



for VMware

VEEAM BACKUP & Replication

- 2-in-1: Backup and Replication
- Support for ESXi and ESXi
- File Level Recovery for Windows & Linux

VMware and Microsoft VSS:

How to correctly backup and recover Microsoft SQL, Exchange, Active Directory and SharePoint in VMware environment

Written by:

Anton Gostev

Product Manager

Veeam Software

CONTENTS

- EXECUTIVE SUMMARY 3
- VSS AWARE BACKUP IN VMWARE 5
- VSS AWARE RESTORE IN VMWARE..... 6
- TESTING YOUR APPLICATION DISASTER RECOVERY PLAN 7
 - PREPARING A TEST LAB 7
 - PERFORMING A BACKUP..... 7
 - SIMULATING POST-BACKUP ACTIVITY AND DISASTER 8
 - PERFORMING A RESTORE..... 8
 - Confirming a Correct Restore 8
 - Confirming an Incorrect Restore..... 9
- CONCLUSION 10
- ABOUT VEEAM SOFTWARE 11

EXECUTIVE SUMMARY

More and more organizations are choosing VMware Infrastructure to virtualize their mission-critical applications (Active Directory, Exchange, SharePoint, SQL Server) to create a flexible, easily administered virtual infrastructure.

Virtual machines (VMs) and any applications they contain must be protected against failure. Typically, in the virtual world, this is done by performing an image-level backup of the whole machine (for instance, using VMware Consolidated Backup). This method results in what is known as a crash-consistent image. Restoring a crash-consistent image is essentially equivalent to rebooting a server after a hard reset. For operating systems, this has not been an issue, since they can easily handle this type of activity. For database applications as well as for applications featuring replication, however, such a restore will often result in lost data, data corruption, or application failure.

To illustrate this concept, let's review the consequences of using different VM disaster recovery methods for one of the most common mission-critical applications: a Microsoft Active Directory domain controller (DC). Depending on the solution used, the following results will be achieved:

VMware Disaster Recovery Solutions	Image Level Backup	VSS Aware Backup	VSS Aware Restore	Disaster Recovery Result
• VMware snapshot made with VC or VI Client user interface • VMware Consolidated Backup (prior to ESX 3.5 Update 2) • SAN snapshot	X			DC is not functional. To recover the DC, you need to forcibly demote it, and then reinstall it.
• Vizioncore vRanger Pro	X	X		DC is not functional. To recover the DC, you need to forcibly demote it, and then reinstall it.
• Veeam Backup • VMware Consolidated Backup (ESX 3.5 Update 2 with VMware Tools VSS support installed)	X	X	X	DC is fully functional. No additional steps are required for DC recovery.

To facilitate a correct application backup, application vendors provide various means for creating a consistent backup of the application and database data. One example is Microsoft Volume Shadow Copy Service (VSS). Using VSS along with an image-level backup of virtual machines (VM) running supported applications allows you to create a transactionally consistent backup image. With such a backup image, you can successfully recover both the VM, and any supported application installed on the VM.

Of course, the only purpose of a backup is recovery. And in the case of VSS-integrated backup and restore, it is critical to properly initialize the application, instructing it to perform the restore procedure from the shadow copy instead of performing a regular start up. Otherwise the application will not restore properly. In other words, an improperly restored transactionally consistent backup image is no more valuable than

the restoration of a crash-consistent image, with both scenarios potentially resulting in data loss or application failure.

This white paper provides guidance on how to easily test and verify whether your current backup approach is able to correctly handle the backup and restore of mission-critical Windows applications. We strongly encourage all organizations to verify their backup approach using this simple test to ensure that the solution you have chosen is able to back up and correctly restore all your VMs hosting mission-critical Windows applications.

VSS AWARE BACKUP IN VMWARE

According to industry analysts' estimations, it is expected that in 3 to 5 years the typical enterprise will have at least half of its currently physical servers virtualized. The VMware Infrastructure is the industry's most widely deployed virtualization solution. More and more companies are choosing VMware Infrastructure to virtualize their mission-critical applications (Active Directory, Exchange, SharePoint, SQL Server) to create a flexible, easily administered virtual infrastructure.

