Running a Domain Controller in Virtual Server 2005

Microsoft Corporation

Published: November 2004

Abstract

This white paper explains the requirements and conditions for running domain controllers in Virtual Server 2005 virtual machines. It describes possible and recommended scenarios for running domain controllers in virtual machines, including the advantages and disadvantages of each. To ensure proper and safe deployment, this paper includes software requirements as well as performance, storage, and security recommendations. It also includes examples of the effects of improper versus proper backup and restore of virtual hard disk files, an explanation of the importance of adhering to software and operational requirements for these processes, and a decision flow chart for ensuring appropriate response in the event of failures.

Contents

Introduction

Microsoft® Virtual Server 2005 is an enterprise-class virtualization solution for server consolidation and the efficient management of multiple operating system environments. Throughout this documentation, Virtual Server refers to both Virtual Server 2005, Standard Edition, and Virtual Server 2005, Enterprise Edition.

Virtual Server is a Microsoft Windows®–based server application that is optimized to provide virtualization of Windows Server™ 2003, Windows 2000 Server, and Windows NT™ 4.0 operating systems concurrently on a single physical server. Virtual Server is designed to run on industry standard X86-based servers (IA32), from entry-level through high-performance models.

With Virtual Server, you can install multiple Windows Server 2003 or Windows 2000 Server domain controllers in separate virtual machines on a single physical server that is running Windows Server 2003 and Virtual Server. In this way, you can effectively host multiple domains, multiple domain controllers for the same domain, or even multiple forests on one physical server that is running a single operating system.

This document is intended for IT administrators, engineers, and architects who are evaluating using Virtual Server to host domain controllers that are running Windows Server 2003 or Windows 2000 Server in virtual machines.

Overview

The combination of Virtual Server 2005 and Windows Server 2003 provides a platform that enables multiple services and applications to run concurrently in separate operating system configurations on the same physical computer.

A typical server configuration associates the hardware of a single computer with one operating system and the applications designed for that operating system. The hardware includes the mouse and keyboard, processor, memory, disk drives and drive controllers, video and network cards, and other physical devices. The operating system runs on and controls the hardware. Applications run on the operating system.

By contrast, the virtual machine technologies built into Virtual Server enable one physical server to run an array of operating systems and related applications concurrently. A virtual machine uses software and selected hardware devices to create an emulated operating environment. By using emulated hardware and the processor of the physical computer, each virtual machine works like a separate physical computer.

By running domain controllers in virtual machines, you can:

- Increase the number of domain controllers relative to the available hardware. This ability is particularly useful in test environments.

- Separate administrator rights and privileges among different types of administrators. When running Active Directory and applications on the same computer, you can independently control the rights and privileges of domain administrators, who require access to domain controllers, and application administrators, who do not.
- Build domain controller images without regard to hardware differences between imaging and production computers.

The ideal application for domain controllers running in virtual machines is to facilitate testing and piloting in pre-production environments. These environments are generally not as busy as the corresponding production environments, and lend themselves well to the use of Virtual Server technology.

In a production environment, deploying domain controllers in virtual machines carries significant risks to directory data if the instructions for handling virtual hard disk files presented in this document are disregarded. Therefore, before implementing domain controllers in virtual servers in a production environment, be sure to read and understand the risks that are described in "Backup and Restore Considerations," as well as the advantages and disadvantages that are presented in "Planning for Domain Controllers in Virtual Machines," later in this document.

For a detailed overview of Virtual Server 2005, see "Microsoft Virtual Server 2005 Technical Overview" on the Web at http://go.microsoft.com/fwlink/?linkID=34709. For deployment, operations, and technical reference information about Virtual Server, see "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.

Virtual Server Terminology

The following table lists key terms and definitions used when discussing Virtual Server 2005.

Virtual Server Terms

Term	Definition
virtual machine	A software-implemented computer that emulates a complete hardware system in a self-contained, isolated software environment and runs its own operating system. In this document, "virtual machine" refers specifically to emulated hardware systems that are implemented by Virtual Server 2005.
guest operating system	The operating system that runs within a virtual machine. A guest operating system runs in its own isolated software partition on a host operating system.
physical computer	The computer hardware that is running Virtual Server 2005 and that hosts one or more guest operating systems.
host operating system	The operating system that runs on the physical computer. Virtual Server is installed on the host operating system.

invocationID	An Active Directory attribute on the NTDS Settings object for a domain controller. This value identifies the domain controller (specifically, the version of the directory database on the domain controller) when it replicates directory data in the forest.
update sequence number (USN)	A tracking number that domain controllers increment every time an object is created, deleted, or updated locally. During Active Directory replication, this number helps determine which changes a source domain controller should replicate to a destination replication partner or the changes a destination domain controller should request from a source replication partner.
.vhd	The file name extension that stands for virtual hard disk. Virtual Server uses .vhd files to store virtual machines.
.vmc	The file name extension that stands for virtual machine configuration. Virtual Server uses XML-based .vmc files to store configuration information for virtual machines.

Guest Operating System Requirements for Domain Controller Virtual Machines

Deploying domain controllers running Windows 2000 Server or Windows Server 2003 in virtual machines that are implemented by Virtual Server 2005 is supported by Microsoft when the appropriate software updates are installed and the guidelines presented in this document are followed.

The 32-bit versions of the following guest operating systems support deploying domain controllers in Virtual Server 2005 virtual machines:

- Windows Server 2003 with updates included with Knowledge Base article 875495. To download this update, see article 875495, "How to detect and recover from a USN rollback in Windows Server 2003" in the Microsoft Knowledge Base on the Web at http://go.microsoft.com/fwlink/?LinkID=4441.
- Windows 2000 Server with Service Pack 4 (SP4) and with updates included with Knowledge Base article 885875. To download this update, see article 885875, "How to detect and recover from a USN rollback in Windows 2000 Server" in the Microsoft Knowledge Base on the Web at http://go.microsoft.com/fwlink/?LinkID=4441.

For detailed information about Virtual Server software and hardware requirements, including host and guest operating systems, see the "Virtual Server Deployment Guide" section of the "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.

Planning for Domain Controllers in Virtual Machines

When planning your Virtual Server implementation, assess the advantages and disadvantages of running domain controllers in virtual machines and determine how they affect your environment. For example, if you use Virtual Server 2005 to host domain controllers in a production forest, carefully consider the personnel who have access to the files that represent those virtual hard disks. These files are the equivalent of a domain controller that is installed on a physical server that is running in the production environment, and must be secured accordingly. Similarly, consider the potential effects of these files being copied and running simultaneously on the network. Each .vhd file represents a complete instance of Active Directory on a domain controller with a unique identity in the forest. Copying such an identity interferes with the operation of the distributed directory service.

Important criteria to analyze when considering a Virtual Server deployment include:

- **Consolidation.** Is it useful to reduce the number of physical computers that you administer?
- **Testing.** Do you want to test new applications or data without building a separate test environment?
- **Administration.** Is it advantageous to separate levels of credentials among multiple application and domain administrators? Can you protect virtual machine files against inappropriate file copying?
- **Deployment.** Do you have disparate hardware platforms that you must incorporate?
- **Performance.** Are your physical computers powerful enough to run multiple virtual machines without unacceptably reducing performance?
- **Security.** Do you have adequate physical security to ensure that virtual machine files are safe from tampering or theft?

The advantages and disadvantages related to these criteria are discussed in the following sections.

