virtual machines in a condensed infrastructure. According to the IT professionals surveyed as part of ESG’s annual research into IT priorities, both server virtualization and improving data backup continue to be major priorities year after year (see Figure 1).\(^1\)

![Figure 1. Top Five IT Spending Priorities for 2014](image)

Most likely, there is a very good reason that virtualization and data backup appear adjacent to each other so consistently in the IT priority list. Namely, it is extremely important to modernize a production infrastructure and related protection capabilities in parallel.

Some organizations do make sure that the two modernization efforts unfold concurrently. Other organizations modernize their production infrastructure while retaining their legacy backup tool. Usually, they realize quickly that older backup products are relatively unreliable at protecting highly modern IT infrastructures—and some can even hinder the production infrastructure.

Sooner or later, however, many IT professionals grow beyond just thinking “backup” in regard to ensuring protection of and recovery agility for a highly virtualized environment. These evolutions in protection strategy are not always coming strictly from traditional backup administrators, either; storage and virtualization admins also make decisions in this area.

With so much riding on the operational success of a virtualized infrastructure—and considering the crucial link between modern virtualization and modern data protection—two trends are becoming common:

- Virtualization administrators (vAdmins) are taking a more active role in protecting and recovering VMs, instead of abdicating that responsibility to the backup administrator.
- VM backups are being supplemented with snapshots and replication.

Virtualization Administrators Are Taking Control

Workload administrators have long been accountable for making sure their systems are accessible for the benefit of the business. These IT professionals are the administrators responsible for:

- Databases, ERPs, and various other business systems.
- E-mail services.
- File- and storage-related offerings.
- Virtualization platforms (i.e., vAdmins).

Traditionally, these IT pros would manage an application’s configurations while other IT professionals managed the underlying storage/compute systems and performed infrastructure support services including backup. For instance, a workload admin would manage the SQL engine, the Exchange server, or the virtualization platform but relied on server, network, and storage admins to provide the underlying infrastructure on which those platforms or applications resided. The workload admin also depended on the backup admin to install agents to protect the data in the servers from afar.

The challenge with “un-enabled” workload administrators was that they were typically the only members of the IT team who understood the business value of the data and knew the steps required to maintain or resume operations. That was a concern—because if a calamity were to strike or even if a minor glitch were to occur, the workload admins (all four types of them) would be at the mercy of other IT teams for component recovery. Only after component recovery was complete could the workload administrator complete the recovery of the application/platform itself.

The Times Are Changing

Recognizing their own unique perspectives regarding which aspects of their systems are high/low priority and thus in need of varying degrees of protection, each of those four types of IT pros wants to be more involved or even autonomous in protecting and ensuring the recoverability of virtualized systems.

In the case of vAdmins specifically, their responsibility is evolving as virtualization matures from being just “another workload with hardware below and services above” to a unified framework in which underlying components are consolidated and abstracted. With the virtualization stack becoming the ubiquitous layer for IT administration, services such as data protection are being integrated directly into the vAdmin’s management purview.

Some IT vendors are now delivering storage management and data protection tools that use taxonomies and management interfaces (UIs) that vAdmins already know and like. In this manner, the vendors are enabling the functions to be administered by the IT professional who understands, more than anyone else, the needs of the virtualization framework and the business requirements of individual VMs and their virtualized workloads.

As a result, the vAdmin is no longer as dependent on storage or backup administrators for those IT functions. In fact, ideally, the trio should become more cooperative and collaborative in sharing the responsibility of ensuring resiliency for the virtualized infrastructure.
Agile Data Protection Is More than Just Backups

IT architects should consider the complete range of data protection mechanisms (see Figure 2) if they wish to achieve the diverse, demanding agility levels that business owners require for assured access to their data.

*Figure 2. The Spectrum of Modern Data Protection*

Long gone are the days when the terms “backup” and “data protection” were synonymous. Today, data protection is a continuum of methods for ensuring agility and data usability within an IT infrastructure. And although backups still underpin a modern data protection strategy, it can be advantageous to supplement backups with snapshots, replication, or both. This is true for any IT infrastructure, but it is even more useful in highly virtualized environments, considering the ways in which vAdmins are supplementing their VM backups with snapshots and/or replication (see Figure 3).²