Virtual machines (VM) and the applications they run must be protected against failure, so they require backup and recovery no less than physical systems do. However, virtual system backup is typically done differently from physical system backup. For more information on backup approaches, please refer to the white paper written by Enterprise Management Associates analyst Andi Mann: "[Virtualization Management Best Practices: Critical Aspects of Virtual System Backup and Recovery](#)".

Virtual machine backup is usually performed by executing an image-level backup of the whole VM using special VM backup tools (for instance, VMware Consolidated Backup). Such tools can only provide what is known as a crash-consistent image, meaning that the image captures the VM in a crash state with file system not being static (open files, incomplete write operations, unflushed file system buffers and incomplete application transactions). Restoring a crash-consistent image is essentially equivalent to rebooting a server after a hard reset. For operating systems, restoration from a crash-consistent image is not an issue, since most operation systems easily handle this type of activity. However, for applications involving any sort of transactional databases, or replication functionality, restore from a crash-consistent image will often result in the loss or corruption of data, which in turn could lead to application failure.

Backup of this type of application has been a problem in the physical world as well. To address this issue and to facilitate correct application backup, application vendors provide various means for creating consistent backups of the application's data. This is achieved by coordinating backup activities with database applications' business logic, the database engine itself, and OS file system services.

One example of this technology is Microsoft Volume Shadow Copy Service (VSS). VSS supports all mission-critical Microsoft applications that require consistent application backup, including Active Directory, Microsoft Exchange, SQL Server, and SharePoint. All these applications are specially designed to work with VSS, processing VSS instructions to perform a full application and database freeze, and preparing applications' files for the restoration procedure (this type of restore is usually referred as "restore from a shadow copy"). Leveraging VSS ensures transactionally consistent backups of database and application files, meaning there are no unfinished database transactions or incomplete application files. Such backups, when restored correctly, result in a fully functional application.

Using VSS technology along with image-level backups of virtual machines running supported applications, VM backup vendors can ensure that their solutions create transactionally consistent backup images. To achieve this, VSS functionality known as "VSS freeze" is leveraged when a VM image is created during the backup procedure. Unlike crash-consistent images, such backup images give you the ability to successfully recover both the VM and any supported application installed on the VM.

VSS AWARE RESTORE IN VMWARE

It goes without saying that the only purpose of a backup is recovery. Backup is usually relatively easy, yet too many people focus their attention completely on the speed and efficiency of backups. Restore can be much more challenging – and that's when the clock is ticking loudest.

With image-level backups, VM restore may seem simple and straightforward in most cases. All that needs to be done is simply recover the image on the host server and start the VM. However, this will not work well for VMs hosting applications featuring transactional databases and replication functionality.

In the physical world, application vendors usually provide comprehensive step-by-step guides explaining what application-specific restoration steps should be performed to ensure a successful restore from the backup made with VSS. If these steps are not followed carefully, the application will not be restored properly, and will in many cases end up failing, rendering the whole disaster recovery procedure useless.

Restoring VMs with applications in the virtual world requires the exact same considerations. Even with transactionally consistent backup images made by leveraging VSS, many applications will not be restored correctly by simply restoring the VM image and starting it. To ensure the successful restore of such applications, it is critical to properly initialize the application during the first VM start up, instructing the application to perform the restore procedure from the shadow copy, instead of performing a regular start up.

If restored improperly, without following the restoration steps, a transactionally consistent backup image is no more valuable than a crash-consistent one, as in both cases you are likely to end up with application failure.

TESTING YOUR APPLICATION DISASTER RECOVERY PLAN

While testing your backup and recovery procedures can be a challenge in the physical world, it is easy to perform in a virtual infrastructure. Below you can find guidance on how to test and verify whether your current VMware backup approach is able to correctly handle backup and restore of a mission-critical database application.

While Microsoft Active Directory domain controllers were selected as a test subject as one of the most common mission-critical applications, everything written in this paper still applies to other common database applications, such as Microsoft Exchange.

Preparing a Test Lab

It is recommended that you do not use your production network as a test lab, and instead create a separate lab not connected to your production network.