Advantages of Deploying Domain Controllers in Virtual Machines

The advantages of using Virtual Server to consolidate, secure, and deploy domain controllers might or might not outweigh the disadvantages. The advantages of using virtual machines to deploy domain controllers include the following:

- **Consolidation.** You can consolidate domain controllers onto a single server. For example, you can consolidate domain controllers for small domains onto one server. If you have multiple domain controllers in the hub site serving a small domain that has a presence in one or more other sites, you need not deploy multiple physical domain controllers to provide bridgehead server and redundancy support.
- **Testing.** Because you can run multiple domain controllers in virtual machines on a single host computer and because testing environments do not require high-performance domain controllers, you can have a configuration that represents your production environment inside your testing environment. You can represent dozens of domain controllers on a few physical computers that have the same Active Directory configuration (domains and sites) as your production domain controllers. You can test complex changes, such as schema changes or large-scale Active Directory site or replication changes, prior to deploying them in production.
- **Administration.** You can provide administrative separation of application service and data owners from directory service and data owners on the same server, thereby minimizing the number of domain administrative group members in your forest. Domain controllers do not have local account databases that store user and group accounts; rather, domain controllers store all accounts in the domain directory partition in the Active Directory database. Therefore, if applications and Active Directory are installed on the same physical computer, at least some of the application owners require administrative rights and privileges on that computer. Because the only administrative groups available for managing a domain controller are those that have rights in the domain, application owners are necessarily provided with domain administrative credentials. Providing domain-level rights and privileges to these administrators jeopardizes the security of the domain and of the forest if the domain is the forest root domain. By installing Active Directory in a virtual machine, you can separate the administration of the domain from the administration of applications that are installed in separate virtual machines on the same physical computer.
- **Deployment.** The Virtual Server emulated hardware environment, once created in a virtual machine, remains unchanged, regardless of the underlying native hardware to which you might transfer the virtual machine. For example, in a pre-production environment, the server hardware used when building the image might be significantly different from the intended production server. With Virtual Server, a virtual machine emulates a standard x86-based computer, including all the basic hardware components except the processor. Therefore, you can build and deploy domain controllers in virtual machines without regard for hardware dissimilarities of the respective physical computers.

Disadvantages of Deploying Domain Controllers in Virtual Machines

Because .vhd files are both easily used and easily misused, it is especially important to carefully manage them when they are deployed in a production environment. When considering whether to run domain controllers in virtual machines, it is absolutely essential to understand that mishandling virtual hard disk (.vhd) image files can result in forestwide corruption. It is extremely important to read this document carefully and understand the risks of running domain controller virtual machines in a production environment. Mishandling a .vhd file could be as easy as starting an older copy of a .vhd file or copying a .vhd file to a different place on the network and running multiple copies at the same time. Using multiple copies of the .vhd file that represents an already deployed domain controller to deploy additional domain controllers is extremely hazardous to your environment and is not supported.

Caution

Domain controllers that are running in virtual machines must be backed up and restored only by using an Active Directory-compatible backup and restore application such as NTBackup.exe. Any other method of backing up and restoring .vhd files is not recommended. Specifically, you must absolutely ensure that no personnel make copies of .vhd files that represent deployed domain controllers for the purpose of deploying additional domain controllers or for restoring a failed domain controller by starting the .vhd copy.

Weigh the advantages of deploying domain controllers in virtual machines against the following disadvantages.

- **Administration.** In a production environment, data corruption that can potentially affect the entire forest can result from deliberate or inadvertent misuse of .vhd files. Most notably, starting an outdated .vhd image in a production environment can cause extensive inconsistencies across the forest. Usually the effects of improperly restoring a .vhd image are mitigated by updates included with Knowledge Base article 875495 (on domain controllers that are running Windows Server 2003) or Knowledge Base article 885875 (on domain controllers that are running Windows 2000 Server with SP4). However, these updates are not guaranteed to protect data from improper restore operations under all circumstances. To protect your forest against the effects of improperly restoring a domain controller that is running in a virtual machine, you must ensure that administrators read and completely understand "Backup and Restore Considerations" later in this document.
- **Performance.** A domain controller that is running in a virtual machine does not perform as well as a domain controller that is running on native hardware. Expect a decrease in performance of 30% to 50% on a domain controller that is running in a virtual machine under heavy load compared to a domain controller that is running on native hardware of the same specifications. Other performance considerations include:

- Virtual Server supports virtual machine access to only one physical CPU. Although you can run Virtual Server on a multiprocessor computer, each virtual machine can use a maximum of one processor. Therefore, advantages of Active Directory multiprocessor capabilities are not available when running domain controllers in virtual machines.
- The following domain controller processes might be noticeably slower: operating system startup and shutdown, LDAP search response times, global catalog lookups, logon authentication, and disk access.

- **Security.** A significant security issue is the protection of .vhd files.
  - Handling image files: Anyone who handles or has other access to .vhd files must be highly trusted within the organization and a member of trusted security groups within the forest. Any user who has the ability to copy a .vhd file effectively owns the forest and its data. An attacker or unauthorized administrator could use a copied virtual machine file to compromise passwords or, in extreme circumstances, corrupt the forest.
  - Securing image files: Unlike the theft of a physical computer, theft of a .vhd file is more likely to go undetected. Consequently, you should secure the host operating system and the guest operating system .vhd files with the same physical and software restrictions you use to secure a physical domain controller. Such restrictions include controlling access to the files and auditing file access. For more information about securing image files, see "Security Recommendations" later in this document.

Deployment Considerations

When deploying domain controllers in virtual machines, consider the Active Directory administrative and operational requirements and the requirements of the applications and services that you use in your business. Certain domain controller roles are not good candidates for virtualization, and the placement of domain controllers relative to applications can affect how you manage your environment.

Virtual Machine Placement

In a production environment, give careful thought to where in the network you will place a domain controller that is running in a virtual machine. Good options are branch locations that service a small number of users and computers (no more than 20). Less desirable options are locations where mission-critical applications, such as Microsoft Exchange, require a domain controller that is capable of above-average performance.

Domain Controller Roles Not Suited to Run in Virtual Machines

Certain domain controller roles require a higher level of availability and performance than others. Domain controllers installed in virtual machines are not recommended for the following roles:

- Operations master role holders (also called flexible single-master operations, or FSMOs): PDC emulator, RID master, infrastructure master, domain naming master, and schema master.
- Global catalog servers that service Exchange clients. Exchange servers are highly dependent on the responsiveness of global catalog servers.
- Bridgehead servers. These servers send and receive intersite replication. In addition to being required to handle significant network traffic, bridgehead servers that experience performance issues can have widespread impact on other services.

For more information about operations master roles, see "Operations Masters Technical Reference" on the Web at http://go.microsoft.com/fwlink/?linkID=34735. For more information about global catalog servers, see "Global Catalog Technical Reference" on the Web at http://go.microsoft.com/fwlink/?linkID=34736. For more information about bridgehead servers, see "Active Directory Replication Topology Technical Reference" on the Web at http://go.microsoft.com/fwlink/?linkID=27912.

Virtualization Scenarios Possible with Domain Controllers

There are three main supported virtualization scenarios for combinations of domain controllers and application services:

- Domain controller running in a virtual machine on a guest operating system with application services running on the host operating system
- Domain controller running on the host operating system with application services running in a virtual machine on a guest operating system
- Domain controllers and applications running in virtual machines on separate guest operating systems with host operating system for administration only

The advantages and disadvantages of each of these scenarios are discussed in the following sections.

Domain Controller Running in a Virtual Machine with Application Services Running on the Host

This configuration has the following advantage:

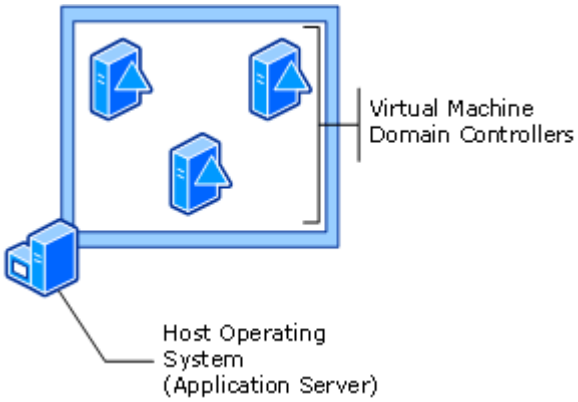
- Restarting the domain controller does not interrupt service by the applications.

