Virtual Domain Controller backups

How to tell whether your host-based backup solution can successfully restore virtual Domain Controllers for Disaster Recovery purposes running on Hyper-V 2.0

Sander Berkouwer
Preface
Running Active Directory Domain Controllers on any virtualization platform have caused serious headaches for many administrators. Whether Hyper-V, vSphere or XENServer is your choice of hypervisor, virtualized Domain Controllers potentially cause more problems than non-virtualized Domain Controllers.

Solving these problems before they actually harm the business is key, because in most environments when the Active Directory goes down, the entire network grinds to a halt. Authenticating into vCenter or starting up a Hyper-V cluster can be extremely challenging without Active Directory.

But even if you’ve planned everything meticulously and deployed it flawlessly, there’s still the need to operate the environment. A big piece in operations is continuity planning and the two big pieces in Active Directory continuity planning are replication and proper restores. For proper restores you’ll need proper backups.

This whitepaper discusses proper backups for Active Directory Domain Controllers running on Windows Server 2008 R2 Hyper-V.

About the author
Sander Berkouwer
Sander Berkouwer is a MCSA, MCSE, MCITP and Microsoft Most Valuable Professional (MVP) on Directory Services. He has ample experience with deploying and maintaining Windows, Windows Server and other Microsoft technologies within hundreds of environments, ranging from four to forty thousand seats. Sander blogs on The Things that are better left Unspoken, ServerCore.Net and the Dutch Microsoft IT Professional Community blog.

Disclaimer
All content provided on this whitepaper is for informational purposes only and is provided “AS IS” with no warranties, and confers no rights. The author makes no representations as to the accuracy or completeness of any information in this document or found by following any link in this document. The author will not be liable for any errors or omissions in this information nor for the availability of this information. The author will not be liable for any losses, injuries, or damages from the display or use of this information. This policy is subject to change at anytime.

Acknowledgements
Thanks to Altaro Software for their assistance in the research for this whitepaper.
Contents
Preface ........................................................................................................................................... 1
The benefits of host-based virtual machine backups ................................................................. 3
  Fewer agents equals fewer licenses ......................................................................................... 3
  Bandwidth optimization means less networking hardware .................................................. 3
  Resource optimization means a smaller backup window ..................................................... 3
  Virtualized backups mean virtualized restores ..................................................................... 3
The challenges related to Domain Controller backups and restores ............................................ 4
  USN Rollbacks ...................................................................................................................... 4
  Lingering objects ............................................................................................................... 6
Best Practices when backing up and restoring virtual domain controllers .............................. 9
  Deploy a minimum of two Domain Controllers per domain .............................................. 9
  Deploy (as) pure (as possible) Domain Controllers ......................................................... 9
  Configure the Directory Services Restore Mode (DSRM) .................................................... 9
  Undo disks, differencing disks and snapshots ..................................................................... 9
  Apply minimum patchlevels to virtual Domain Controllers ........................................... 10
  Install the Integration components .................................................................................... 10
  Do not restore Domain Controllers beyond the tombstone lifetime ................................ 10
  Backup and restore Domain Controllers the right way .................................................... 11
Identifying Active Directory-aware host-based backup solutions .......................................... 12
  Active Directory-aware backups ....................................................................................... 12
  Active Directory-aware restores ....................................................................................... 13
  Checking for event 1109 ................................................................................................... 13
  Checking the DSA Previous Restore Count ..................................................................... 14
Steps to perform when working with non-Active Directory-aware host-based backup solutions .. 16
  How to handle USN Rollbacks ......................................................................................... 16
    Windows Server 2003 and Windows Server 2003 R2-based Domain Controllers .............. 16
    Windows Server 2008 and Windows Server 2008 R2-based Domain Controllers ............ 18
  How to handle lingering objects ....................................................................................... 19
Summary .................................................................................................................................... 20
The benefits of host-based virtual machine backups

In traditional non-virtualized datacenters, servers get backed up using traditional methods. These include local backups to tape and shares and remote backups using backup agents. In all cases a locally installed program is responsible for making the backup. These methods have been optimized through the years with Volume Shadow Copy backups and application aware backups, but remain bound to the same principles.