The following hardware and virtual machines will be required to perform the testing:

- 1 ESX server to host your lab computers
- 2 VMs running Microsoft Windows Server 2003 (SP1 or later is preferred for easier detection of failed restore)
- Additional VMs as needed to host your VM disaster recovery solution

As soon as you prepare the hardware, follow these steps to prepare your lab for testing:

- Assign clear names to both of your Microsoft Windows Server 2003 machines, for instance DC1 and DC2
- Promote DC1 to the domain controller role, using the DCPROMO command. In the DCPROMO wizard, use all default settings and choose to create a new forest (for instance, *contoso.com*). Wait for DC1 promotion to fully complete before proceeding to the next step.
- Similarly, promote DC2 to the domain controller role. In the DCPROMO wizard, instead of creating a new forest, choose to make DC2 a domain controller of the root domain of the existing forest that you have created in the previous step.
- Ensure that DNS in your lab is configured correctly (some disaster recovery applications might refuse to work correctly if DNS is not configured properly). The easiest way to set up DNS in the lab conditions is to simply use an AD-integrated DNS server.
- Run the domain controller diagnostic tool (DCDIAG.exe) on both controllers to verify that both domain controllers are functioning normally.
- Verify that the system event logs on both domain controllers have no replication errors, and that replication is working normally between the two domain controllers (you can test this by changing some object's attribute value on one DC, and observing this change replicated to the other one).
- Install and configure your VM disaster recovery solution in the same lab.

Alternatively, you can simply copy virtual machines from your production environment to the test lab (just be sure that your test lab is completely isolated).

Performing a Backup

When you are ready to continue with the testing, perform a backup of one of the live domain controllers using your VM disaster recovery solution. Ensure that you use VSS

integration (if this functionality is provided by your backup solution), so that the created backup is transactionally consistent.

Simulating Post-Backup Activity and Disaster

In order to test the real-world situation of a domain controller backup, you need to generate some directory updates on both domain controllers after the backup is performed. To do this, connect to DC2 with the Active Directory Users and Computers snap-in, and create a few new users.

Be sure to wait for a few moments for the replication between DCs to complete, and the newly created users to be replicated to DC1. Then simulate a disaster by performing a hard shut-down of the DC2 domain controller, leaving DC1 intact and running.

Performing a Restore

Now recover the shut down domain controller using your disaster recovery solution from the backup you created earlier, start the domain controller, and proceed to review the recovery results.

Proper domain controller restore can only be achieved if your VM disaster recovery product features complete VSS support, including both leveraging VSS freeze to create transactionally consistent backups, and VSS-aware application restore procedure, which instructs the application to restore itself from the shadow copy, instead of performing a regular start up.

Since disaster recovery solutions with partial or missing VSS support simply start up the domain controller, instead of following the required restore procedure, such “recovery” causes the domain controller to fail.

To test whether your domain controller recovery was successful, connect to the recovered domain controller DC2 with the Active Directory Users and Computers snap-in, and create additional test users. Then wait for a few moments for replication between DCs to complete, and verify if the newly created users are replicated to DC1 successfully.

To confirm the result you are seeing, simply review the event log of the restored domain controller for the presence of the events listed below.

Confirming a Correct Restore

If your disaster recovery application features full and correctly implemented VSS support, the successful domain controller restore should be verifiable with the following system Event Log messages appearing:

Event Type: Information

Event ID: 1920

Description: Active Directory shadow copy restore was successful.

and

Event Type: Information

Event ID: 1109

Description: Active Directory has been restored from backup media, or has been configured to host an application partition. The invocationID attribute for this domain controller has been changed.

If you see these events, it means that your restore procedure was performed correctly, and your domain controller is fully functional.

If you do not see these events, it means that your domain controller was restored incorrectly, and is likely placed into a failing state as described in the following chapter.

Confirming an Incorrect Restore

In case of an incorrect restore of an Active Directory domain controller from backup, the domain controller is put into the condition known as an Update Sequence Number rollback, or USN rollback. When a USN rollback occurs, modifications to objects and attributes that occur on the recovered domain controller do not replicate to other domain controllers in the forest, because the other domain controllers believe they already have an up-to-date copy of the Active Directory database. Depending on how old your backup is, and how many directory updates happened after the backup was made, the size of the USN hole may represent hundreds, or even thousands of changes to users, groups, computers, passwords, trusts etc..