This configuration has the following disadvantages:

- Domain controller performance is reduced due to virtualization.
- Restarting the application server interrupts service by the domain controller.
- If the application owner has local administrative rights, the owner can obtain access to the domain controller .vhd files. Although this configuration does provide administrative separation between application and domain administrators, it does not provide true security separation between domain and local computer administration.

The following figure illustrates this configuration.

Domain Controllers in Virtual Machines With Applications on the Host



Domain Controller Running on the Host with Applications Running in a Virtual Machine

This configuration has the following advantages:

- Roles for administration are separated. Application owners do not have to be members of the Domain Admins security group or otherwise be given high-level administrative rights and privileges in the domain.
- Restarting the application servers does not inherently interrupt service provided by the domain controller.

This configuration has the following disadvantages:

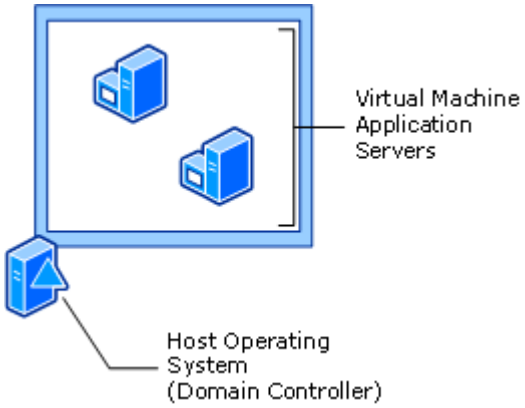
- Restarting the domain controller interrupts service provided by the application servers.
- Service principal names (SPN)s are not created automatically for constrained delegation.

Note

Constrained delegation is the ability to specify that a service or computer account can perform Kerberos delegation to a limited set of services. If the Virtual Server resource files (for example, .vhd files) are stored on a computer other than the computer that is running the Virtual Server service (Vssrvc.exe), you must configure constrained delegation. For more information about constrained delegation, see "Configuring constrained delegation" in the "Virtual Server Deployment Guide" section of the "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.

The following figure illustrates this configuration.

Applications in Virtual Machines With the Domain Controller on the Host



When setting the properties of constrained delegation for the computer account of the domain controller that is hosting the Virtual Server service, the SPNs for vssrvc/<NetBIOS name> and vssrvc/<fully qualified domain name (FQDN)> might not be not listed. In this case, you must add these SPNs manually by using Setspn.exe.

Setspn.exe is a command-line utility that is available as follows:

- For domain controllers that are running Windows Server 2003, Setspn.exe is available in Windows Support Tools. You can install Windows Support Tools from the \Support\Tools folder on the Windows operating system CD or by clicking Tools in Help and Support Center in Windows Server 2003.
- For domain controllers that are running Windows 2000 Server, Setspn.exe is a Windows 2000 Server Resource Kit tool that is available on the Web at http://go.microsoft.com/fwlink/?LinkId=35710.

After the appropriate SPNs are added manually, constrained delegation can be configured.

If you cannot configure constrained delegation due to missing SPNs, use the following procedure to register the SPNs on the domain controller that is running on the Virtual Server host computer.

To add SPNs for constrained delegation

1. On the domain controller that is running Virtual Server 2005 and for which you want to configure constrained delegation, open a command prompt.
2. At the command prompt, type the following commands, and press Enter following each:

```
SETSPN /A vssrvc/<NetBIOS name> <NetBIOS name>

SETSPN /A vssrvc/<FQDN> <NetBIOS name>

SETSPN /A vmrc/<NetBIOS name>:<VMRC port> <NetBIOS name>

SETSPN /A vmrc/<FQDN>:<VMRC port> <NetBIOS name>
```

   where NetBIOS name is the NetBIOS computer name of the domain controller, FQDN is the fully qualified DNS name of the domain controller, and VMRC port is the Virtual MachineRemote Control server port number (5900 by default). Because of the way

Setspn.exe processes information, you must type the NetBIOS name twice, separated by a space, where indicated.

Domain Controllers and Applications Running in Virtual Machines with No Application Services Running on the Host

This configuration has the following advantages:

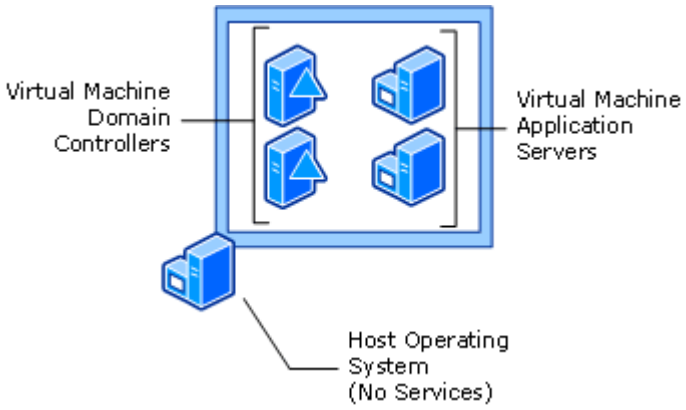
- Roles for administration are separated. Application owners do not need to be members of the Domain Admins security group or otherwise be given high-level administrative rights and privileges in the domain.
- Restarting the application servers or domain controller does not interrupt service provided by any virtual machine.
- The host operating system can be locked down by using a firewall or other security measures such as those discussed in the "Windows Server 2003 Security Guide" on the Web at http://go.microsoft.com/fwlink/?LinkId=34739.
- Only limited access to the host operating system is required for processes such as patch maintenance and updates to hardware drivers.

This configuration has the following disadvantage:

- Restarting the administration server interrupts service provided by the domain controllers and the application servers.

The following figure illustrates this configuration.

Applications and Domain Controllers in Virtual Machines With No Application Services on the Host



Selection of a Virtualization Configuration

When determining which of the three supported configurations you should use, employ the following guidelines:

- If you have a high-security environment with a high domain controller workload, place the domain controller on the host computer and run the application servers in virtual machines.

- If you do not have stringent security requirements but do have a high application service workload and a low domain controller workload, place the application service with the highest workload on the host computer and place all other application services and the domain controllers in virtual machines.
- If you have a high-security environment with a low-to-medium workload for the domain controllers and other application services, use a dedicated administrative host and place all applications and domain controllers in virtual machines.

Installation Recommendations

Adhering to the following performance, security, and storage recommendations during installation of domain controllers in virtual machines can improve the stability and effectiveness of your domain controller instances.

Performance Recommendations

You can improve performance by installing Virtual Machine Additions as soon as the guest operating system is up and running. Virtual Machine Additions is a set of features that improves the integration of the host and guest operating systems. It also improves the performance and manageability of the guest operating system. You must install Virtual Machine Additions on all virtual machines. Virtual Machine Additions adds the following enhancements to a guest operating system:

- Improved mouse cursor tracking and control.
- Greatly improved overall performance.
- Virtual machine heartbeat generator.
- Optional time synchronization with the clock of the physical computer. This feature is enabled by default and must be disabled for domain controllers that are running in virtual machines.
- Increased small computer system interface (SCSI) controller performance.
- Support for two-node clustering between virtual machines for testing and development scenarios.

Virtual Server adds the following registry key to the host operating system:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Virtual Server

The security on this registry key determines which users can view the Virtual Server event log.

The following registry key is added to the guest operating system:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Software\Microsoft\Virtual Machine

Virtual Machine Additions adds entries under this key to facilitate management. You can query the registry to determine information about the virtual machine and the physical computer that is running Virtual Server. For more information about these entries, see “Virtual Server registry

entries" in the "Virtual Server Technical Reference" of the "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.

Security Recommendations

It is recommended that .vhd files, including backup files, be as well secured as a physical server that is running as a domain controller. For information about how to secure domain controllers, see "Best Practice Guide for Securing Active Directory Installations" on the Web at http://go.microsoft.com/fwlink/?LinkID=28521.