Virtualization adds many benefits to running datacenters. Optimization of resources is often mentioned as a cost saving benefit. Backups, however, can also be added to the list of benefits. No longer do the traditional backup principles have to apply to virtualized servers. These servers run on top of virtualization hosts and/or on Storage Area Networks (SANs), collectively known as the virtualization platform. Virtualized servers can be backed up from the virtualization platform. Host-based backups can be a more cost effective way to backup virtual servers than the traditional methods:

Fewer agents equals fewer licenses
In a virtualized datacenter with a decent virtualization ratio a serious number of virtualized servers run on each virtualization host. Using the traditional backup method means installing an agent to each virtual server. This method requires an expensive backup agent license on each server. With host-based backups license is either required per host or per environment. In many licensing models a host-based backup license typically equals the licensing costs of six normal backup agent licenses.

Bandwidth optimization means less networking hardware
Host-based backups represent a bandwidth optimization when run through separate backup networks. In traditional non-virtualized environments to run backups over a dedicated backup network requires Network Interface Cards (NICs) for each server and networking infrastructure to tie everything together. Host-based backups require a single NIC per virtualization host. This equals less networking equipment.

Resource optimization means a smaller backup window
In traditional non-virtualized environments, backups are initiated sequentially from the media server(s) or written to a centralized backup location simultaneously. Host-based backups deliver the best of both worlds. Backups of virtual servers are initiated sequentially by each backup host and written simultaneously to a central backup location. This represents a low backup overhead load per virtualization hosts, while benefiting from an optimized backup window.

Virtualized backups mean virtualized restores
A host-based backup is an ideal path to perform a fast disaster recovery restore. Since a virtualization host known everything about the configuration of its virtual guests, it can backup both the contents of the disks and the accompanying configuration, including Processor, RAM and NIC settings. Restoring this backup package can then be done on any virtualization host, running the backup program. In a non-virtualized datacenter you’d have the need to purchase expensive and typical hardware running the same specs as the original box. In an environment with backup agents you would either have to purchase expensive Disaster Recovery licenses or configure a virtual server with the same specifications, install the Operating System and the backup agent on it and then perform a restore.
The challenges related to Domain Controller backups and restores

Over the years, we’ve seen a lot of issues with image-based backups of Domain Controllers. When you’re running an environment with a single Domain Controller you won’t encounter issues with this kind of backups, but when you’re running multiple Domain Controllers (a best practice), you might encounter USN Rollbacks. Also, when you don’t take into account your tombstone lifetime, you might end up with Lingering objects.

USN Rollbacks

Domain Controllers replicate changes. Whenever a change occurs on a Domain Controller, the Unique Serial Number (USN) of that Domain Controller increases. Each Domain Controller records the USNs it sees of its replication partners. This is recorded in the High Watermark Table. Replication partners are denoted using Invocation IDs in this table. The combination of USN and Domain Controller is captured as the up-to-dateness vector.

When you restore a Domain Controller to an earlier state, you would restore the USN to an earlier state. This is called an USN rollback.

Since its replication partners have seen a future USN for the Domain Controller, no changes will be replicated out until the restored Domain Controller reaches the USN recorded in the High Watermark Table. The effect is that user accounts and computer accounts that are created on the restored domain controller do not exist on replication partners. Or, the password updates that originated there do not exist on replication partners.

An example

Fabrikam has a Hyper-V host running Windows Server 2008 R2. Two virtual guests running Windows Server are hosted on the Hyper-V host. These two servers are Domain Controllers for the domain fabrikam.local. These two virtual servers are named DC1.fabrikam.local and DC2.fabrikam.local and are located within the same Active Directory domain and site. Replication occurs without problems.

Graphically this environment looks like this:
Looking at the High Watermark tables and Up-to-dateness vectors on each Domain Controllers, the following information becomes apparent:

<table>
<thead>
<tr>
<th>Domain Controller name</th>
<th>USN</th>
<th>InvocationID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC1.fabrikam.local</td>
<td>12787</td>
<td>de235686-7bc1-4412-941a-4f6e7e248be1</td>
</tr>
<tr>
<td>DC2.fabrikam.local</td>
<td>12382</td>
<td>471565bf-636d-4c7b-ac20-e96420df8517</td>
</tr>
</tbody>
</table>

This means DC1 knows all changes from its replication partner DC2 with InvocationID 471565bf-636d-4c7b-ac20-e96420df8517 up to USN 12382. DC2 knows all changes from DC1 with InvocationID de235686-7bc1-4412-941a-4f6e7e248be1. This looks like this:

