How to Protect Data in Virtual Environments

Virtualisation is a transformational technology, and most organisations are now using it to consolidate their IT infrastructures, increase operational efficiency, and improve disaster recovery and business continuity of applications and growing volumes of distributed information.

As server virtualisation becomes mainstream, businesses are investing a lot of time researching the most suitable virtualisation platform for their environment. Equally as important, and sometimes overlooked, organisations also need to address how to best protect their data, which is now held across both physical and virtual machines. Additionally, virtualisation opens new opportunities to deliver business continuity and disaster recovery.

They also need to consider how they will migrate data from existing (physical) machines to new (virtual) ones. This IDC Analyst Connection explores the key considerations for the protection of data in virtual environments and offers some best practices for doing so.

Key Considerations for Protecting Data in Virtual Environments

When planning protection of virtual servers, many of the same rules from the physical world apply. Virtual servers are subject to the same variety of loss scenarios as their traditional physical counterparts (whether this be natural disasters, viruses or hard disk corruption) — as well as an array of additional ones that arise from the nature of virtualisation technology itself.

- **How to migrate data.** When companies start to deploy virtual machines, the first big challenge to address is data migration. IDC believes that image-based snapshots are an efficient way to not only migrate data and system information from physical to virtual machines and back again, but also to migrate data between virtual machines.

- **Juggling multiple virtual platforms.** As organisations typically have various server and storage brands in their environments, IDC has seen an increasing number of organisations use different virtualisation technologies in these environments, most prominently VMware and Microsoft Hyper-V. Managing this extra dimension of diversity is a key challenge when protecting data in virtualised environments.

- **Data protection of virtual machines and performance impact.** Scalability issues arise as the number of virtual machines increases. Agent-based backups tend to impact the performance of the host due to many simultaneous backup streams. Additionally, virtual machines are often created on the fly and might not be protected from the start, as virtual machines sprawl and IT managers are not aware of their existence.

- **Disaster recovery and high availability.** Data protection needs to be cluster-aware in order to support high availability and disaster recovery. As virtual machines are moving from host to host in a high availability or disaster recovery scenario, they also need to continue to be protected.

- **Speed and granularity of recovery.** The recovery time objective (RTO) is key when recovering virtual machines, as many users expect a seamless data and application experience. Granularity of recovery is a key parameter. In some cases the recovery of the whole virtual machine file is needed, whereas in other cases only one file inside the virtual machine needs to be recovered.

- **How does data deduplication work in a virtual world?** Data deduplication has a big effect on backup streams and even more so in virtual environments, due to the large percentage of duplicate data in virtual machine files. Deduplication at the source is most beneficial, if data needs to be sent across a network for backup or DR purposes.

Best Practices for Protecting Data in Virtual Environments

Just as similar threats prevail in both physical and virtual environments, some of the best practices from the physical world are even more pronounced in the virtual world.
• Can I migrate data easily between physical and virtual machines? A software layer that lets you execute any of these four options simply and efficiently is a great benefit, as migration of data is a huge challenge for end users, but not very often talked about by storage vendors.

• Can I manage [data protection from one central console? Most companies have a data protection process for their physical assets in place. It is a key advantage if their software also allows them to manage their virtual environment under the same management framework, including storage groups and policies. Likewise, the solution should support all major virtualisation platforms to protect a mixed environment. Ideally, software deduplication could also be integrated and managed from this console in order to compress the data at the source, before it gets sent over a network.

• Can I test my disaster recovery setup? Testing of the disaster recovery setup is a painful process for many organisations, and as a result many of them avoid it. With the right solution, you can simulate the recovery of your applications by spinning them up as virtual machines within minutes. Therefore you can always validate that you are able to recover and you can test your recoverability frequently.

Virtualisation is fast maturing into an effective means of optimising IT infrastructures, and the protection of data in virtualised infrastructures should be a key consideration in each virtualisation rollout. With its latest product release, Acronis has taken a clear initiative in simplifying the data protection for virtualised environments, helping companies to reap the benefits of a virtualisation deployment.

IDC Recommends

• Choose a data protection and disaster recovery solution that allows you to manage physical, virtual and cloud environments under the same framework.

• Select a solution that supports all major virtual platforms.

• Choose a data protection and disaster recovery solution that includes data deduplication at the source, as it will have a huge impact in backup streams from virtual environments.

• Ask carefully about data migration options, as they can sometimes be a hidden stumbling block.

• Test your disaster recovery and high availability solutions on a regular basis. Virtualisation enables painless testing.

• Use an agentless approach for protecting virtual machines both on-premises and in cloud environments.

• Choose image-based backups for your physical, virtual and cloud environments.

ABOUT THIS ANALYST

Carla Arend is a program manager with the European Infrastructure Software research team, responsible for managing the European storage software and services research service. Arend provides clients with key insight into market dynamics, vendor activities, and end-user trends in storage software and services markets. She is also responsible for the Western European Storage Software Tracker. In addition, she has worked on several consulting projects identifying opportunities in the European storage software and services market and has authored white papers on a range of storage topics. She presents at industry events, sales training, and end-user events.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localisation of this document requires an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms. Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com.