To secure virtual machine domain controller files, complete the following tasks on the host computer during domain controller installation, and repeat them for all locations where system state backup files are kept:

- Be sure that only reliable and trusted administrators are allowed access to the domain controller .vhd files.
- Create a folder for storing all virtual machine domain controller files (.vhd, .vmc, and so on).
- Assign permissions to the folder that contains the .vhd and .vmc files so that only domain administrators have access to the folder. Additionally, ensure that the security account that Virtual Server is running under has access to the folder holding the .vhd and .vmc files.
- Audit Read\Write access to the .vhd folder and monitor the security logs for unauthorized access attempts.
- Secure the Virtual Server Administration Website tool (VSWebApp.exe) so that only privileged users have access to the Virtual Server service (Vssrvc.exe). The Administration Website is a browser-based tool for configuring and managing Virtual Server 2005 and its associated virtual machines and virtual networks. For information about securing Internet Information Services (IIS) and the Administration Website, see "Securing Virtual Server" in "Virtual Server Deployment Guide" of the "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?LinkID=27540.
- Use Group Policy to manage who can restart a host server that is running domain controllers on guest operating systems in virtual machines.

Storage Recommendations

Virtual Server 2005 emulates most of the hardware components for virtual machines. For SCSI storage, Virtual Server emulates the Adaptec 7870 SCSI adapter chip set. You can configure as many as four SCSI adapters on a virtual machine. Each SCSI adapter supports up to seven virtual hard disks of up to 2 terabytes each.

To optimize the performance of the domain controller virtual machine, follow these recommendations for storing operating system, Active Directory, and .vhd files:

Guest Storage Recommendations

Use the following recommendations for guest operating system files and Active Directory files:

- Store the operating system files on a separate virtual SCSI disk attached to SCSI port zero.

- Store the Active Directory database file (Ntds.dit), log files, and SYSVOL files on a separate virtual SCSI disk from the operating system files. Using virtual SCSI storage prevents a rare condition with Virtual IDE hard drives in which data loss could result from a power outage.

> **Note**
> For the Virtual Machine Additions accelerated SCSI adapter to be installed automatically, the SCSI controller must be installed in the virtual machine before installing Virtual Machine Additions.

Host Storage Recommendations

Host storage recommendations apply to storage of .vhd files. To obtain maximum performance, do not store the .vhd files on a busy disk, such as the system disk on which the host Windows operating system is installed. Store each .vhd file on a separate partition (ideally separate physical drives) from the host operating system and any other .vhd files.

Time Synchronization Recommendations

For virtual machines that are configured as domain controllers, the Host time synchronization feature of Virtual Machine Additions should always be disabled. Instead, accept the default W32time domain hierarchy time synchronization.

The Host time synchronization feature allows guest operating systems to synchronize their system clocks with the system clock of the host operating system. Because domain controllers have their own time synchronization mechanism, Host time synchronization must be disabled on virtual machines that are configured as domain controllers. If domain controllers synchronize time from their own source and also synchronize time from the host, the domain controller time can change frequently.

Use the Administration Website to disable Host time synchronization when the virtual machine is turned off. You can disable Host time synchronization during or after installing Virtual Machine Additions.

For information about how to use the Administration Website, see the "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.

Operational Considerations

You can use all the standard administrative tools that you use for managing any domain controller running on native hardware to manage domain controllers that are running in virtual machines. Managing the virtual machine itself is performed by using the Administration Website.

For domain controllers that are running in virtual machines, there are special recommendations related to the .vhd files that represent the domain controllers, and also some important restrictions. Backing up and restoring domain controllers running in virtual machines also

involve special considerations and recommendations for ensuring the proper creation of backups and the validity of restored virtual machine domain controller replicas.

Operational Restrictions

Domain controllers that are running in virtual machines have restrictions that do not apply to domain controllers that are not running in virtual machines. The following activities are not supported because they interfere with proper Active Directory replication:

- Do not use the Undo Disks feature on a virtual machine configured as a domain controller. Problems will occur with replication when you revert the virtual machine to an earlier state.
- Do not use a differencing disk as a virtual hard disk on a virtual machine configured as a domain controller. A differencing disk can be used to isolate changes to a virtual hard disk or the guest operating system by storing them in a separate file.
- Do not pause or store the saved state of a domain controller in a virtual machine for extended periods of time and then resume from the paused or saved state. Doing so can interfere with timely replication.

For information about Undo Disks, differencing disks, and pausing virtual machines, see the "Virtual Server Operations Guide" section of the Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.

Backup and Restore Considerations

Backing up domain controllers is a critical requirement for any environment to protect against data loss in the event of domain controller failure or administrative error. If such an event occurs, it is necessary to roll back the system state of the domain controller to a point in time prior to the error or failure. The supported method of restoring a domain controller to a healthy state is by using an Active Directory-compatible backup application to restore a system state backup that originated from the current installation of the domain controller.

With the advent of virtual machine technology, certain requirements of Active Directory restore operations take on added significance. One requirement—the updating of the database version on a domain controller when it is restored from backup—is skipped if you simply make a copy of a .vhd file to back it up and then restore a domain controller by starting the backed-up copy. If you do so, replication will proceed with inappropriate tracking numbers, resulting in an inconsistent database among domain controller replicas. In most cases, this problem goes undetected by the replication system and no errors are reported, despite inconsistencies between domain controllers.

Software updates for the Windows Server 2003 and Windows 2000 Server operating systems enable detection of some instances of improper system state rollbacks on domain controllers.

> **Important**
>
> The software updates that are available for download with Knowledge Base article 875495 and 885875are not guaranteed to detect 100 percent of improper rollback conditions. When only minimal changes are affected by the rollback condition, the problem might not be detected.

To download these updates, see article 875495, "How to detect and recover from a USN rollback in Windows Server 2003" for domain controllers that are running Windows Server 2003, or article 885875, "How to detect and recover from a USN rollback in Windows 2000 Server," for domain controllers that are running Windows 2000 Server with SP4, in the Microsoft Knowledge Base on the Web at http://go.microsoft.com/fwlink/?LinkID=4441.

The details of the way the replication system tracks directory changes, the process of recovery following a restore procedure, and the operating system changes that protect against inappropriate replication are described in this section. This information is provided to explain the changes that are applied by the updates that are recommended if you plan to run Windows Server 2003 and Windows 2000 Server as guest operating systems in virtual machines that are configured as domain controllers.

Background: Replication Update Tracking and Database Version

Domain controllers use a tracking system for changes they receive from their replication partners. Information is exchanged prior to replication that indicates to the source domain controller the level of changes that the destination has already received and, therefore, does not need. This information includes the following:

- Update sequence numbers: Values that indicate the latest changes a domain controller has originated or received through replication.
- Replication identity (invocation ID): The identity of the directory database of the domain controller.

Update Sequence Numbers

Domain controllers that are running Windows 2000 Server and Windows Server 2003 use update sequence numbers (USNs) to track updates originating from the local domain controller. For each directory partition that a destination domain controller stores, it uses USNs to track the latest originating update it has received from each source replication partner, as well as the status of every other domain controller that stores a replica of the directory partition. When a domain controller is restored following a failure, it queries its replication partners for changes with USNs greater than the USN of the last change it received from each partner prior to the time of the backup.

Two values that contain USNs are used by source and destination domain controllers to filter updates when the destination requests changes from the source replication partner:

- **Up-to-dateness vector**. The current status of the latest originating updates to occur on all domain controllers that store a replica of a specific directory partition. Because the up-to-dateness vector contains originating updates for all domain controllers and because the source provides its up-to-dateness vector to the destination following replication, the destination domain controller can also track non-originating updates that it has received through replication.
- **High-watermark (direct up-to-dateness vector)**. The latest originating update to a specific directory partition that has been received by a destination from a specific source replication partner during the current replication cycle.

Both of these values also specify the invocation ID of the source domain controller.