Suppose we make a backup of DC1 at this point and after the backup we make some changes inside Active Directory on DC1. We create some users, reset some passwords and create a couple of computer accounts. After replication the situation looks like this:

As you can clearly see the changes get replicated without problems and the Unique Serial Numbers (USNs) on both Domain Controllers get updated.
Lingering objects
When you delete an object in Active Directory it doesn’t get deleted, it gets tombstoned. In this process all but its most critical attributes (objectGUID, objectSid, nTSecurityDescriptor uSNChanged and sIDHistory) are stripped and the changes are replicated between Domain Controllers. Only after the tombstone lifetime, the object gets deleted. This deletion takes place every 12 hours by the Garbage Collection process per Domain Controller.

In normal situations, the tombstone process allows Domain Controllers to have sufficient time to replicate the tombstones. However, when you restore a Domain Controller to a point in time beyond the tombstone lifetime, the process may fail and objects that you expect to have been deleted may still exist on some Domain Controllers. These objects are called lingering objects.
An example

Contoso has two locations. On each location a Hyper-V host exists, running Windows Server 2008 R2. On each of these hosts, a virtual Domain Controller keeps the domain corp.contoso.com up and running. The two Domain Controllers are called dc1.corp.contoso.com and dc2.corp.contoso.com. They are placed within different Active Directory sites of the same Active Directory domain. Replication occurs without problems over the WAN link between the two locations. Admins work in the location where DC1 resides. The location with DC2 has a dial-in server.

The WAN connection between the two locations isn’t very reliable (that’s an understatement). One day when the WAN connection was failing an admin deleted a user object on DC1. This user object belongs to a salesperson who was found guilty of fraud. Because the WAN connection was down, this change was not replicated. At night both Domain Controllers were successfully backed up. In this backup, the following depicts the state of the user account:

The WAN connection eventually came back online, but unfortunately that night was the last night backups of DC2 were successful. Seven months later one of the Hyper-V host fails. It is the host responsible for DC2. A new Hyper-V host gets placed and all virtual machines are restored to their last backup. Now, the situation looks like this:
In the past seven months the objects tombstone event was replicated between DC1 and DC2. After the tombstone lifetime had passed, the Garbage Collection process on both DC1 and DC2 had deleted all references to the user object.

Now, unfortunately, DC2 was restored to a moment in time where the user account still existed and DC1 did not receive the tombstone event. Suppose the USN rollback would have been taken care off, the object tombstone event will never reach DC2, since the object does not exist anymore on DC1.

The roaming user belonging to the deleted user account would be able to access resources through the dial-up server after this time. This, of course, poses a security risk.
**Best Practices when backing up and restoring virtual domain controllers**

When running Active Directory Domain Controllers as virtual guests the following can be described as best practices:

**Deploy a minimum of two Domain Controllers per domain**

A minimum of two Domain Controllers should be deployed in every environment, except for the smallest Small Business Server environment. Having two Domain Controllers allows the loss of one of the Domain Controllers with a minimal disruption of service.

Also, in environments with two Domain Controllers you can log on with domain credentials when you enter the Directory Services Restore Mode (DSRM).

**Deploy (as) pure (as possible) Domain Controllers**

Domain Controllers that don’t also have other roles and Active Directory-integrated applications (Microsoft Exchange Server for instance) installed can be restored much faster and easier. While this sounds like a waste of resources and licenses, it should not be that way. When you license the physical processors in the virtualization hosts with Windows Server Datacenter Edition, you are entitled to run unlimited Windows Server guests on them. Creating dedicated guests with Windows Server 2008 R2-based Domain Controllers suddenly sounds feasible.

**Configure the Directory Services Restore Mode (DSRM)**

On Windows 2000 Server and Windows Server 2003-based Domain Controllers, a Directory Services Restore Mode startup option is added to the boot menu automatically. After you start this mode, you can log on using the Directory Services Restore Mode (DSRM) password, set when you promoted the server to a Domain Controller. You can change this password with the instructions found in Microsoft Knowledgebase article 322672. I recommend changing the DSRM password on a regular basis and document them diligently. Remember the DSRM password is a per Domain Controller setting.

I recommend performing the same actions on Windows Server 2008 and Windows Server 2008 R2-based Domain Controllers. Also, the Directory Services Restore Mode startup option is not created by default on these two platforms. I have instructions to create the DSRM startup option on my blog here.

