Article ID: 875495 - Last Review: February 10, 2011 - Revision: 19.0

How to detect and recover from a USN rollback in Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2

Hotfix Download Available
View and request hotfix downloads

For a Microsoft Windows 2000 Server version of this article, see 885875 (http://support.microsoft.com/kb/885875/) .

SUMMARY

This article describes a condition that occurs when a domain controller that is running Windows 2000, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 starts from an Active Directory database that has been incorrectly restored or copied into place. This condition is known as an update sequence number rollback, or USN rollback.

When a USN rollback occurs, modifications to objects and attributes that occur on one domain controller do not replicate to other domain controllers in the forest. Because replication partners believe that they have an up-to-date copy of the Active Directory database, monitoring and troubleshooting tools such as Repadmin.exe do not report any replication errors.

After hotfix 875495 or Windows Server 2003 Service Pack 1 is installed, a Microsoft Windows Server 2003 domain controller logs Directory Services event 2095 when it encounters a USN rollback. The text of the event message directs administrators to this article to learn about recovery options.

Because it is difficult to detect and recover from a USN rollback, we recommend that administrators install hotfix 875495 or the latest service pack that is available) on Windows Server 2003 RTM. The hotfix is included in Windows Server 2003 SP1 as well as in Windows Server 2008 and Windows Server 2008 R2. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

> *888794 (http://support.microsoft.com/kb/888794/) Considerations when hosting Active Directory domain controller in virtual hosting environments*

INTRODUCTION

This article discusses the following topics:

- Supported methods to back up Active Directory on domain controllers that are running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2
- Typical behavior that occurs when you restore an Active Directory-aware system state backup
- How copying a previous Active Directory database into the folder that contains the current Active Directory database without restoring the system state can lead to a USN rollback
- How Active Directory replication is affected when a Microsoft Windows Server 2003-based domain controller experiences a USN rollback
- Ways to recover an Active Directory domain controller after it experiences a USN rollback
- Enhancements in hotfix 875495 (and in Windows Server 2003 Service Pack 1, Windows Server 2008, and Windows Server 2008 R2) to detect USN rollbacks and to quarantine affected domain controllers

Over a domain controller's life cycle, you may have to restore, or "roll back," the contents of the Active Directory database to a known good point in time. Or, you may have to roll back elements of a domain controller's host operating system, including Active Directory, to a known good point.

The following are supported methods that you can use to roll back the contents of Active Directory:

- Use an Active Directory-aware backup and restoration utility that uses Microsoft-provided and Microsoft-tested APIs. These APIs non-authoritatively or authoritatively restore a system state backup. The backup that is restored should originate from the same operating system installation and from the same physical or virtual computer that is being restored.
- Use an Active Directory-aware backup and restoration utility that uses Microsoft Volume Shadow Copy Service APIs. These APIs back up and restore the domain controller system state. The Volume Shadow Copy Service supports creating single point-in-time shadow copies of single or multiple volumes on computers that are running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. Single point-in-time shadow copies are also known as snapshots. For more information, visit the following Microsoft Web site and search for "Volume Shadow Copy Service":
  http://support.microsoft.com/ (http://support.microsoft.com/)
- Restore the system state. Evaluate whether valid system state backups exist for this domain controller. If a valid system state backup was made before the rolled-back domain controller was incorrectly restored and if the backup contains recent changes that were made on the domain controller, restore the system state from the most recent backup.

MORE INFORMATION

Typical behavior that occurs when you restore an Active Directory-aware system state backup

Windows Server 2003 domain controllers use USNs together with the invocation IDs to track updates that must be replicated between replication partners in an Active Directory forest.

Source domain controllers use USNs to determine what changes have already been received by the destination domain controller that is requesting changes. Destination domain controllers use USNs to determine what changes should be requested from source domain controllers.

The invocation ID identifies the version or the instantiation of the Active Directory database that is running on a given domain controller.

When Active Directory is restored on a domain controller by using the APIs and methods that Microsoft has designed and tested, the invocation ID is correctly reset on the restored domain controller. Domain controllers in the forest receive notification of the invocation reset. Therefore, they adjust their high watermark values accordingly.

