10 Essential Best Practices for Virtual Server Backups

By Brien M. Posey

ALTARO

TABLE OF CONTENTS

INTRODUCTION

Systems administrators have been backing up their servers for decades, and yet comprehensive data protection can still be elusive, even after all of this time. Part of the reason for this has to do with the fact that technology is continuously changing. Perhaps no change has impacted the backup and recovery process more than server virtualization.

In many ways, server virtualization makes the backup process easier. The virtualization infrastructure gives administrators backup and recovery options that were not previously possible. Even so, server virtualization adds a layer of complexity to the backup process. It is no longer enough to simply make a backup of the server. Now, administrators must determine how the virtualization stack will impact their backups.

Unfortunately, there isn't a simple technique that administrators can use to ensure that their backups are always perfect. Instead, achieving consistently reliable data protection involves three main tasks.

THESE TASKS INCLUDE:

- Comprehensive disaster recovery planning
- An understanding of the virtualization infrastructure and how it impacts the backup process
- An adherence to established best practices for protecting virtualized environments

Although there is ultimately no shortcut to these three tasks, this white paper will discuss a number of different best practices for backing up virtualized environments.

HOW VIRTUAL SERVER BACKUPS ARE DIFFERENT

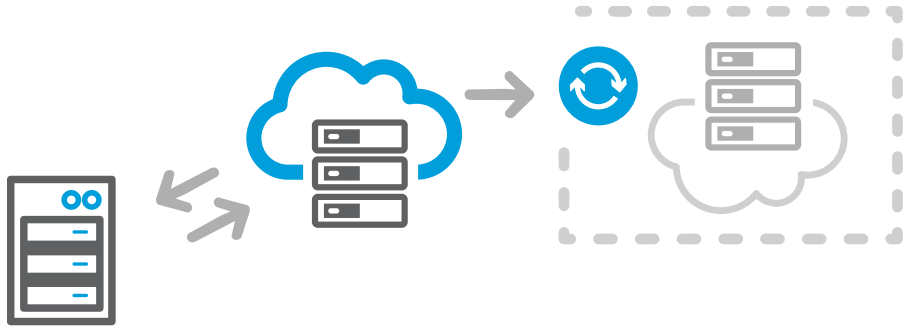
Before an administrator can adequately protect their virtualized servers, they must understand how virtual server backups differ from backups within a physical data center. The primary difference in protecting the two environments is that while physical environments are generally made up of hardware and operating systems, virtualized environments make use of an entire virtualization stack. Administrators have a few different options for where in the stack they can choose to run the backup. The administrator's choice impacts what will be backed up and the granularity with which data can be recovered.

With this in mind, it is necessary to recognize that not all backup applications are created equally. Not only does each backup vendor offer their own set of features and capabilities, there are architectural differences as well.

Some of the backup applications that are in use today could be classified as legacy backups. A legacy backup application might refer to an older backup application that was created in the days before server virtualization went mainstream, or it could refer to a backup application that was originally created for backing up physical servers but was later retrofit to allow virtual servers to be backed up as well.

Conversely, most modern backup applications have been specifically built for backing up virtualized environments. Some of the products that fall into this category are specifically dedicated to backing up virtualized environments, while other modern backup applications also support backing up physical servers.

The important thing to realize is that nearly every backup application that is being sold today claims to be able to back up a virtual environment. Even though most backup vendors make this claim, the backup products offer varying levels of support for protecting virtualized environments.



Just because a backup application can back up a virtualized environment does not necessarily mean that the backup application will be a good fit for your organization.

The reason for this is that the way in which the backup product interacts with the virtualization stack makes a huge difference in the level of protection that the backup product provides. Backups of virtualized environments generally fall into three categories:

GUEST LEVEL BACKUPS

HOST LEVEL BACKUPS

STORAGE BACKUPS

Guest level backups are often used by legacy backup products. These types of backups are also sometimes used when backing up a virtual machine that is not fully supported for host level backups.

Guest level backups refer to backups that are made at the virtual machine level. These backups usually involve installing a backup agent directly onto a virtual machine's operating system.