*Figure 3. Supplementing VM Backups with Snapshots and Replication*

<table>
<thead>
<tr>
<th>Mechanisms used to protect Hyper-V virtual machines vs. VMware virtual machines.</th>
<th>Percent of respondents, multiple responses accepted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshots of the datastores via storage systems</td>
<td>32%</td>
</tr>
<tr>
<td>Replication of storage volumes/LUNs</td>
<td>30%</td>
</tr>
<tr>
<td>Replication within virtualized applications (e.g. database mirroring, DAG)</td>
<td>31%</td>
</tr>
<tr>
<td>Snapshots of virtual machines</td>
<td>33%</td>
</tr>
<tr>
<td>Additional backups/dumps of data from within the virtualized applications</td>
<td>27%</td>
</tr>
<tr>
<td>Extension of on-premise backup with cloud-based repositories</td>
<td>20%</td>
</tr>
<tr>
<td>We do not use any other approaches besides virtual machine backups</td>
<td>8%</td>
</tr>
</tbody>
</table>

As Figure 3 shows, a wide range of snapshot and replication options are in use today, but the most telling statistic is the lowest one in the chart. It shows that less than 10% of respondents’ virtualized environments are being protected by VM-backups alone. The other 91%+ of virtualized environments supplement their VM backups with replication and/or snapshots because they need recovery agility that is broader than what backups alone can offer.

Snapshots

Snapshots from primary storage enable a level of near-instantaneous recovery that simply isn’t possible with backup systems (because backup systems need to restore data before it is usable). Even compared with the “instant recovery” features of some backup solutions, snapshot reversion is often perceived as superior.

Most instant-VM capabilities begin with restarting a VM from its storage within the backup server storage pool, and then near-transparently moving the virtual disks from the protection storage to the production storage behind the scenes. Reverting to a snapshot within the primary storage results in the same effect of rapidly restarting the VM from a previous point in time—without involving data movement between storage devices. In both cases (snapshots and instant-VM recoveries), the goal is to resume VM functionality faster (reducing RTO) than would be possible by restoring from a traditional backup.

Snapshots have been part of primary systems for many years. However, the recent trend centers on providing virtualization administrators with more control over their own destiny—by enabling snapshot management within the vAdmin’s management UI and within the context of the virtualization framework.

Replication

Replication between primary storage systems also enables levels of service availability not feasible with backup systems alone—and ideally, the replication management capability would be available to the virtualization administrator as well. To be clear, bringing replication to a virtualized environment isn’t the same thing as a virtualization vendor developing replication technology (think SQL database mirroring). This advancement is about giving the virtualization platform and the vAdmin who manages it a way to utilize efficient replication via the underlying infrastructure components, including storage or server/OS technologies.

Certainly, other DP methods worth mentioning exist beyond the stereotypical “backups plus snapshots plus replication.” Those methods can involve local or remote copies, as well as periodic replication and continuous data protection, which itself includes both CDP and near-CDP offerings:

- **“Pure” continuous data protection (CDP)** typically implies real-time replication at a very granular level that enables data restoration to any previous point in time, similar to rolling back a SQL database using its transaction log.

- **Near-CDP** technologies can provide near-real-time replication, such as sending a copy of data fragments as part of low-level [FileWrite] or [FileClose] operations. Near-CDP technologies typically do not have the “infinite points of restore” that CDP boasts. However, they still provide a continually updated, survivable copy of data usable in availability or continuity solutions.

The key is to recognize that as much as backup copies are a key, core component of data protection, modern data protection requires a broader range of capabilities than what “backup” alone can muster. Backup must be one part of a bigger data protection vision.

**EMC RecoverPoint for Virtual Machines**

That vision—what ESG refers to as the data protection spectrum (see Figure 2)—EMC calls the Data Protection Continuum (see Figure 4). EMC recognizes that protection should encompass a range of mechanisms to enable myriad recovery capabilities.
To deliver that continuum of capabilities, EMC offers a comprehensive data protection portfolio that includes:

- **EMC NetWorker**—enterprise backup software with more than 20 years of success in protecting heterogeneous environments.
- **EMC Avamar**—with options to use a dedicated range of Avamar-based hardware (storage and controllers) or EMC Data Domain deduplicated protection storage systems.
- **EMC Data Domain**—deduplicated protection storage usable not only by EMC Avamar and EMC NetWorker, but also by nearly all enterprise-credible backup software offerings being sold today.
- **EMC SourceOne**—enterprise archiving, also included in the EMC Data Protection software suite.
- **EMC Data Protection Advisor**—providing a single pane of glass to monitor the operations of EMC and non-EMC backup software and storage replication mechanisms.
- **Mozy by EMC**—cloud-based backup for endpoint devices, remote offices, and smaller organizations.
- **VMware VDP/VDPA**—virtualization-specific protection within the vSphere architecture, powered by EMC Avamar technology.
- **EMC VPLEX**—providing continuous availability and agility across or between data centers.
- **EMC RecoverPoint**—storage-centric synchronous and asynchronous replication

The newest addition to the EMC data protection portfolio is **RecoverPoint for Virtual Machines** (see Figure 5), which provides the same hypervisor-integrated approach to replication for VMware environments that physical environments have come to depend on with EMC RecoverPoint.
As Figure 5 shows, this new EMC solution has three core components:

1. A hypervisor-based I/O splitter that transparently intercepts disk writes from the VMs going through the hypervisor before going to any storage data store.
2. An appliance that manages replication of data between hypervisors.
3. A vCenter plug-in for management because the solution is intended to be managed by a vAdmin (rather than a storage admin).