Software and methodologies that cause USN rollbacks

When the following environments, programs, or subsystems are used, administrators can bypass the checks and validations that Microsoft has designed to occur when the domain controller system state is restored:

- Starting an Active Directory domain controller whose Active Directory database file was restored (copied) into place by using an imaging program such as Norton Ghost.
- Starting a previously saved virtual hard disk image of a domain controller. The following scenario can cause a USN rollback:
    1. Promote a domain controller in a virtual hosting environment.
    2. Create a snapshot or alternative version of the virtual hosting environment.
    3. Let the domain controller continue to inbound replicate and to outbound replicate.
    4. Start the domain controller image file that you created in step 2.
- Examples of virtualized hosting environments that cause this scenario include Microsoft Virtual PC 2004, Microsoft Virtual Server 2005, and EMC VMWARE. Other virtualized hosting environments can also cause this scenario.
- For more information about the support conditions for domain controllers in virtual hosting environments, click the following article number to view the article in the Microsoft Knowledge Base:

    888794 (http://support.microsoft.com/kb/888794/) Considerations when hosting Active Directory domain controller in virtual hosting environments

- Starting an Active Directory domain controller that is located on a volume where the disk subsystem loads by using previously saved images of the operating system without requiring a system state restoration of Active Directory.

    Scenario A: Starting multiple copies of Active Directory that are located on a disk subsystem that stores multiple versions of a volume

    1. Promote a domain controller. Locate the Ntds.dit file on a disk subsystem that can store multiple versions of the volume that hosts the Ntds.dit file.
    2. Use the disk subsystem to create a snapshot of the volume that hosts the Ntds.dit file for the domain controller.

3. Continue to let the domain controller load Active Directory from the volume that you created in step 1.
4. Start the domain controller that the Active Directory database saved in step 2.

Scenario B: Starting Active Directory from other drives in a broken mirror

1. Promote a domain controller. Locate the Ntds.dit file on a mirrored drive.
2. Break the mirror.
3. Continue to inbound replicate and outbound replicate by using the Ntds.dit file on the first drive in the mirror.
4. Start the domain controller by using the Ntds.dit file on the second drive in the mirror.

Even if not intended, each of these scenarios can cause domain controllers to roll back to an older version of the Active Directory database by unsupported methods. The only supported way to roll back the contents of Active Directory or the local state of an Active Directory domain controller is to use an Active Directory-aware backup and restoration utility to restore a system state backup that originated from the same operating system installation and the same physical or virtual computer that is being restored.

Microsoft does not support any other process that takes a snapshot of the elements of an Active Directory domain controller's system state and copies elements of that system state to an operating system image. Unless an administrator intervenes, such processes cause a USN rollback. This USN rollback causes the direct and transitive replication partners of an incorrectly restored domain controller to have inconsistent objects in their Active Directory databases.

The effects of a USN rollback

When USN rollbacks occur, modifications to objects and attributes are not inbound replicated by destination domain controllers that have previously seen the USN.

Because these destination domain controllers believe they are up to date, no replication errors are reported in Directory Service event logs or by monitoring and diagnostic tools.

USN rollback may affect the replication of any object or attribute in any partition. The most frequently observed side effect is that user accounts and computer accounts that are created on the rollback domain controller do not exist on one or more replication partners. Or, the password updates that originated on the rollback domain controller do not exist on replication partners.

The following steps show the sequence of events that may cause a USN rollback. A USN rollback occurs when the domain controller system state is rolled back in time using an unsupported system state restoration.

1. An administrator promotes three domain controllers in a domain. (In this example, the domain controllers are DC1, DC2, and DC2, and the domain is Contoso.com.) DC1 and DC2 are direct replication partners. DC2 and DC3 are also direct replication partners. DC1 and DC3 are not direct replication partners but receive originating updates transitively through DC2.
2. An administrator creates 10 user accounts that correspond to USNs 1

through 10 on DC1. All these accounts replicate to DC2 and DC3.

3. A disk image of an operating system is captured on DC1. This image has a record of objects that correspond to local USNs 1 through 10 on DC1.
4. The following changes are made in Active Directory:
    - The passwords for all 10 user accounts that were created in step 2 are reset on DC1. These passwords correspond to USNs 11 through 20. All 10 updated passwords replicate to DC2 and DC3.
    - 10 new user accounts that correspond to USNs 21 through 30 are created on DC1. These 10 user accounts replicate to DC2 and DC3.
    - 10 new computer accounts that correspond to USNs 31 through 40 are created on DC1. These 10 computer accounts replicate to DC2 and DC3.
    - 10 new security groups that correspond to USNs 41 through 50 are created on DC1. These 10 security groups replicate to DC2 and DC3.
5. DC1 experiences a hardware failure or a software failure. The administrator uses a disk imaging utility to copy the operating system image that was created in step 3 into place. DC1 now starts with an Active Directory database that has knowledge of USNs 1 through 10.