Backups made at the guest level are able to fully protect a virtual machine's contents. Even so, there are some distinct disadvantages to using guest level backups. One such disadvantage is that guest level backups can be difficult to manage. Guest level backups require each virtual machine to be protected individually. As such, administrators will have to make sure that every virtual machine that needs to be protected receives a backup agent. While it is often possible to include backup agents within gold images or to push backup agents to virtual machines using scripts or group policy settings, there may not be an easy way to ensure that newly created virtual machines are always added to a backup job.

Another disadvantage to performing guest level backups is that because the backup agent resides within the virtual machine, the backup application is oblivious to the virtualization stack. For all practical purposes, the backup application assumes that it is backing up a physical server.

The reason why this is a problem is because none of the virtualization specific components are backed up. There is more to a virtual machine than just a virtual hard disk. Virtual machines include a configuration file that defines hardware allocations for the virtual machine. There may also be snapshots associated with the virtual machine. These types of resources are not backed up as a part of a guest level backup.

Host level backup is the preferred method of backing up a virtualization infrastructure. In other words, the backup software targets a virtualization host server rather than attempting to back up each virtual machine individually. The advantage to using this approach is that it eliminates the need for virtual machine level backups. If a new virtual machine is created on or live migrated to a virtualization host, the host level backup will automatically backup that new virtual machine without the administrator having to explicitly instruct the backup software to do so.

Unfortunately, host level backups are not suitable for every situation. Some legacy backup applications for instance, are incapable of creating host level backups. There are also some types of virtual machines for which guest level backups are more appropriate. This is especially true for virtual machines that are running obscure or outdated operating systems or that are running applications that require special attention. The reason for this is that if backups are being created at the host level then the backup application needs to be able to look inside of each virtual machine. Otherwise, granular restoration of files, folders, applications, etc. is impossible.

Storage level backup is the third way in which virtual machines can be backed up. This approach usually involves copying individual storage blocks from a storage array to a backup appliance. Although this particular approach does work, storage level backups may lack virtual machine and application awareness, which can make granular recovery difficult.

GOALS AND CHALLENGES

Before implementing a backup solution for your virtualized environment, it is important to determine the goals that you hope to accomplish with your proposed backup solution.

Proper planning is one of the most crucial tasks in data protection, and defining your goals and objectives is the first step in the overall planning process.

The sections below list some important questions that must be considered as you define your data protection objectives

WHAT DO YOU NEED TO BACK UP?

Prior to implementing a virtualization backup solution, the organization must determine what needs to be backed up. Although this is a seemingly simple question, answers such as "everything" are inadequate.

When deciding what to back up, the organization must decide whether host servers need to be backed up, or just the virtual machines. The IT staff will also need to determine whether there are any virtual machines that do not need to be backed up. For example, most organizations have several domain controllers that have been put in place either as a way of improving Active Directory performance or as mechanisms for preventing Active Directory level failures. If multiple, redundant domain controllers do exist, do they all need to be backed up? If so, why?

This isn't to say that redundant domain controllers should never be backed up. In many instances, an administrator's time is the limiting factor. If an administrator is strapped for time, then there is certainly nothing wrong with backing up all virtual machines rather than picking and choosing which virtual machines to back up. The tradeoff for doing so is that backing up all virtual machines will presumably consume more space on the backup target than a more selective backup might. Even so, backing up all VMs does provide the greatest degree of protection and may very well be the best option for time strapped administrators.

WHAT LEVEL OF GRANULARITY IS REQUIRED FOR RESTORATION?

Another consideration that must be taken into account is the level of granularity that will be required for restoration operations. The required level of recovery granularity will impact not only your choice of backup software, but also the type of backup that you have to perform. Backups can be made at various levels of the virtualization stack (as will be discussed in the next section) and the stack level at which the backup is created has a direct impact on the backup contents.

Because not every virtual machine backup provides the same level of data protection, it is important as a best practice to determine your data recovery goals before implementing a virtualization backup solution.

In other words, the organization must determine what needs to be recoverable in the event of a data loss event.