Although traditional storage-centric replication solutions would need matching physical storage arrays across the environment in order to work correctly, this solution works with any storage scenario supported by the hypervisor because the EMC (virtual) appliance is running within the hypervisor framework – including SAN (iSCSI or FC), NAS, DAS or vSAN. By utilizing similar splitter methodologies as EMC’s previous RecoverPoint version, many of the same solution scenarios can be achieved:

- Transparent, non-impactful I/O capture and transmission between sites.
- Synchronous and asynchronous replication, dynamically switched based on bandwidth.
- Mirrored provisioning, so that new VMs on one side result in new resource provisions on the other.
- WAN-optimized replication.
- Any previous point-in-time restoration using journal technology.

That said, RecoverPoint for VMs is more than a virtualized version of RecoverPoint, boasting several virtualization-specific features:

- VM-level granular protection and recovery.
- Orchestrated VM recovery between sites, without the need for VMware Site Recovery Manager (SRM).
- Multiple VMs per Consistency Group, including write-order fidelity between VMs for multi-machine application and data validity—even spanning across ESX clusters.
- Ability to test, fail over, and fail back individual VMs.

Most importantly, the entire RecoverPoint for VMs is managed through vCenter, so that the vAdmin can do everything from installation, to configuration and overall operation within the virtual management framework (without relying on a storage-UI or a storage administrator).

**Why Virtualization Administrators Should Look at RecoverPoint for VMs**

In much the same way that vAdmins have been taking a more hands-on approach to backups by employing mechanisms that are meant to be managed by vAdmins instead of backup administrators, they also should look for an optimized approach to leveraging that hypervisor-integrated protection:

- In lieu of generic storage-centric replication between paired arrays, EMC RecoverPoint for VMs can protect individual VMs, groups of VMs, or whole hosts without dependency on a particular hardware solution.
- Management of both replication and failover/failback are performed within vCenter as vAdmin actions.
- Environments considering hybrid architectures for BC/DR can use RecoverPoint for VMs between self-managed sites and cloud service providers in private, hybrid, public, or multi-public cloud configurations.

Storage replication enables service availability and data survivability across an enterprise campus or an intranet, and it isn’t hard to imagine RecoverPoint for VMs evolving in the future to be a similar replication mechanism that enables hybrid architectures between private cloud sites or perhaps across public clouds for DRaaS solutions.

The power of RecoverPoint for VMs centers on more than just empowering a vAdmin with self-service control over protection. This product also enables IT to natively protect a software-defined data center. Being able to define protection policies that are VM/host savvy might exceed even a vAdmin’s expectations. It becomes possible to
adhere to a policy in which, as new VMs are created, the virtualization host and the vAdmin understand the business preservation and resiliency requirements—and accordingly, RecoverPoint for VMs ensures the correct level(s) of protection.

The Bigger Truth

As organizations modernize their production infrastructures through virtualization, they must also modernize their protection and recovery capabilities. In many cases, VM backups may not be enough to satisfy the range of recovery agility requirements that the business demands. Those VM backups should, therefore, be supplemented with snapshots, replication or both.

EMC understands the need for a multitude of recovery capabilities, and it has responded by delivering myriad protection mechanisms encompassing backup software, archive software, deduplicated storage, etc. With EMC’s pedigree in enterprise primary storage, it should not be a surprise to see innovative protection mechanisms coming from/for the storage product lines, as well.

EMC RecoverPoint for VMs enables virtualization administrators to manage replication using the VMware infrastructure they are accustomed to, with the object (VM) granularity and taxonomy they know, and via the management experience they already operate in. For vAdmins who require a broader range of recovery options, VM-centric replication that they can manage may provide the right answer. But doing it through traditional storage tools or legacy arrays can be suboptimal without contextual awareness of VMs and the hypervisor perspective on infrastructure.

RecoverPoint for VMs addresses those challenges by bringing EMC’s storage protection capabilities under the purview of the vAdmin who is responsible for ensuring the availability of systems hosted in a virtual infrastructure.