   Because the operating system image was copied into place, and a supported method of restoring the system state was not used, DC1 continues to use the same invocation ID that created the initial copy of the database and all changes up to USN 50. DC2 and DC3 also maintain the same invocation ID for DC1 well as an *up-to-date vector* of USN 50 for DC1. (An up-to-date vector is the current status of the latest originating updates to occur on all domain controllers for a given directory partition.)

   Unless an administrator intervenes, DC2 and DC3 do not inbound replicate the changes that correspond to local USN 11 through 50 that originate from DC1. Also, according to the invocation ID that DC2 uses, DC1 already has knowledge of the changes that correspond to USN 11 to 50. Therefore, DC2 does not send those changes. Because the changes in step 4 do not exist on DC1, logon requests fail with an "access denied" error. This error occurs either because passwords do not match or because the account does not exist when the newer accounts randomly authenticate with DC1.
6. Administrators who monitor replication health in the forest note the following situations:
    - The **Repadmin /showreps** command-line tool reports that two-way Active Directory replication between DC1 and DC2 and between DC2 and DC3 is occurring without error. This situation makes any replication inconsistency difficult to detect.
    - Replication events in the directory service event logs of domain controllers that are running Windows Server do not indicate any replication failures in the directory service event logs. This situation makes any replication inconsistency difficult to detect.
    - Active Directory Users and Computers or the Active Directory Administration Tool (Ldp.exe) show a different count of objects and different object metadata when the domain directory partitions on DC2 and DC3 are compared to the partition on DC1. The difference is the set of changes that map to USN changes 11 through 50 in step 4.

      Note In this example, the different object count applies to user accounts, computer accounts, and security groups. The different object metadata represents the different user account passwords.

    - User authentication requests for the 10 user accounts that were created in step 2 occasionally generate an "access denied" or "incorrect password" error. This error may occur because a password mismatch exists between these user accounts on DC1 and the accounts on DC2 and DC3. The user accounts that experience this problem correspond to the user accounts that were created in step 4. The user accounts and password resets in step 4 did not replicate to other domain controllers in the domain.
7. DC2 and DC3 start to inbound-replicate originating updates that correspond to USN numbers that are greater than 50 from DC1. This replication proceeds normally without administrative intervention because the previously recorded up-to-dateness vector threshold, USN 50, has been exceeded. (USN 50 was the up-to-dateness vector USN recorded for DC1 on DC2 and DC3 before DC1 was taken offline and restored.) However, the new changes that corresponded to USNs 11 through 50 on the originating DC1 after the unsupported restore will never replicate to DC2, DC3, or their transitive replication partners.

Although the symptoms that are mentioned in step 6 represent some of the effect that a USN rollback can have on user and computer accounts, a USN rollback can prevent any object type in any Active Directory partition from replicating. These object types include the following:

- The Active Directory replication topology and schedule
- The existence of domain controllers in the forest and the roles that these domain controllers hold

  Note These roles include the global catalog, relative identifier (RID) allocations, and operations master roles. (Operations master roles are also known as flexible single master operations or FSMO.)
- The existence of domain and application partitions in the forest
- The existence of security groups and their current group memberships
- DNS record registration in Active Directory-integrated DNS zones

The size of the USN hole may represent hundreds, thousands, or even tens of thousands of changes to users, computers, trusts, passwords, and security groups. (The USN hole is defined by the difference between the highest USN number 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.)

Detecting a USN rollback on a domain controller that is running Windows Server

Because errors are not logged in the event log or in the replication engine, a USN rollback can be difficult to detect.

One way to detect a USN rollback is to use the Windows Server version of Repadmin.exe to run the **repadmin /showutdvec** command. This version of Repadmin.exe displays the up-to-dateness vector USN for all domain controllers that replicate a common naming context. To detect a USN rollback, compare the output of the **repadmin /showutdvec** command on the domain controller with the output of the same command on the domain controller's replication partners. If the direct replication partners have a higher USN number for the domain controller than

the domain controller has for itself, and the **repadmin /showreps** command does not report replication errors between direct replication partners, you have compelling evidence of a USN rollback.