It can be tempting to dismiss this question by simply stating that the organization needs to be able to recover everything. However, things aren't quite that simple. Server virtualization involves a lot of different moving parts, each with their own data protection needs. The method or methods used to back up your virtualization infrastructure will directly impact your ability to perform various types of recoveries.

The Hypervisor

The first level that should be considered is the hypervisor itself. Hypervisor backups are relatively unimportant since the hypervisor can simply be reinstalled in the event of a server level failure. Just be sure to document the hypervisor version that is in use and make sure to keep the hypervisor installation media handy since some virtual machines can be sensitive to the hypervisor version.

The Virtual Machines

The most important level of the virtualization stack to protect is the virtual machines themselves. It more or less goes without saying that the entire point of backing up your virtualization infrastructure is to have the ability to recover virtual machines following a data loss event.

File Data

A third level of granularity that is usually required is the ability to recover file and folder data within a virtual machine. File level restorations have been a part of backup applications for so long that it may seem strange to even include the ability to restore individual files and folders among the list of requirements. However, there is a reason for doing so.

Some of the first generation of backup products to support server virtualization lacked the granularity to recover individual files and folders within virtual machines if the backup was created at the host level. Such products allowed virtual machines to be restored as a whole, but did not have the ability to look inside of a virtual machine in order to backup or recover individual files or folders.

Today, pretty much every major backup vendor will allow the recovery of file data in virtualized environments, but you should definitely test to see if you have this capability (or if you need to do something special to utilize this capability) if you are using an older backup product.

If you are using an older backup solution and simply do not have time to test its ability to restore individual files and folders then your best option is to update to a newer, fully virtualization aware application rather than taking a chance on your existing software. Although it may be tempting to dismiss the idea of replacing your backup software because of concerns about cost, reasonably priced virtual server backup solutions do exist.

Line of Business Applications

As is the case for file data, a virtualization aware backup application should ideally be able to protect your line of business applications that are running inside of virtual machines. Most modern backup applications include application awareness for some of the more popular business applications such as Microsoft Exchange Server or SQL Server. Even so, there are varying levels of application support from one product to the next.

Suppose for a moment that a particular backup application advertises the ability to protect Microsoft Exchange Server. In some cases, this ability can only be unlocked by purchasing an Exchange backup license that is separate from the core backup application. For the sake of discussion however, let's assume that the product in question has native support for protecting Exchange Server. What does that really mean?

In many cases, products that advertise the ability to protect Exchange Server are able to make application consistent Exchange Server backups and are able to perform a point in time recovery if necessary.

Other products go beyond basic application level support and allow granular recovery operations to be performed within Exchange Server. Such a product might for instance allow an administrator to recover an individual mailbox or a specific E-mail message.

The point is, that backup products provide varying degrees of granularity with regard to support for line of business applications. It is critically important to choose a backup application that delivers the level of protection that you need for your applications.

Infrastructure

Another level of granularity that is sometimes overlooked is the ability to protect infrastructure components such as the Active Directory. Just as your backup solution should be able to protect files, folders, and applications, it also needs to have the ability to protect the Active Directory and any other infrastructure services that your organization depends on.

WHAT ARE YOUR RPO AND RTO REQUIREMENTS?

One of the most important things that you must do with regard to goal setting is to determine your RPO and RTO requirements. RPO stands for Recovery Point Objective. This term refers to the frequency with which recovery points are created. The more frequently recovery points are made, the less data could potentially be lost in the event of a disaster. For example, a backup that is made on a daily basis could potentially lose almost 24 hours' worth of data if a crash were to occur just prior to a backup operation starting. Similarly, a backup system that creates recovery points every five minutes' risks losing just under five minutes' worth of data in the event of a crash.

RTO stands for Recovery Time Objective. This term refers to how long the organization can tolerate waiting for a restoration to complete. Some organizations might have an RTO of a day or more, while others need recovery operations to occur almost instantly.

There is no right or wrong answer when it comes to selecting an RTO and RPO. You have to do what is right for your own organization. This means striking a balance between data protection and administrative effort. After all, the best backups in the world will do little good if managing those backups requires an unrealistic time commitment from an already overworked administrative staff.