**Undo disks, differencing disks and snapshots**

Don't use undo disks, differencing disks or snapshots. These sets of functionality can be disastrous when used with virtual Domain Controllers. Microsoft recommends not using them, since they can result in loss of Active Directory information when the link between the original disk and the new information gets lost. Undoing changes on a Domain Controller may result in the same consequences.
Apply minimum patchlevels to virtual Domain Controllers
When deploying Active Directory Domain Controllers as Hyper-V Child Partitions be sure they have at least the following patchlevel:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack level</th>
<th>Additional hotfixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Server</td>
<td>Service Pack 4</td>
<td>KB885875</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>Service Pack 2</td>
<td>KB875495</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>Service Pack 1</td>
<td>- none -</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>- none -</td>
<td>- none -</td>
</tr>
</tbody>
</table>

Install the Integration components
Meeting the Service Pack level requirement allows you to install the Operating System as a Child Partition in Hyper-V and install the Hyper-V RTM Integration Components (ICs).

The purpose of these Integration Components is to enlighten the virtual guests and to provide drivers and services. Enlightened virtual guests know they are virtual machines and are therefore able to interoperate with the virtual host. Integration Components are also sets of drivers and services that help your Virtual Machines have more consistent state and perform better by enabling the guest to use the synthetic devices offered by the virtual host.

Do not restore Domain Controllers beyond the tombstone lifetime
To prevent lingering objects in your Active Directory environment, do not restore (virtual) Domain Controllers with backups that are older than the tombstone lifetime. The table below shows the default tombstone lifetimes in days per Windows Server version. It indicates the default tombstone lifetime for the Windows Server version that was used to create the forest. This is the tombstone lifetime when the default value has not been changed.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack level</th>
<th>Tombstone lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Server</td>
<td>- all -</td>
<td>60 days</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>- none -</td>
<td>60 days</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>Service Pack 1</td>
<td>180 days</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>Service Pack 2</td>
<td>180 days</td>
</tr>
<tr>
<td>Windows Server 2003 R2</td>
<td>Service Pack 1</td>
<td>60 days</td>
</tr>
<tr>
<td>Windows Server 2003 R2</td>
<td>Service Pack 2</td>
<td>180 days</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>Service Pack 1</td>
<td>180 days</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>Service Pack 2</td>
<td>180 days</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>- none -</td>
<td>180 days</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Service Pack 1</td>
<td>180 days</td>
</tr>
</tbody>
</table>

1 This Service Pack is included in Windows Server 2008.
2 This Service Pack is included when you install Windows Server 2003 R2
3 This Service Pack is included when you install Windows Server 2008
When you suspect the tombstone lifetime has been changed, use the following command to find the tombstone lifetime (also in days):

```
    dsquery * "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
    DC=domain,DC=tld" -scope base -attr tombstonelifetime
```

Where DC=domain,DC=tld represents the domain infrastructure. In the case of Fabrikam this would be DC=Fabrikam,DC=local. In the case of Contoso, this would be changed to DC=corp,DC=contoso,DC=com.

The above command line was truncated. It is a single command.

**Backup and restore Domain Controllers the right way**

Only use Active Directory-aware backup and restore programs to backup and restore Active Directory Domain Controllers, since the default checks of Active Directory consistency will only be performed when the Domain Controller is aware of a restore.

Copying the virtual hard disk (*.vhd file) while a virtual Domain Controller is running equals using an imaging solutions in traditional environments. Microsoft has always recommended not using imaging solutions for Domain Controller backups.

To make backups of virtual Domain Controllers, two supported ways exist:

- Use a host-based Active Directory-aware backup and restore program.
- Use an Active Directory-aware backup and restore program from within the Virtual Domain Controller. Using Windows Backup to perform a System State Backup within a guest falls under this category.

All other backup and restore techniques are not supported. These include but are not limited to image-based backups and restoration of single Active Directory-related files.
Identifying Active Directory-aware host-based backup solutions

So, backing up and restoring Active Directory the right way is a best practice and therefore when choosing for host-based backups you should Use a host-based Active Directory-aware backup and restore program. The remaining question is:

Is my host-based backup and restore program Active Directory aware?

Luckily, there is a way to tell.

I recommend testing your host-based backup and restore on the production Hyper-V environment with virtual domain controllers running a test domain. This way, you can determine whether the host-based backup solution of your choice works in your environment, without risking the integrity of your production Active Directory environment.