Note A correctly restored domain controller resets its local invocation ID attribute when it restarts into Active Directory after its system state is restored by using a supported backup and restore method. When the reset invocation ID is outbound-replicated, remote domain controllers in the forest record the reset invocation ID as a new database instance on the restored domain controller. Although the restored domain controller is still the same domain controller, the remote domain controllers acknowledge this restored domain controller as a new replication partner because the invocation ID changed. (The invocation ID is the identity of the database instance.) The restored domain controller itself will accept changes from other remote domain controllers that originated on the remote domain controllers and on the domain controller before it was restored.

The following example shows the output of the **repadmin /showutdvec** command on DC1 and DC2 in the contoso.com domain. In this example, the command is run immediately following the rollback in step 5.

```
C:\>Repadmin /showutdvec dc1 dc=contoso,dc=com
Caching GUIDs...
Site1\DC1 @ USN 10 @ Time 2004-08-04 15:07:15
Site2\DC2 @ USN 24805 @ Time 2004-08-04 15:06:59
C:\>Repadmin /showutdvec dc2 dc=contoso,dc=com
Caching GUIDs...
Site1\DC1 @ USN 50 @ Time 2004-08-04 15:07:15
Site2\DC2 @ USN 24805 @ Time 2004-08-04 15:06:59
```

The output from DC1 shows a local USN of 10. DC2 has inbound-replicated USN 50 and will ignore the Active Directory updates that correspond to the next 40 USN numbers from the originating DC1.

Detecting a USN rollback on a Windows Server domain controller that has the 875495 hotfix (or an operating system that includes this hotfix) installed

Because a USN rollback is difficult to detect, a Windows Server domain controller that has the 875495 hotfix functionality installed logs event 2095 when a source domain controller sends a previously acknowledged USN number to a destination domain controller without a corresponding change in the invocation ID.

To prevent unique originating updates to Active Directory from being created on the incorrectly restored domain controller, the Net Logon service is paused. When the Net Logon service is paused, user and computer accounts cannot change the password on a domain controller that will not outbound-replicate such changes. Similarly, Active Directory administration tools will favor a healthy domain controller when they make updates to objects in Active Directory.

On a domain controller that has the 875495 hotfix functionality installed, event messages that resemble the following are recorded if the following conditions are true:

- A source domain controller sends a previously acknowledged USN number to a destination domain controller.
- There is no corresponding change in the invocation ID.

Message 1

Event Type: Error
Event Source: NTDS Replication
Event Category: Replication
Event ID: 2095
Date: 3/10/2005
Time: 4:26:51 PM
User: USN\2B25VB$
Computer: 2B9A
Description: During an Active Directory replication request, the local domain controller (DC) identified a remote DC which has received replication data from the local DC using already-acknowledged USN tracking numbers. Because the remote DC believes it is has a more up-to-date Active Directory database than the local DC, the remote DC will not apply future changes to its copy of the Active Directory database or replicate them to its direct and transitive replication partners that originate from this local DC. If not resolved immediately, this scenario will result in inconsistencies in the Active Directory databases of this source DC and one or more direct and transitive replication partners. Specifically the consistency of users, computers and trust relationships, their passwords, security groups, security group memberships and other Active Directory configuration data may vary, affecting the ability to log on, find objects of interest and perform other critical operations. 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. Remote DC: b55ee67f-ed73-4970-b2d4-7dc6f571439f Partition: CN=Configuration,DC=usn,DC=loc USN reported by Remote DC: 24707 USN reported by Local DC: 20485 For more information, see Help and Support Center at http://support.microsoft.com.

Message 2

Event Type: Warning
Event Source: NTDS General
Event Category: Replication
Event ID: 1113
Date: 3/10/2005
Time: 4:26:51 PM
User: USN\2B25VB$
Computer: 2B9A
Description: Inbound replication has been disabled by the user. For more information, see Help and Support Center at http://support.microsoft.com.