WHO WILL BE RESPONSIBLE FOR BACKUP AND RECOVERY OPERATIONS?

While you are planning for your backup, it is important to make decisions about who will be responsible for backup and recovery operations. Most organizations designate a specific person from the administrative staff or from the helpdesk staff to handle backup and recovery operations. In smaller IT shops however, there may only be one or two people who can oversee the backups.

In such environments, it is extremely important to choose a backup solution that is reliable and that requires minimal administrative effort since the limited IT staff probably does not have time to take on additional responsibilities.

As you make this decision as to who will perform the backups, it is important to also designate at least one other staff member who can handle backup and recovery operations in the event of an emergency (assuming that such a luxury exists). After all, someone needs to be able to perform the recovery operation if a data loss event were to occur while the primary backup operator is out of the office on vacation.

This leads to a somewhat related point. As you choose the backup software that your organization will use, it is a good idea to pick something that is intuitive and easy to figure out. The reason for this is that it is impossible to predict when a disaster will strike, and who will ultimately end up having to perform the recovery operation. Disasters by their very nature are unpredictable, and sometimes the best plans simply do not hold up in times of disaster.

Since you never really know for sure who is going to end up having to perform the restoration operation during a large-scale disaster, it is important for the backup software to be easy enough to use that anyone can perform a successful restoration.

Obviously letting an untrained staff member perform a restoration violates almost every established best practice. After all, a disaster is not the time to be figuring out how your backup software works. Even so, smaller shops might only have a single administrator and if that administrator happens to be on vacation, or out with the flu when disaster strikes then someone in the office needs to be able to perform the restoration. Disaster readiness is based on preparing for the worst case scenario and part of that preparation means avoiding using a backup application that is so complex that only those with specialized training can make it work.

Even if you do not buy into the idea that someone in your office who is not normally responsible for backups could end up having to perform a recovery operation during an emergency, there is still something to be said for having a backup application that is easy to use. Recovery operations are always stressful and there is a lot of pressure to return everything to working order as quickly as possible. Stress can lead to mistakes, but the chances of a mistake being made are greatly reduced by a simple and intuitive backup interface.

WHAT ARE YOUR STORAGE REQUIREMENTS?

While planning your backups, you must also determine your backup storage requirements. This involves more than just estimating the volume of data that needs to be backed up and the number of retention points that you want to keep on hand. You must also plan for future data growth so that your backup target will be able to accommodate newly created data for the foreseeable future.

WHAT IS YOUR DATA PROTECTION BUDGET?

Cost is almost always a factor in developing an organization's data protection plan. There is usually a trade-off that strikes a balance between the level of protection that the organization would ideally like to have and the amount of money that the organization is willing to spend.

When it comes to backups, it is easy to spend huge amounts of money. If your goal is to keep the cost of your data protection solution reasonable then you should pay attention to the way that your backup software is licensed. Ideally, data protection software should be licensed on a per host basis.

Some of the available backup products use per VM or per socket licensing, which can cause data protection costs to snowball as an organization's virtualization infrastructure grows.

As you evaluate the licensing costs for the products that you are considering, it is important to watch out for any additional costs beyond that of the required license. For example, some backup applications require a SQL server, which would dramatically increase the amount of money that your organization will have to spend.

BEST PRACTICES

As previously explained, there are a number of established best practices for backing up virtual machines and the virtualization infrastructure. The remainder of this white paper will be dedicated to discussing some of these best practices.

1 BACK UP YOUR BACKUPS

In order for an organization's data to be safe, the organization needs to have three copies of its data. One of these copies is the live, production data that is actively in use. The second copy is a backup. The third copy of the data could be thought of as a backup of the backup.

One of the main reasons why organizations create backups of their data is because of the potential for hardware failure. If for example, the storage array containing all of an organization's virtual machines were to fail then the virtual machines would fail as a result. Backups provide a way of rebuilding the contents of the failed storage array.