Directory Database Identity (Invocation ID)

In addition to USNs, domain controllers keep track of the identity of the directory database of source replication partners. The identity of the directory database running on the server is maintained separately from the identity of the server object itself. The directory database identity on each domain controller is stored in the **invocationID** attribute of the NTDS Settings object (cn=NTDS Settings,cn=*ServerName*,cn=Servers,cn=*SiteName*,cn=Sites,cn=Configuration,dc=*ForestRootDomain*). The server object identity is stored in the **objectGUID** attribute of the NTDS Settings object. The identity of the server object never changes. However, the identity of the directory database changes when a system state restore procedure occurs on the server or when an application directory partition is added or removed from the server.

Consequently, the invocation ID effectively relates a set of originating updates on a domain controller with a specific version of the directory database. When Active Directory is properly restored on a domain controller, the invocation ID is reset and the new value is replicated to all domain controllers in the forest. In response to this change, other domain controllers in the forest update their high-watermark and up-to-dateness USNs to match the highest USNs contained in the system state of the restored domain controller. In this way, partner domain controllers recognize the restored domain controller's highest USN as current rather than old.

The invocation ID is a GUID-based value that is visible at the top of the output of the command **repadmin /showrepl** (**/showreps** on domain controllers that are running Windows 2000 Server).

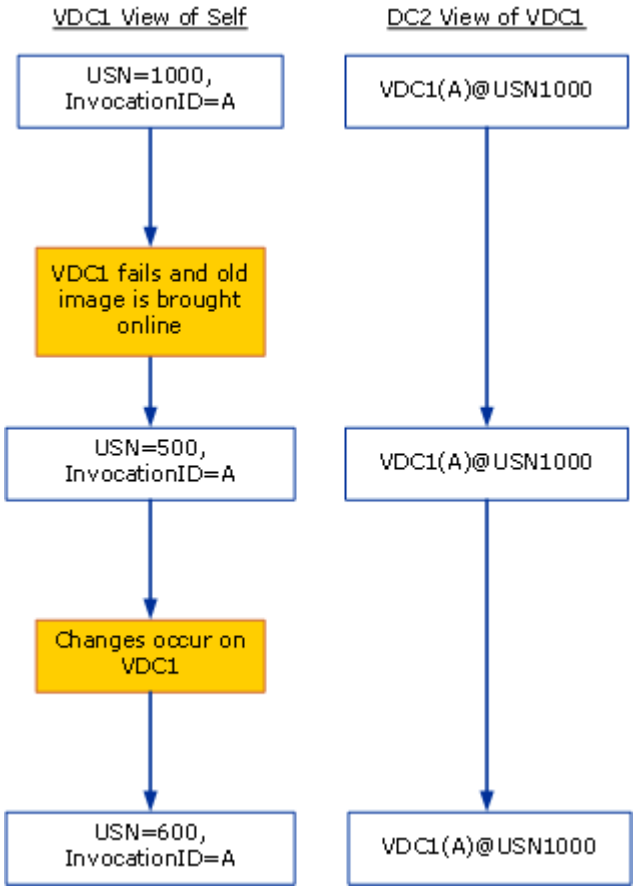
Note

Repadmin is a Windows Support Tool. You can install Windows Support Tools from the \Support\Tools folder on the Windows operating system CD or by clicking Tools in Help and Support Center in Windows Server 2003.

The following figure illustrates the importance of resetting the invocation ID for replicating partners following a restore procedure. In the figure, the actual USN and invocation ID values for a domain controller that is running in virtual machine VDC1 are identified as they occur on that domain controller. Meanwhile, replication partner DC2 keeps track of VDC1 in its up-to-dateness value. The perception of the replication state of VDC1 that is represented in the up-to-dateness value on DC2 is the critical information that leads to inappropriate replication states following an improper restore of VDC1. This perception is based on the fact that following an

improper restore of VDC1, the highest USN on VDC1 has reverted from 1000 to 500 but the invocation ID value has not changed. As a simple illustration, the invocation ID value in the figure is represented as a single letter "A."

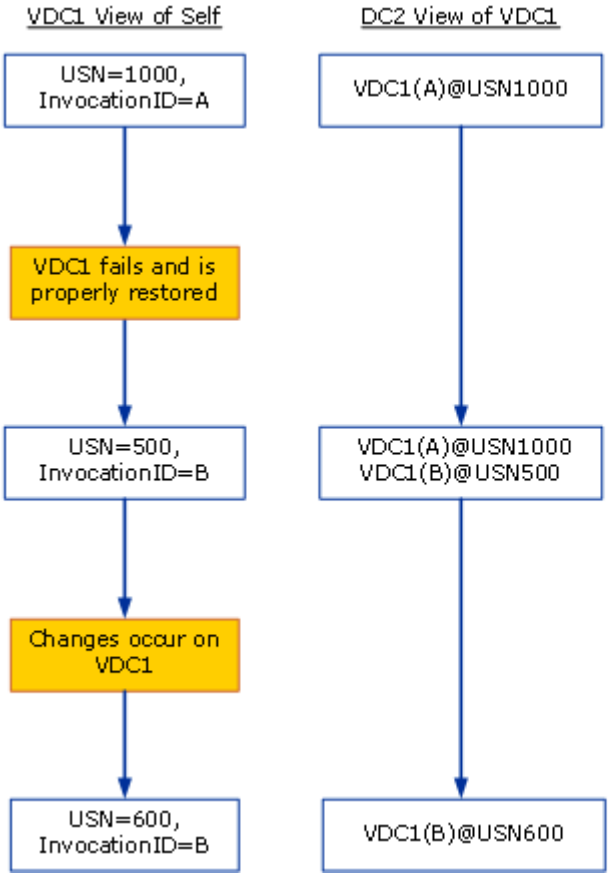
Perception of No New Updates on Improperly Restored Domain Controller Virtual Machine



After being improperly restored by starting an old image of VDC1, 100 new changes originate on VDC1. When DC2 attempts to replicate from VDC1, DC2 requests changes greater than USN 1000. Because the highest update on VDC1 is represented as USN 600, VDC1 sends no changes to DC2. The 100 new updates are never replicated from VDC1 to DC2. VDC1 will replicate changes to DC2 only when the highest USN on VDC1 exceeds 1000, resulting in 500 missing changes.

The following figure shows the difference in the perception of DC2 about VDC1 when the invocation ID value is reset. In this case, the change to the invocation ID on VDC1 replicates to DC2. DC2 thereby recognizes VDC1 as a restored domain controller and resets its up-to-dateness value for VDC2 to the value that reflects the current state of the restored directory database.

Perception of New Updates on a Properly Restored Domain Controller Virtual Machine



When changes occur on VDC1, its highest originating USN increases from 500 to 600. DC2 requests changes greater than USN 500 because its up-to-dateness value for VDC1 with invocation ID B now shows 500, not 1000. After replicating the new changes, DC2 adjusts its up-to-dateness value for VDC1 accordingly.

For more information about how domain controllers track updates, see "How the Active Directory Replication Model Works" on the Web at http://go.microsoft.com/fwlink/?LinkID=27636.

Restoration of System State

To be able to restore a domain controller in the event of failure, you must regularly back up system state, which includes Active Directory data and log files, the registry, the system volume (SYSVOL folder), and various elements of the operating system. This requirement is no different for a domain controller that is running in a virtual machine than for a domain controller that is running on native hardware. System state restore procedures performed by Active Directory-compatible backup applications are designed to ensure the consistency of local and replicated

Active Directory databases after a restore process, including the notification to replication partners of invocation ID resets. However, using virtual hosting environments and disk or operating system imaging applications makes it possible for administrators to bypass the checks and validations that ordinarily occur when domain controller system state is restored.

The only recommended way to roll the contents of a single domain controller back in time is by using an Active Directory-compatible backup and restore utility to restore a system state backup that originated from the same operating system installation as the one being restored.

Effects of Improper Restore Operations

Microsoft does not support any process that takes a copy or snapshot of all or individual elements of system state from a past date and time and effectively copies all or individual elements of that system state to the same or a different operating system image. Such an invalid restore results in a USN rollback that, without administrative intervention, can cause the direct and transitive replication partners of the improperly restored domain controller to have inconsistent objects in their Active Directory databases.