I have personally checked out several Backup solutions and found Altaro Hyper-V Backup the best host-based Hyper-V solution for Active Directory-aware backups and restores.

Active Directory-aware backups

If the backup solution is Active Directory-aware, Event ID 1917 would be recorded:

![Event Properties - Event 1917, ActiveDirectory_DomainService](image)
In Windows Server 2008 and Windows Server 2008 R2 this event would have source ActiveDirectory_DomainService and would be recorded in the Directory Services event log (in the Applications and Services Logs).

In Windows Server 2003 and Windows Server 2003 this event would have source NTDS Backup and would be recorded in the Directory Services root log.

**Active Directory-aware restores**

After a successful Active Directory-aware restore, Windows Server will take care of USN Rollbacks and the problems these might cause.

The way this is done, is quite ingenious. Since Domain Controllers do not replicate with each other through their (DNS) names but through InvocationIDs, simply resetting the InvocationID on the restored Domain Controller would present it as a new replication partner to the other Domain Controller(s).

After restoring a successful backup, you should focus on two things:

1. The InvocationID should be reset on the restored Domain Controller as indicated by event 1109;
2. The Directory Services Agent Previous Restore Count should have changed the value in registry;

**Checking for event 1109**

After you start the restored Domain Controller, whether or not it is connected on the same network as its replication partners, it should log event 1109.

This event clearly states Active Directory was aware of a restore and the InvocationID was changed. Both the old InvocationID and the new InvocationID will be logged, together with the Unique Serial Number (USN) the Domain Controller was restored to.

In Windows Server 2008 and Windows Server 2008 R2 this event would have source ActiveDirectory_DomainService and would be recorded in the Directory Services event log (in the Applications and Services Logs).

In Windows Server 2003 and Windows Server 2003 this event would have source NTDS Replication and would be recorded in the Directory Services root log.

A sample Event 1109 is displayed on the next page.
Checking the DSA Previous Restore Count

In addition to the InvocationID, the value for the DSA Previous Restore Count key in the registry gets upped. This key is found in HKLM\SYSTEM\CurrentControlSet\services\NTDS\Parameters.

If this key does not exist, it means the Domain Controller hasn’t been restored using an Active Directory-aware restore in its lifetime. In the screenshot on the next page, it is clear this restore was the first restore in its lifetime.

Although the screenshot on the next page was made on a Windows Server 2008 R2-based Domain Controller (The System Schema version key kinda gives it away…) you should see the DSA Previous Restore Count key get altered with every successful Active Directory restore on Windows Server 2003, Windows Server 2003 R2 and Windows Server 2008.
Steps to perform when working with non-Active Directory-aware host-based backup solutions

If a restore is not Active Directory-aware you should see the restored Domain Controller turn its back on other Domain Controller(s). This behavior occurs when all Domain Controllers run at least Windows Server 2003 with Service Pack 1. Also, the NetLogon service on the restored Domain Controller is paused and event ID 2013 is logged in the Directory Services log.

If you meet this situation your restored Domain Controller is in a USN Rollback state

How to handle USN Rollbacks

Luckily, when you’ve read the best practices and deployed your environment accordingly, there is a rather painful way to get out of this situation. It means demoting the restored Domain Controller to a member server in the domain, rebuild the server with a fresh copy of Windows Server and promote it back to a Domain Controller.

Windows Server 2003 and Windows Server 2003 R2-based Domain Controllers

When the restored Domain Controller was running Windows Server 2003 with Service Pack 1 or Windows Server 2003 R2, you should perform the following steps:

1. Demote the failed Domain Controller
   a. Log on to the failed Domain Controller
   b. Run `dcpromo.exe /forceremoval` from a command prompt or through the Run command in the Start Menu.
   c. Follow the on screen instructions
   d. Reboot the server
2. Run a metadata cleanup of the failed Domain Controller on a healthy Domain Controller
   a. Log on to a healthy Domain Controller with an account that is at least a member of the Domain Admins group.
   b. At a command prompt run the following commands:
      i. `Ntdsutil.exe`
      ii. `Metadata cleanup`
      iii. `Connections`
      iv. `Connect to server localhost`
      v. `Quit`
      vi. `Select operations target`
      vii. `List domains`
      viii. Now note the number in front of the domain name the failed Domain Controller belonged to.
      ix. `Select domain x`, where x depicts the domain the failed Domain Controller belonged to. An example of this command would be `Select domain 0`.