Like the storage array in the previous example, backup storage can also fail. Imagine for a moment that an organization is using a disk based backup solution and the storage array containing the backups fails. In this type of situation, the production data is not impacted by the failure. However, the backups would be lost as a result of this failure. Consequently, the organization would lose the ability to revert a virtual machine to an earlier point in time. Furthermore, if the organization's primary storage array were to fail then there would be no way of recovering from the failure.

There are a number of different ways of creating a secondary backup. The easiest solution is to use a backup application that has the ability to simultaneously write data to multiple targets. If that isn't an option, then you might consider creating multiple backup jobs, selecting a different backup target for each job. Many other options are available (such as data replication), but tend to be more expensive to implement.

2 CREATE BACKUPS IN A WAY THAT AVOIDS FAILURE DOMAINS

Another best practice for virtual server backups is to create backups in a way that avoids the possibility of the backups being lost during a data loss event. Imagine for example that your organization has a single virtualization host and half a dozen virtual machines that all reside on Direct Attached Storage.

The easiest way to create a backup of such an environment is probably to run the backup software from within a dedicated virtual machine. Although doing so is an acceptable practice, it is extremely important to write the backups to a separate physical location. If the backups were to be written to a virtual hard disk on the same physical storage that is being used by the virtual machines, then a storage level failure could destroy the backups. Consider writing the backups to a NAS device, an old server that is no longer being used, or possibly to tape.

3 MAKE USE OF HYPERVISOR TOOLS

Another best practice is that you should use hypervisor tools within virtual machines whenever possible. Most major hypervisors include a set of drivers that are more commonly referred to as tools. These drivers help the guest operating system to work smoothly with the virtual hardware.

Each vendor has their own approach to the hypervisor tools. VMware for instance, aptly refers to their tools as the VMware Tools. Microsoft calls their tools the Hyper-V Integration Services. Citrix refers to their tools as the XenServer Tools.

The hypervisor tools help a virtual machine's guest operating system to run efficiently, but the tools can also have an impact on the backup process. Take Microsoft Hyper-V for example. Host level backups of Microsoft Hyper-V servers are based on the Volume Shadow Copy Services (VSS). VSS and the Hyper-V VSS writer collectively allow running virtual machines to be backed up while the VM remains online. In order to do so however, the virtual machine must adhere to several requirements.

SOME OF THE MORE NOTABLE REQUIREMENTS INCLUDE:

- The Integration Services must be installed into the guest OS and must be running
- The VM must be in a running state
- The virtual machine's snapshot file location must reside in the same physical volume as the virtual machine's virtual hard disk
- All of the virtual machine's virtual hard disks must be formatted using a file system (such as NTFS) that supports virtual machine snapshots

There are a few additional requirements that will be discussed later. For right now the most important takeaway is that the VSS writer will not allow an online backup of a virtual machine unless the Integration Services are installed and are running. Unfortunately, Hyper-V does not install the Integration Services into virtual machines by default (although some Windows operating systems pre-install the Integration Services) and there are some versions of Windows that are not compatible with the Integration Services.

If the Integration Services are not installed (or are not running) on a particular virtual machine, then VSS is unable to perform an online backup of that virtual machine. That being the case, the VM is temporarily placed into a saved state while a snapshot is created. Although this process does not last long, it does mean that the VM becomes momentarily unavailable.

Regardless of whether you are using Hyper-V or some other hypervisor, you should install the hypervisor tools into your virtual machines whenever possible. Although the Integration Services can be installed manually, you might be able to save time by using group policy settings to push them to your virtual machines.

It is worth noting that hypervisor vendors tend to update the hypervisor tools over time and that virtual machine performance can sometimes be improved by deploying the latest version of the tools. In Hyper-V environments this is currently a manual process. However, Microsoft has already announced that in Windows Update will automatically keep the Hyper-V Integration Services up to date after the release of Windows Server 2016.

4 USE SNAPSHOTS RESPONSIBLY

Another best practice recommendation is to use hypervisor snapshots sparingly. Although hypervisor snapshots will allow you to revert a virtual machine back to an earlier point in time, snapshots are not a backup substitute. There are at least three reasons why snapshots should be used sparingly and should never take the place of a backup.