The following sequence of events illustrates how this inconsistency occurs and its effects on replication:

1. In the hub site, an administrator installs three domain controllers in the same domain:
   - DC1 is installed on native hardware.
   - VDC2 is installed in a virtual machine.
   - DC3 is installed on native hardware.
2. An administrator creates 100 user accounts on VDC2, corresponding to USNs 101 through 200 on VDC2, all of which replicate to DC1 and DC3.
3. An operating system image is created of VDC2 that contains knowledge of objects corresponding to local USN 1-200 on VDC1. This image is created by making a copy of the .vhd file. A system state backup is not performed.
4. On VDC2, 100 passwords for the existing users created in step 2, corresponding to USNs 201 through 300, are reset and replicate to DC1 and DC3.
5. DC3 is taken offline for a hardware update.
6. On VDC2, 50 new computer accounts, corresponding to USNs 301 through 350, are created and replicate to DC1 while DC3 is offline.
7. Prior to replicating changes corresponding to USN 301 through 350 to DC3, VDC2 experiences a catastrophic failure.
8. Against recommendations, the administrator attempts to restore VDC2 by starting the .vhd image copy that was created in step 3. VDC2 starts with knowledge of local USNs 1 through 200 that existed at the time the .vhd file was copied.
9. DC3 is brought back online.
10. When an administrator makes subsequent changes on VDC2, these changes begin at USN 201. Because the operating system image created at an earlier point in time was

essentially copied into place, as opposed to the recommended method of restoring system state, VDC2 maintains its original invocation ID. As a result, DC1 and DC3 maintain their up-to-dateness values for VDC2 of USN 350 and USN 300, respectively. Without administrative intervention, DC1 and DC3 request changes from VDC2 according to their current up-to-dateness values, resulting in the following inconsistencies:

- DC1 does not receive changes for USNs 201 through 350 because DC1 continues to request changes for USNs that are greater than 350.
- DC3 does not receive changes for USNs 201 through 300, but does receive changes for USNs 301 through 350 because DC3 requests changes for USNs that are greater than 300.

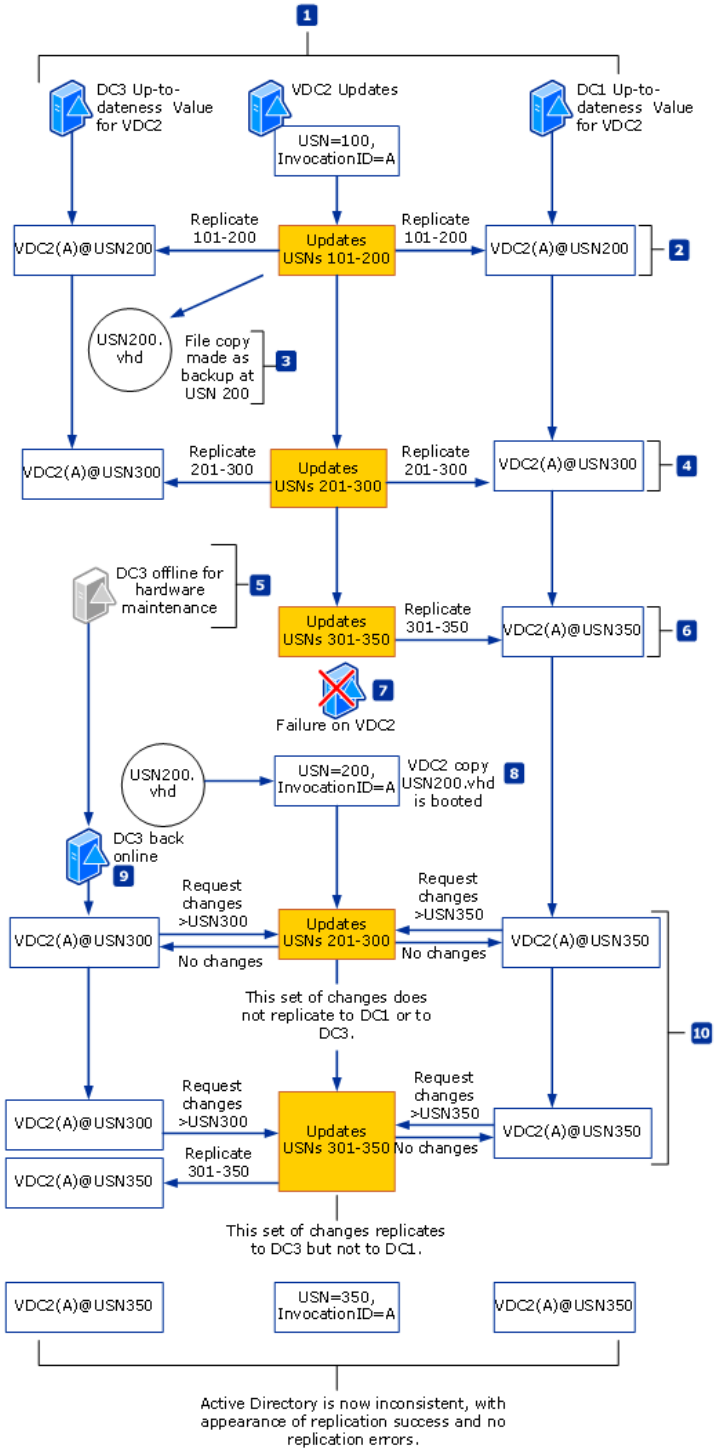
Without administrative intervention, DC1 and DC3 continue replicating updates from VDC2 that correspond to changes greater than USN 350.

Administrators monitoring replication health in the forest note the following:

- **Repadmin /showrepl** (**/showreps** on domain controllers that are running Windows 2000 Server) reports that two-way Active Directory replication between VDC2 andDC1, and between VDC2 and DC3, is occurring without error.
- Replication events in the Directory Service event logs of domain controllers running versions of Windows 2000 Server with no updates, Windows 2000 Server with Service Pack 1 (SP1) to SP4, and Windows Server 2003 with no updates do not indicate any replication failures.
- Views in the Active Directory Users and Computers MMC snap-in and Windows Support Tools ADSI Edit and LDP show a different number of objects and different object metadata when the domain directory partition on VDC2 is compared to those on DC1 and DC3. The difference is the set of changes that map to originating changes that occurred on VDC2 following the improper restore." On DC1 these changes correspond to VDC2 USNs 201-350. On DC3 these changes correspond to VDC2 USNs 201-300.
- User and computer authentication requests fail intermittently for some user and computer accounts. Some users experience an access denied error, suggesting a password mismatch between the domain controllers. The users who are experiencing problems correspond to the user and computer accounts that were created in steps 2 and 7 and password resets in step 5 that never replicated to other domain controllers in the domain.

The following figure maps the steps in the foregoing sequence that results in Active Directory inconsistencies when an earlier copy of a .vhd file is started in the production environment in an attempt to restore a failed domain controller that is running in a virtual machine.

Improper Backup and Restore Causes Inconsistencies in Active Directory



Although the results depicted in this example illustrate the impact on user and computer accounts, note that a USN rollback can prevent any object type in any Active Directory partition from replicating, including:

- Active Directory replication topology and schedule
- The existence of domain controllers in the forest and their roles
- The existence of domain and application directory partitions in the forest
- The existence of security groups and their current group membership
- DNS record registration in Active Directory-integrated DNS zones

Similarly, the size of the USN gap or "hole" (defined by the delta of the highest USN value that existed when the restored system state backup was made and the number of originating changes that were created on the rolled-back domain controller before it was taken offline) could represent hundreds, thousands, or even tens of thousands of changes to users and computers and their passwords, trust relationships and their passwords, and security groups.