---

4 At the time of publishing of this whitepaper, Windows Server 2003 with Service Pack 2 was the lowest supported Windows Server version. All Domain Controllers should meet these requirements to be in a supported state.
x. **List sites**
   xi. Again note a number. This time the number represents Active Directory sites. Note the number of the Active Directory site the failed Domain Controller belonged to.
   xii. **Select site x**, where x depicts the site.
   xiii. **List servers in site**
   xiv. From the output of the above command, locate the failed Domain Controller. Note the number in front of the X500 name of the server.
   xv. **Select server x**, where x depicts the failed Domain Controller.
   xvi. **Quit**
   xvii. **Remove selected server**
   xviii. Read the warning. Then press **Yes**
   xix. **Quit**
   xx. **Quit**

c. In Active Directory Sites and Services (dssite.msc) delete the server object of the failed Domain Controller.

d. In Active Directory Users and Computers (dsa.msc) delete the failed Domain Controller from the Domain Controllers container. Select the ‘This DC is permanently offline and can no longer be demoted using the Active Directory Installation Wizard (DCPROMO)’ option. Reply to the typical ‘Are you sure?’ question with **Yes**.

3. **Remove references to the failed Domain Controller from DNS**
   a. Log on to a healthy Domain Controller or your DNS Server.
   b. Open the DNS Management tool (dns.msc) Remove the CNAME record in the _msdcs.root domain of the forest zone. Also delete the HOSTNAME and other DNS records you may come across referring to the failed Domain Controller.
   c. If the server was in use as a forwarder, change settings on other DNS servers with a new forwarder

4. **Take care of Global Catalog and Flexible Single Master Operations (FSMO) roles placement**
   a. If the failed Domain Controller was the only Global Catalog in the environment, make a healthy Domain Controller a global catalog, using Active Directory Sites and Services (dssite.msc). Microsoft Knowledgebase article 313994 explains this further.
   b. If the failed Domain Controller held any Flexible Single Master Operations (FSMO) roles, these roles should be seized on other Domain Controllers. Microsoft Knowledgebase article 255504 explains this step in full detail.

5. **Reinstall the failed Domain Controller with a fresh copy of Windows Server.** Give this server the same name and IP address(es) as the failed Domain Controller.

6. **Promote the newly created server to a Domain Controller using dcpromo.exe.**

7. **Check for proper replication after promotion and initial replication, using the following command:**

   dcdiag.exe /test:replications

---

5 Do not use a clone or non-sysprepied image for this purpose.
**Windows Server 2008 and Windows Server 2008 R2-based Domain Controllers**

The steps to repromote a failed Windows Server 2008 or Windows Server 2008 R2-based Domain Controller are basically the same as the steps to repromote a failed Windows Server 2003 or Windows Server 2003 R2-based Domain Controller, except step 2 is a whole lot shorter, since metadata cleanup is now automated.

You can initiate metadata cleanup in three ways:

(Each option presents a complete way to perform a metadata cleanup)

1. Delete the failed Domain Controller from Active Directory Sites and Services (dssite.msc), where you delete the ‘NTDS Settings’ object below the server object while connected to a healthy Domain Controller.
2. Delete the failed Domain Controller from the Domain Controllers container in Active Directory Users and Computers (dsa.msc) while connected to a healthy Domain Controller.
3. Perform an automated metadata cleanup from the command line. At a command prompt on a healthy Domain Controller run the following commands:
   a. `ntdsutil.exe`
   b. `metadata cleanup`
   c. `remove selected server DC1`, where `DC1` is used as an example of a failed Domain Controller. Replace it with the name of the actual failed Domain Controller.
   d. Read the warning. Then press `Yes`
   e. `Quit`
   f. `Quit`
How to handle lingering objects
Coping with lingering objects is a whole other game. You might not be aware of lingering objects, unless you keep an eye out for really unexpected Active Directory behavior. You don’t need to be sharp-eyed to notice lingering objects though. You can periodically check for them using the following commandline:

```
Repadmin.exe /removelingeringobjects <FQDN of Domain Controller with suspected lingering objects> <objectGUID of Domain Controller with correct data> <Distinguished Name of partition containing lingering objects> /advisory_mode
```