The first reason is that unlike a backup, snapshots do not actually copy your data. Instead, the hypervisor creates a differencing disk. A differencing disk is a special type of virtual hard disk that has a parent/child relationship to the primary virtual hard disk. Once the differencing disk is created, all write operations are directed to the differencing disk. The primary virtual hard disk remains in a pristine and unmodified state, which is why it is possible to roll the virtual machine back to an earlier point in time

The second reason why snapshots should be used sparingly is because snapshots are not usually application aware. Snapshots are great for protecting a system against a configuration change or a service pack installation because if something goes wrong the system can easily be reverted to its previous state. However, there can be major consequences to rolling back an application server. In many cases, using a snapshot to revert a database driven application server to a previous state results in application corruption. Windows Server 2016 Hyper-V is going to offer an application aware snapshot feature, but the capability does not yet exist.

A third reason for using snapshots sparingly is that snapshots can impact virtual machine performance. As previously mentioned, when an administrator creates a virtual machine snapshot, the hypervisor creates a differencing disk and protects the original virtual hard disk against any future write operations. Creating multiple snapshots causes chains of differencing disks to be created. These chains of differencing disks impact read performance because if a virtual machine needs to read data it must work through the entire chain of differencing disks until the requested data is eventually found.

5 BE AWARE OF HYPERVISOR LIMITATIONS

Yet another best practice for virtual server backup is to be acutely aware of hypervisor limitations that might impact the backup process. On the surface, virtual machine backups seem relatively straightforward. A host level backup for example, is run against the parent partition and backs up all of the virtual machines in the process.

However, every hypervisor has certain nuances that can impact this process. There might also be limitations inherent in the backup application. Windows Server Backup for example, is unable to back up Cluster Shared Volumes.

Hypervisor specific issues vary from one hypervisor vendor to the next. Microsoft Hyper-V for example, does not support host level backup of some storage resources. For example, if a virtual machine has its own iSCSI initiator (within the guest operating system) then a host level backup will not back up any volumes that are connected directly to the guest operating system via iSCSI. This issue occurs as a result of a limitation in the Hyper-V VSS writer. Keep in mind that the inability to backup iSCSI connected volumes applies only to guest level iSCSI connections. If the host operating system has been configured with iSCSI connectivity, then those iSCSI connected volumes are backed up. Similarly, if a guest OS establishes iSCSI connectivity to a remote storage LUN then the storage can be backed up at the guest level because the Hyper-V VSS writer is not involved in guest level backups.

A similar limitation comes into play for Hyper-V virtual machines that use SCSI pass through disks. Hyper-V virtual machines can be configured to make direct use of a physical SCSI disk rather than using a virtual hard disk. The connected disk is referred to as a SCSI pass through disk. The Hyper-V VSS writer is incapable of backing up the contents of a SCSI pass through disk. Consequently, virtual machines making use of SCSI pass through disks must be backed up at the guest level.

VSS writer limitation also prevent online backups of virtual machines containing dynamic disks. This limitation has nothing to do with dynamically expanding virtual hard disks (thinly provisioned virtual hard disks), but rather with dynamic disks (as opposed to basic disks) defined by the guest operating system.

If a virtual machine contains one or more dynamic disks then the virtual machine can still be backed up, it just cannot be backed up while the VM is online. Hyper-V handles this situation by momentarily placing the virtual machine into a saved state while a snapshot is created.

If your organization uses Hyper-V then as a best practice you should avoid using guest level iSCSI connectivity or dynamic disks, and you should also avoid using SCSI pass through disks.

The bigger lesson is that every hypervisor has certain limitations that can impact the backup process. As such, it is important to understand the backup related limitations for the hypervisor that you are using, to avoid any unwelcome surprises during data recovery operations.

6 INSTANT RECOVERY IN YOUR DISASTER RECOVERY PLANS

As another best practice, it is a good idea to leverage your backup software's instant recovery capabilities. Not every backup application has an instant recovery feature, but modern backup applications that are specifically designed to protect virtual servers may include such capabilities.

