Knowledge Base

How To Perform an Authoritative Restore to a Domain Controller in Windows 2000

PSS ID Number: 241594

Article Last Modified on 7/15/2004

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server

This article was previously published under Q241594

IN THIS TASK

- SUMMARY
  - Perform an Authoritative Restore
  - Restore a Subtree
- REFERENCES

SUMMARY

This article discusses how to perform an authoritative restore of the Active Directory directory service to a Windows 2000-based domain controller.

During a typical file restore operation, Microsoft Windows Backup operates in non-authoritative restore mode. In this mode, Windows Backup restores all files, including Active Directory objects, with their original Update Sequence Number (USN) or numbers. The Active Directory replication system uses the USN to detect and replicate changes to Active Directory to all the domain controllers on the network. All data that is restored non-authoritatively appears to the Active Directory replication system as old data. Old data is never replicated to any other domain controllers. The Active Directory replication system updates the restored data with newer data from other domain controllers. Performing an authoritative restore resolves this issue.

Note Use an authoritative restore with extreme caution because of the effect it may have on Active Directory. An authoritative restore must be performed immediately after the computer has been restored from a previous backup, before restarting the domain controller in normal mode. An authoritative restore replicates all objects that are marked authoritative to every domain controller hosting the naming contexts that the objects are in. To perform an authoritative restore on the computer, you must use the Ntdsutil.exe tool to make the necessary USN changes to the Active Directory database.

There are certain parts of Active Directory that cannot or should not be restored in an authoritative manner:

- You cannot authoritatively restore the schema.
- The configuration naming context is also very sensitive, because changes will affect the whole forest. For example, it does not make sense to restore connection objects. Connection objects should be recreated by the Knowledge Consistency Checker (KCC) or manually. Restoring server and NTDS settings objects makes sense when no destructive troubleshooting was done before. If you are unsure, contact Microsoft Product Support Services for help:

    http://support.microsoft.com/default.aspx?scid=fh;EN-US;CNTACTMS

- In the domain context, do not restore any objects that deal with relative identifier (RID) pools. This includes the subobject "Rid Set" of domain controller computer accounts and the RidManager$ object in the SYSTEM container.
- Another issue is that many distinguished name-type links may break when you restore. This may affect objects that are used by the File Replication Service (FRS). These exist underneath CN=File Replication Service,CN=System,DC=*yourdomain* and CN=NTFRS Subscriptions,CN=*DC computer account*.
- Attempts to authoritatively restore a complete naming context will always include objects that can disrupt the proper functionality of crucial parts of Active Directory. You should always try to authoritatively restore a minimal set of objects.
- Finally, similar issues might exist for objects created by other applications. These go beyond the scope of this article.

A system state restore replaces all new, deleted, or modified objects on the domain controller that is being restored.

A system state restore of a naming context that contains two or more replicas is an authoritative merge. In an authoritative merge, all objects that are deleted or modified are rolled back to when the backup was made. Objects that were created after the backup are replicated from naming context replicas. An authoritative merge represents a merge of the state that existed when the backup was made with new objects that were created after the backup.

When you non-authoritatively restore a naming context that contains a single replica, you actually perform an authoritative restore.

back to the top

Perform an Authoritative Restore

After the data has been restored, use Ntdsutil.exe to perform the authoritative restore:

1. At a command prompt, type `ntdsutil`, and then press ENTER.
2. Type `authoritative restore` and then press ENTER.
3. Type `restore database`, press ENTER, click **OK**, and then click **Yes**.

back to the top

Restore a Subtree

In many cases you may not want to restore the entire database due to the replication impact this would have on your domain or forest. The following steps will allow you to authoritatively restore a subtree within a Forest.

1. Restart the domain controller.
2. When the Windows 2000 Startup menu is displayed, select Directory Services Restore Mode, and then press ENTER.

3. At a command prompt, type "ntdsutil" (without the quotation marks), and then press ENTER.

4. Type "authoritative restore" (without the quotation marks), and then press ENTER.

5. Type "restore subtree "ou=<OU Name>,dc=<domain name>,dc=<xxx>"" (without the quotation marks), and then press ENTER, where <OU Name> is the name of the organizational unit you want to restore, <domain name> is the domain name the OU resides in, and <xxx> is the top level domain name of the domain controller, such as com, org, or net.

6. Type "quit" (without the quotation marks), press ENTER, type "quit" (without the quotation marks), and then press ENTER.

7. Type "exit" (without the quotation marks), and then press ENTER.

8. Restart the domain controller.

back to the top

REFERENCES

For additional information about restoring the system state to a domain controller from a previous backup, click the article number below to view the article in the Microsoft Knowledge Base:

240363 How To Use the Backup Program to Back Up and Restore the System State in Windows 2000

For additional information about the impact of performing an authoritative restore, click the article number below to view the article in the Microsoft Knowledge Base:

216243 Authoritative Restore of Active Directory and Impact on Trusts and Computer Accounts

248132 Recover a Deleted Domain Controller Computer Account

back to the top

Keywords: kbHOWTOmaster kbnetwork KB241594
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch

Send feedback to Microsoft