Detection of USN Rollbacks With 875495 or 885875 Updates Installed

In most cases, the updates that are included with Knowledge Base article 875495, "How to detect and recover from a USN rollback in Windows Server 2003" and article 885875, "How to detect and recover from a USN rollback in Windows 2000 Server," detect inconsistency due to improper restore procedures that result in USN rollback on a domain controller virtual machine without a corresponding reset of the invocation ID. The updates provide protections against inappropriate replication following an improper domain controller restore operation. These protections are triggered by the fact that an improper restore operation results in lower USNs that represent originating changes that the replication partners have already received.

Caution

Even with the updates included with Knowledge Base article 875495 or 885875 applied, USN rollback detection will not occur under the following conditions:

- The .vhd file is running in multiple locations simultaneously.
- The USN range between the restored domain controller and the old domain controller are close enough that the protection behavior is not triggered.

With the updates installed, when a domain controller requests changes using a previously used USN, the response by its initial replication partner is interpreted by the requesting domain controller to mean that its replication metadata is outdated, indicating that it has been rolled back to a previous version of the virtual machine .vhd file. In this case, the rolled-back domain controller initiates the following quarantine measures:

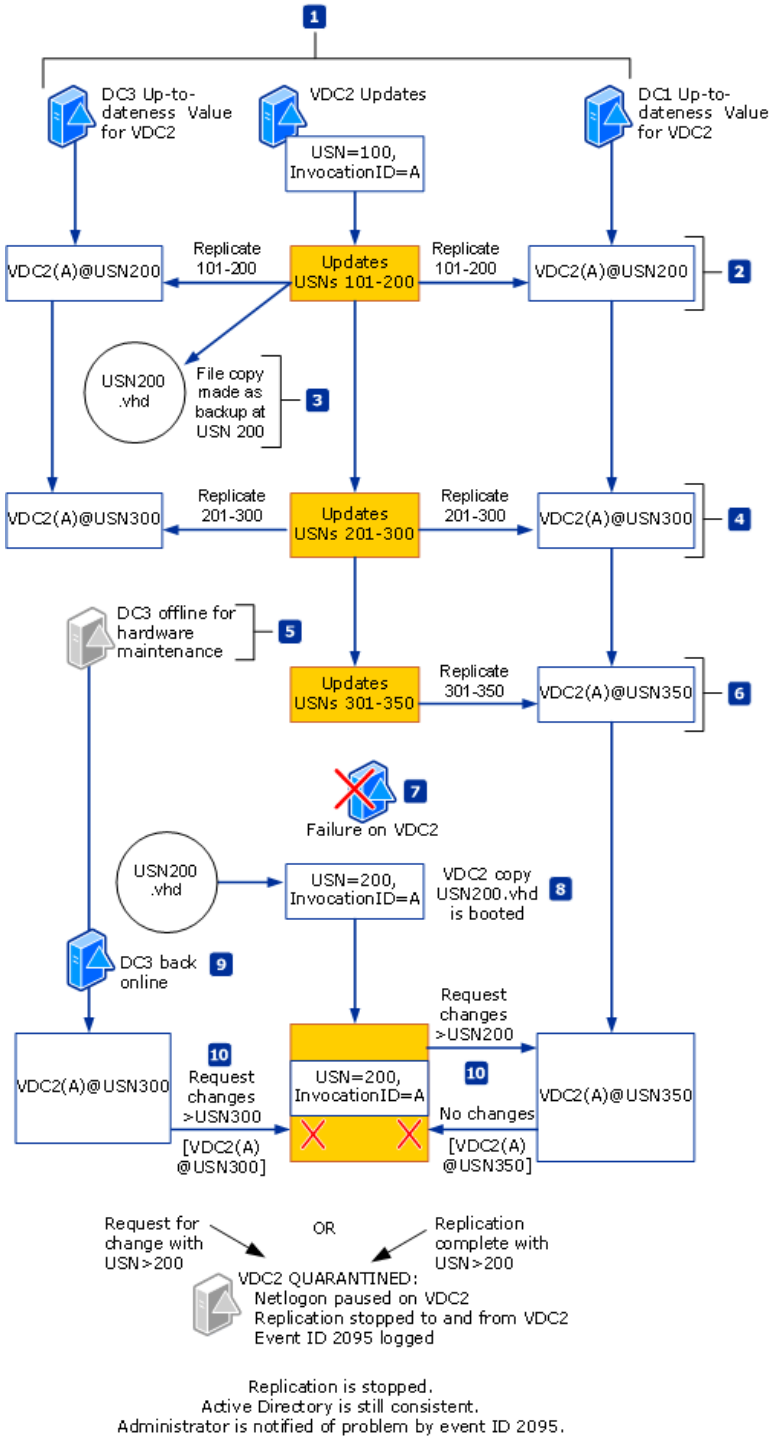
- Pauses the Net Logon service, which prevents user and computer accounts from changing account passwords. This action prevents losing such changes should they occur following an improper restore.
- Disables inbound and outbound Active Directory replication.
- Generates event ID 2095 in the Directory Service event log to indicate the condition.

The following figure shows the sequence of events that occurs when USN rollback is detected on VDC2, the domain controller running in a virtual machine whose updates are illustrated in "Effects of Improper Restore Operations" earlier in this document. In the following figure, the detection of USN rollback occurs on VDC2 when it first receives an up-to-dateness USN value from a replication partner that is higher than its own local USN value. Up-to-dateness values are received in the following ways:

- During a request for replication: The destination replication partner sends its up-to-dateness value for the source in the request.
- During a completion of replication: The source sends its up-to-dateness value for the destination at the completion of a successful replication cycle.

Step 10 in the sequence is shown as it can occur in both a request for changes or in a replication completion message. Whichever event occurs first on the rolled back domain controller prompts the USN rollback detection behavior.

USN Rollback Detection Causing Domain Controller Quarantine



When the updates included with Knowledge Base article 875495 (Windows Server 2003) or 885875 (Windows 2000 Server with SP4) are installed, if a replication partner has a significantly higher USN for the domain controller that is running in a virtual machine, the latter interprets this condition as meaning that it has been rolled back to a previous version of its .vhd file without its invocation ID being reset. This domain controller logs event ID 2095, which alerts the administrator that action is required to change the invocation ID of the domain controller that logged the event.

Event ID 2095 displays the following message:

```
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.


To determine if this misconfiguration exists, query this event ID using
http://support.microsoft.com or contact your Microsoft product support.


The most probable cause of this situation is the improper restore of Active
Directory on the local domain controller.


User Actions:

If this situation occurred because of an improper or unintended restore, forcibly
demote the DC.
```

Immediate Steps to Take on Encountering Event ID 2095

If the Directory Service event log reports event ID 2095, take the following steps immediately:

1. Shut down the domain controller virtual machine that recorded the error and ensure that no one restarts it online.
2. Contact Microsoft Product Support Services, who will assist in determining whether any changes originated on this domain controller between the time event ID 2095 error was logged and the time the domain controller was shut down.
3. Forcefully demote the domain controller as instructed by Product Support Services.
4. Destroy all old .vhd files for this domain controller.