As the name implies, an instant recovery feature allows the organization to immediately recover virtual machines following a data loss event. By using such a feature, the organization is able to bring virtualized workloads back online almost immediately, without having to wait for a traditional restoration to complete.

Typically, the backup software monitors the file system used to store virtual server components (such as virtual hard disks and virtual machine configuration files) to watch for any changes. If any storage blocks are created or modified, then those blocks are copied to a disk based backup solution. Blocks are copied to the backup target in batches. These copy operations are scheduled, but occur on an almost continuous basis. For example, batches of changed storage blocks might be copied to the backup target every five minutes.

Now suppose that a virtual machine was to fail and that the organization needed to bring the virtual machine back online immediately. The backup target is a disk based storage array containing a nearly current copy of the virtual machine. Because of this, the backup software is able to recreate the virtual machine on another host server and then link the virtual machine to its components residing on the backup storage array. The virtual machine is able to be run directly from backup storage.

Of course this presents a few issues. For starters, it is critically important to make sure that the backup copy of the virtual machine remains unmodified. If the backup VM were to be indiscriminately used as a production VM then the backup would be modified by write operations that occur through normal VM usage.

The way that the backup software avoids this problem is by creating a virtual machine snapshot. Hence, all new write operations are directed to a differencing disk. The original virtual hard disk remains unmodified, thereby preserving the integrity of the backup.

Each backup vendor implements instant recovery in a slightly different way, but in most cases instant recovery leverages disk based backups, virtual machine live migrations, and hypervisor snapshots.

Once the virtual machine is running from backup storage it can be used in the normal manner. Even so, the administrator must work to restore the virtual machine back to its original location. Backup servers can be used to run the VM on a temporary basis, but do not generally provide the same level of performance as the production environment.

Because the backup remains unmodified, the backup can be restored to the production environment while the users continue to use the backup copy of the VM. Once the backup has been restored, the contents of the differencing disk are copied to the production server and then a live migration or a similar mechanism is used to redirect user traffic back to the production environment. At that point, the snapshot is removed from the backup server and backup operations resume in the normal manner.

7 TAKE THE TIME TO CONFIGURE ALERTS AND NOTIFICATIONS

Another best practice for virtual machine backups is to take the time to configure alerts and notifications. It is admittedly difficult for an overworked administrator to take the time to do extra configuration work, but these steps often pay off in the long run.

It is easy to assume that your backup software will let you know when a problem occurs. However, on screen messages do little good unless you just happen to be looking at the console at the time when the problem occurs.

By configuring alerts and notifications you can be made immediately aware of any backup related problems that occur. Although the initial alert configuration process involves a small time commitment, doing so will likely save you time in the long run because you won't have to check on the backup server as often.

8 TESTING AND VERIFICATION

Backup testing is the only way to know for sure that a backup will work when it is needed.

It is important to understand that testing and verification are two completely different things. Verification is a function within the backup software that compares the contents of the backup media against the original data as a way of ensuring that no backup errors exist. Testing involves performing a restoration of the data in order to make sure that the backup can be used in times of crisis.

On the surface, testing and verification seem like the same thing. However, it is possible for a backup to be verified, but still be bad. Verification only confirms that the data on the backup media matches the data on the servers that are being backed up. It does not verify that the data is good. Imagine for a moment that the system files required to boot a server were accidentally deleted. These files are only used during the boot process, so the server would continue running without them. The problem would only become obvious when the server was rebooted. In this type of situation, a backup would be successfully verified because everything on the server is presumably backed up, but restoring the backup would still result in an unbootable server if the backup was created after the system files were already deleted. Backup testing would allow an administrator to proactively find and correct the problem.

There are a number of different types of backup testing. When testing your backups, you should test your ability to restore an entire physical server, but you should also test your ability to recover at various levels of granularity. For instance, you might test an application level restoration and a VM level restoration.

9 SECURITY

Another important best practice is to consider your security needs as you plan for your backups. Remember that without proper security there is little stopping someone from stealing your backup drives, restoring them on their own servers, and gaining access to all of your data.

Most backup applications will allow you to secure your backup media using encryption. By encrypting the backup media, the media becomes unusable to anyone other than you, the owner of the unique encryption key. Consequently, you will not have to worry about data leakage in the event that a piece of backup media is stolen.