Message 3

Event Type: Warning
Event Source: NTDS General
Event Category: Replication
Event ID: 1115
Date: 3/10/2005
Time: 4:26:51 PM
User: USN\2B25VB$

Computer: 2B9A
Description: Outbound replication has been disabled by the user. For more information, see Help and Support Center at http://support.microsoft.com

Message 4

Event Type: Error
Event Source: NTDS General
Event Category: Service Control
Event ID: 2103
Date: 3/10/2005
Time: 4:26:51 PM
User: USN\2B25VB$
Computer: 2B9A
Description: The Active Directory database has been restored using an unsupported restoration procedure. Active Directory will be unable to log on users while this condition persists. As a result, the Net Logon service has paused. User Action See previous event logs for details. For more information, see Help and Support Center at http://support.microsoft.com.

These events may be captured in the Directory Service event log. However, they may be overwritten before they are observed by an administrator.

Recovering from a USN rollback

There are two approaches to recover from a USN rollback:

Remove the Domain Controller from the domain, following these steps:

1. Remove Active Directory from the domain controller to force it to be a stand-alone server. For more information, click the following article number to view the article in the Microsoft Knowledge Base:
   332199 (http://support.microsoft.com/kb/332199/) Domain controllers do not demote gracefully when you use the Active Directory Installation Wizard to force demotion in Windows Server 2003 and in Windows 2000 Server
2. Shut down the demoted server.
3. On a healthy domain controller, clean up the metadata of the demoted domain controller. For more information, click the following article number to view the article in the Microsoft Knowledge Base:
   216498 (http://support.microsoft.com/kb/216498/) How to remove data in Active Directory after an unsuccessful domain controller demotion
4. If the incorrectly restored domain controller hosts operations master roles, transfer these roles to a healthy domain controller. For more information, click the following article number to view the article in the Microsoft Knowledge Base:
   255504 (http://support.microsoft.com/kb/255504/) Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller
5. Restart the demoted server.
6. If you are required to, install Active Directory on the stand-alone server again.
7. If the domain controller was previously a global catalog, configure the

domain controller to be a global catalog. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

313994 (http://support.microsoft.com/kb/313994/) How to create or move a global catalog in Windows 2000

8. If the domain controller previously hosted operations master roles, transfer the operations master roles back to the domain controller. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

   255504 (http://support.microsoft.com/kb/255504/) Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller

Restore the system state of a good backup.

Evaluate whether valid system state backups exist for this domain controller. If a valid system state backup was made before the rolled-back domain controller was incorrectly restored, and the backup contains recent changes that were made on the domain controller, restore the system state from the most recent backup.

You can also use the snapshot as a source of a backup. Or you can set the database to give itself a new invocation ID using the procedure in the section "To restore a previous version of a virtual domain controller VHD without system state data backup" in this article: http://technet.microsoft.com/en-us/library/dd363545(WS.10).aspx (http://technet.microsoft.com/en-us/library/dd363545(WS.10).aspx)

Hotfix information

A supported hotfix is available from Microsoft. However, this hotfix is intended to correct only the problem that is described in this article. Apply this hotfix only to systems that are experiencing this specific problem. This hotfix might receive additional testing. Therefore, if you are not severely affected by this problem, we recommend that you wait for the next software update that contains this hotfix.

If the hotfix is available for download, there is a "Hotfix download available" section at the top of this Knowledge Base article. If this section does not appear, contact Microsoft Customer Service and Support to obtain the hotfix.

Note If additional issues occur or if any troubleshooting is required, you might have to create a separate service request. The usual support costs will apply to additional support questions and issues that do not qualify for this specific hotfix. For a complete list of Microsoft Customer Service and Support telephone numbers or to create a separate service request, visit the following Microsoft Web site:

http://support.microsoft.com/contactus/?ws=support
(http://support.microsoft.com/contactus/?ws=support)

Note The "Hotfix download available" form displays the languages for which the hotfix is available. If you do not see your language, it is because a hotfix is not available for that language.

File information

The English version of this hotfix has the file attributes (or later file attributes) that are listed in the following table. The dates and times for these files are listed in Coordinated Universal Time (UTC). When you view the file information, it is converted to local time. To find the difference between UTC and local time, use the **Time Zone** tab in the **Date and Time** item in Control Panel.Restore the system

state.

Evaluate whether valid system state backups exist for this domain controller. If a valid system state backup was made before the rolled-back domain controller was incorrectly restored, and the backup contains recent changes that were made on the domain controller, restore the system state from the most recent backup.

APPLIES TO

- Microsoft Windows Server 2003 Service Pack 2
- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise

Keywords: kbautohotfix kbqfe kbhotfixserver KB875495