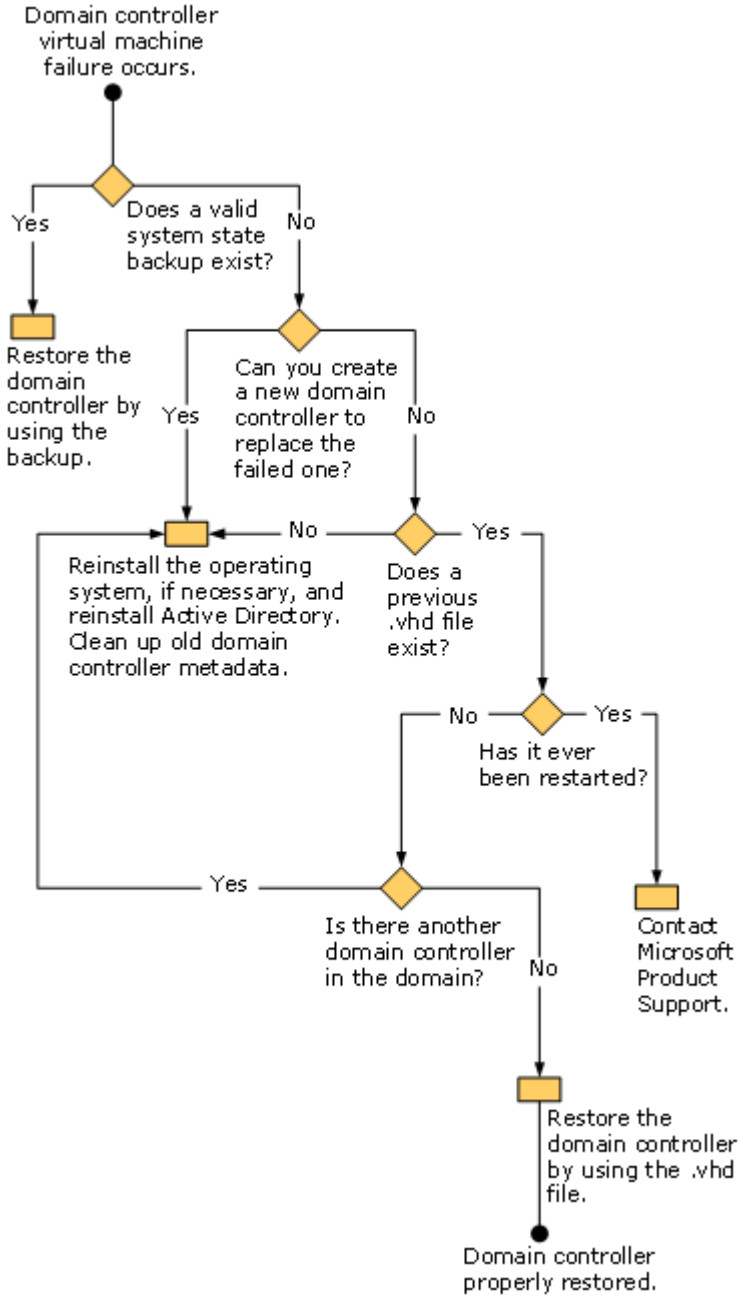
Options for Restoring a Domain Controller Running in a Virtual Machine

When a domain controller virtual machine fails and you have not received event ID 2095, there are supported options for recovery when one of the following conditions exists:

- **A valid system state backup exists:** Restore system state by using the restore option of the backup utility you used to create the backup. In this discussion, a valid system state backup is one that is created by using an Active Directory-compatible backup utility and is created within the span of a tombstone lifetime (by default, no more than 60 days).
- **A clean .vhd image is available, but no system state backup is available:** Disconnect the domain controller from the network and restore the virtual machine by using the registry, as described in "Restoration of a .vhd Image When No Valid System State Backup Exists" later in this document.

Use the process shown in the following figure to determine the proper course of action.

Recommendations for Restoring a Failed Domain Controller Virtual Machine



Restoration of System State Backup of a Domain Controller Virtual Machine

If a valid system state backup exists for the domain controller virtual machine, you can safely restore the backup by following the restore procedure prescribed by the backup utility that you used to back up the .vhd file.

For information about how to restore a domain controller by using a system state backup, see "Microsoft Solutions for Management: Managing the Windows Server Platform Active Directory Directory Service Product Operations Guide" on the Web at http://go.microsoft.com/fwlink/?LinkId=34771.

Restoration of a .vhd Image When No Valid System State Backup Exists

When no properly backed-up .vhd file exists, you can use a previous .vhd file to safely restore a domain controller that is running in a virtual machine. Follow this procedure only when the previous .vhd file has never been booted.

Restoring a previous .vhd image can be achieved by editing a registry entry that effectively creates a system state backup and immediately restores it. Use this procedure only under the following conditions:

- Updates included with Knowledge Base article 875495 (Windows Server 2003) or article 885875 (Windows 2000 Server with SP4) were installed on the domain controller prior to the failure.
- The previous .vhd file has not been booted.
- The domain controller is offline.

Important

When restoring a domain controller that is running in a virtual machine by using an earlier .vhd file that has not been properly backed up, do not restart the domain controller in normal operation mode. Simply starting a domain controller in normal operation mode, even if it is disconnected from the network, causes changes in the directory service that will increment USNs on the domain controller. You must start the domain controller in Directory Services Restore mode only and then use the recovery steps in the following procedure.

To restore a previous .vhd image when USN rollback has not occurred

1. Using the previous .vhd, start the domain controller in Directory Services Restore mode.
2. In a registry editor, if the entry **DSA Previous Restore Count** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters** is visible, make a note of the value. If the entry is not visible, assume a value of 0. Do not add the entry.

3. Add the registry entry **Database restored from backup** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**

   Data type: REG_DWORD

   Value=1

   This setting creates a valid system state backup and immediately restores the backup.

   > **Note**
   > The Database restored from backup entry is available on domain controllers that are running Windows 2000 Server with SP4 and domain controllers that are running Windows Server 2003 with updates included with Knowledge Base article 875495 installed.

4. Restart the domain controller normally.
5. In the registry, check to be sure that the value in **DSA Previous Restore Count** is equal to its previous value plus 1.
6. In the Directory Service event log, check to see that event ID 1109 appears. This event confirms that the .vhd file has been restored and the invocation ID has been changed. Event ID 1109 places the following information in the log:

```
Active Directory has been restored from backup media, or has been configured
to host an application partition. The invocationID attribute for this
directory server has been changed. The highest update sequence number at the
time the backup was created is a%n

%nInvocationID attribute (old value):%n%1

%nInvocationID attribute (new value):%n%2

%nUpdate sequence number:%n%3

%n

%nThe invocationID is changed when a directory server is restored from
backup media or is configured to host a writeable application directory
partition.
```

Summary

The most useful and safe application of Virtual Server 2005 with Windows Server 2003 is to host domain controllers in virtual machines as a test platform. In addition, with strict adherence to security and operations recommendations regarding access to and restoration of .vhd files, deployment in the production environment can also be successful and beneficial.

In production, domain controllers running in virtual machines can be useful when hardware is not available for the number of domain controllers needed. When using domain controller virtual machines, it is best to avoid using them in high-availability roles in the forest, such as global catalog servers, operations masters, and bridgehead servers.

To be certain that the consistency and reliability of directory data is maintained when running domain controllers in virtual machines, you must:

- Ensure that all domain controllers that are running in virtual machines comply with the software requirements provided in this document, including having the updates provided with Knowledge Base article 875495 (Windows Server 2003) or article 885875 (Windows 2000 Server with SP4) installed.
- Protect all .vhd files that represent domain controllers with the same level of security as a domain controller that is running on native hardware.
- Ensure that domain controllers running in virtual machines are backed up by using an Active Directory-compatible backup and restore application such as Ntbackup.
- Ensure that copies of .vhd files that represent production domain controllers are never started on the network.

Additional Information

- For an overview of Virtual Server technology, see "Microsoft Virtual Server 2005 Technical Overview" on the Web at http://go.microsoft.com/fwlink/?linkID=34709.
- For deployment, operations, and technical reference information about Virtual Server, see "Virtual Server 2005 Administrator's Guide" on the Web at http://go.microsoft.com/fwlink/?linkID=27540.
- For information about deploying Active Directory, see "Designing and Deploying Directory and Security Services" of the Windows Server 2003 Deployment Kit on the Web at http://go.microsoft.com/fwlink/?LinkId=34775.
- For technical information about Active Directory, including Active Directory replication, see "Windows Server 2003 Active Directory Technical Reference" at http://go.microsoft.com/fwlink/?LinkID=18540.
- For information about securing Windows Server 2003 domain controllers, see "Best Practice Guide for Securing Active Directory Installations" on the Web at http://go.microsoft.com/fwlink/?LinkID=28521.
- For information about securing Windows 2000 Server domain controllers, see "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations, Part I" on the Web at http://go.microsoft.com/fwlink/?LinkID=21258.