If you do opt to encrypt your backups then it is critically important that you export a copy of your encryption keys and store those keys offsite in a secure location. Remember that without the encryption keys you will be unable to restore your own backups.

There have been documented, real world situations in which organizations have lost all of their data even though they had a perfectly good backup simply because the organization's encryption keys were lost due to a datacenter level disaster.

10 SELECT A BACKUP SOLUTION THAT SUITS YOUR NEEDS

One final best practice is to choose the best backup solution for your organization. Remember, there are dozens of backup products that are available for use. The one thing that most of these products have in common with one another are that they claim to be the best. Even so, the best backup product in the world does little good if it doesn't meet your organization's needs and gives you confidence in keeping your VMs protected reliably. It is therefore in your organization's best interest to evaluate your data protection needs and then compare those needs to the available solutions rather than merely purchasing a backup product that someone recommended.

Does the solution you're evaluating allow you the flexibility you need to store backups in multiple locations, with zero impact on your live environment? Will you be able to retrieve individual files or emails without having to restore a full VM? Do you have the ability to run automated integrity tests and verify backups stored? Can the solution be used by anyone in the team, so that recovery doesn't depend on a few expert users who may not be available at the time of an incident?

The previously discussed best practices should help you to narrow down the capabilities that would be the most beneficial to you and your organization. Above all though, the solution that you choose needs to be cost effective, easy to use, and support for the product must be readily available, effective and fast.

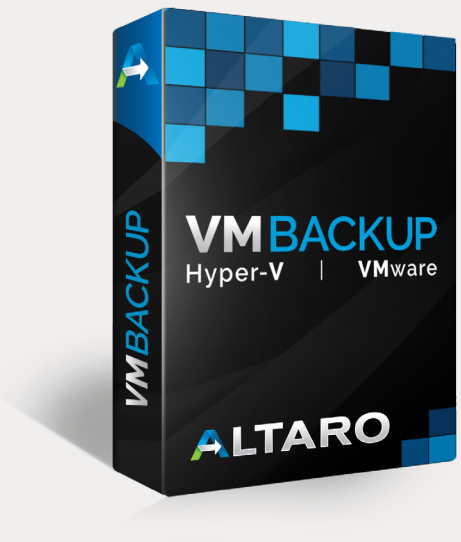
CONCLUSION

Although most organizations back up their virtual machines, there have been many documented instances of administrators finding out the hard way that their backups are unusable. The best ways to avoid this nightmare scenario are to frequently test your backups and to adhere to established best practices for data protection.

VM BACKUP
Hyper-V | VMware

If you're looking for a backup solution to protect your Hyper-V and/or VMware VMs that ticks the boxes for all of these best practices, have a look at Altaro VM Backup. It's designed to be easy to use, install and configure and you'll be up and running in a matter of minutes.

You get all the flexibility and functionality you need for a rock solid backup and recovery strategy, at an affordable price. Benefit from unbeatable value, outstanding support and a backup solution that protects Hyper-V and VMware VMs from a single console, across all your hosts.



Hassle-free and effective

Unbeatable value

Outstanding Support

DOWNLOAD A 30-DAY TRIAL

WATCH A 10-MIN DEMO

ALTARO

More info: altaro.com/vm-backup/

ABOUT ALTARO

Altaro is a fast-growing developer of easy to use and affordable backup solutions for small- to medium-sized businesses, specializing in backup for virtualized environments.

Our aim is to delight our customers with full-featured, affordable backup software backed by an outstanding, personal Support team who are determined to help you succeed in protecting your environment.

ABOUT THE AUTHOR

Brien Posey is a 14 time Microsoft MVP with over two decades of IT experience. Prior to going freelance, Brien worked as CIO for a national chain of hospitals and healthcare facilities. He has also served as a network engineer for the United States Department of Defense at Fort Knox and as a network administrator for some of the country's largest insurance companies. In addition to his work in IT, Brien is currently training to be a civilian astronaut. You can access Brien's Web site at http://www.brienposey.com