An example of this commandline for Fabrikam would be:

```
Repadmin.exe /removelingeringobjects DC2.fabrikam.local de235686-7bc1-4412-941a-4f6e7e248be1 DC=fabrikam,DC=local /advisory_mode
```

Where the Active Directory admin for Fabrikam found the ObjectGUID of DC1 through the following command:

```
dsquery * “CN=<hostname>,OU=Domain Controllers,DC=Fabrikam,DC=local”
-scope base -attr objectguid
```

If the environment has lingering objects, events 1946 will be logged for each lingering object in the Directory Services log on the Domain Controller hosting the lingering objects. These events would be marked by event 1938, marking the start of the detection process and event 1942, with the final detection summary.

To remove the lingering objects perform the earlier repadmin.exe command lines, but without the `/advisory_mode` switch.
Summary

Host-based backups present a cost-effective way to backup and restore virtual Domain Controllers for disaster recovery purposes. However, these kinds of backups and restores need to be Active Directory-aware. Also, the person responsible for restores should be careful not to restore a Domain Controller with a backup older than the tombstone lifetime.

Also, the Active Directory environment should be equipped with a minimum of two (as) pure (as possible) Domain Controllers per domain, each running the minimum patch levels to be able to run as virtual guests in a supported manner. Virtualization admins should refrain from snapshotting Domain Controller or placing them on differencing disks. The Hyper-V Integration Components should always be installed on virtual Domain Controllers.

If these requirements are not met, restoring a virtual domain controller results in USN rollbacks and/or lingering objects. When encountering these situations, often a complete rebuild of a Domain Controller is necessary to ensure Active Directory integrity and redundancy.

Choosing the right host-based backup solution is key.

A quick note about Altaro Hyper-V Backup

Personally, I recommend using Altaro Hyper-V Backup. Altaro Hyper-V backup lets you make Active Directory-aware backups. It allows you to restore these backups to the same host or other Hyper-V hosts running the product, with the network connection either connected or disconnected.

Altaro Hyper-V Backup is a safe solution. The product offers both host-based and file level restore. When restoring a virtualized domain controller the Altaro host-based restore should be used as like that you are restoring Active Directory in a supported way. You may be tempted to use the file level restore to restore individual Active Directory-related files (like ntds.dit) instead of the host-based restore but I don't recommend you to do that. When restoring virtualized domain controllers always use the Altaro host-based restore functionality.

As with any other product when restoring virtualized domain controllers make sure that the backup you are restoring is not older then the tombstone lifetime. More information about the tombstone lifetime can be found on page 10.

I’ve tested this solution thoroughly and found it complies with all host-based backup best practices. Altaro Hyper-V Backup is available in both a paid and a freeware edition. Download it here.

Because this product is such a great solution I did not have to think twice to write this whitepaper as a sponsored whitepaper.
Easy to use Host-Backup Solution for MS Hyper-V – Freeware Edition

Altaro Hyper-V Backup is a powerful Microsoft Hyper-V and CSV aware backup solution that easily backs up Microsoft Hyper-V Virtual Machines. Altaro Hyper-V Backup takes the guesswork out of backing up Hyper-V, you won’t find an easier to use or quicker to configure solution.

More Info Link:  http://www.altaro.com/hyper-v-backup/

Some of the features in Altaro Hyper-V Backup include:

- **Fully Hyper-V Aware**
  Does all the complex config connections and allows you to back up any instance in 5 clicks or less.

- **Agent-less (no in-VM agents needed)**
  Easy and to the point. Install on the Hyper-V host without installing anything within the virtual machine itself.

- **Hot Backups – Microsoft VSS Integrated**
  Back up live VMs with zero downtime by leveraging the Microsoft Hyper-V VSS Writer.

- **Restore to different Hyper-V host**
  Restore an individual or a group of VMs to a different Hyper-V host.

- **Backs up Hyper-V CSV clusters**
  Cluster CSV support for multiple node setups.

- **Restore Clones**
  Restore VMs to the same Hyper-V host but with a different name (cloned VM)

- **Supports Microsoft Hyper-V Server (Core Install)**
  Supports the the free Microsoft Hyper-V Server (core).

... And more.

Altaro Hyper-V Backup is available also in a Freeware Edition.

Download

Altaro Hyper-V Backup 30 Day Free Trial

Link:  http://www.altaro.com/hyper-v-backup/