On earlier versions of Windows Server, the USN rollback condition causes no replication errors reported in Directory Service event logs, while monitoring and diagnostic tools such as **Repadmin.exe** do not report any replication errors. Replication simply does not work, and you might not even notice this until users start complaining about incorrect group membership, password problems etc. However, Windows Server 2003 SP1 or later is able to detect and report the USN rollback situation when it encounters the issue, and Windows protects your Active Directory by automatically disabling inbound and outbound replication with the affected domain controller.

So, if you are using a Windows Server 2003 SP1 or later domain controller, you would observe the following events in the Event Log after the restored domain controller is first started after an improper restore.

Event Type: Error

Event ID: 2095

Description: During an Active Directory replication request, the local domain controller (DC) identified a remote DC which has received replication data from the local DC using already-acknowledged USN tracking numbers. Because the remote DC believes it is has a more up-to-date Active Directory database than the local DC, the remote DC will not apply future changes to its copy of the Active Directory database or replicate them to its direct and transitive replication partners that originate from this local DC. If not resolved immediately, this scenario will result in inconsistencies in the Active Directory databases of this source DC and one or more direct and transitive replication partners. Specifically the consistency of users, computers and trust relationships, their passwords, security groups, security group memberships and other Active Directory configuration data may vary, affecting the ability to log on, find objects of interest and perform other critical operations. The most probable cause of this situation is the improper restore of Active Directory on the local domain controller. **Event User Actions:** If this situation occurred because of an improper or unintended restore, forcibly demote the DC.

and

Event Type: Error

Event ID: 2103

Description: The Active Directory database has been restored using an unsupported restoration procedure. Active Directory will be unable to log on users while this condition persists. As a result, the Net Logon service has paused.

Along with these errors, you would also receive additional warnings (Event ID 1113 and 1115) stating that inbound and outbound replication has been disabled by the user.

The only way to recover a DC from rollback is to forcibly demote the domain controller, and reinstall it. If the domain controller in question is used to hold FSMO roles, you will need to use **Ntdsutil.exe** to transfer these roles to another DC to ensure that your production Active Directory does not stop functioning completely as a result of the improper restore of a single domain controller.

For more information about detecting and resolving USN rollback issue, please refer to the following support KB article <http://support.microsoft.com/kb/875495>.

CONCLUSION

As you can see based on the provided example, some applications cannot be restored correctly by simply starting up the VM image. Many VSS-aware applications, especially those featuring replication, require a certain sequence of actions to be restored from a backup made by leveraging VSS. Similarly to the domain controller example we have reviewed, Microsoft Exchange Server is another example of a critical application that must be restored using an application-specific restore technique (please refer to the following support KB article for more information <http://support.microsoft.com/kb/822896>).

Even in the case where a VM image created by a backup application is transactionally consistent, the restore could still fail because of not following the restoration steps recommended by the application vendor. For instance, in the case of a domain controller restore, for proper restore it is essential that the domain controller is first started in the Directory Services Restore Mode. If your VM disaster recovery solution does not facilitate the correct restore procedure, it is completely useless, regardless of any other functionality it may feature – because it is unable to fulfill its primary purpose, correctly restoring the VM.

To sum up, it is critical that your VM disaster recovery solution features VSS support. But it is not only the VM backup application's ability to *create* transactionally consistent backup image that you should be concerned with. Rather, you should ensure that your VM backup application feature *complete* VSS support, including both producing transactionally consistent backup images, and performing the correct restore procedure for all the applications hosted inside the VM images.

ABOUT VEEAM SOFTWARE

Veeam Software, a premier-level VMware Technology Alliance Partner and member of the VMware Ready Management program, provides innovative software for managing VMware vSphere 4 and Virtual Infrastructure 3. Veeam offers an award-winning suite of tools to assist the VMware administrator, including #1 for **VMware backup**: Veeam Backup & Replication; Veeam Reporter Enterprise, for **VMware performance, storage, capacity reporting** and chargeback; **Veeam Configurator**, offering complete host configuration management; and Veeam Monitor, for **VMware performance monitoring and alerting** across multiple vCenters. With its acquisition of nworks, Veeam's products include the **nworks Smart Plug-in** and the **nworks Management Pack** that incorporate VMware data into enterprise management consoles from HP and Microsoft. Learn more about Veeam Software by visiting www.veeam.com.