How to Restore System State on an Active Directory Domain Controller

Information

The Active Directory database can be restored via System State on a Windows Domain Controller. However, this process requires special procedures which are different from a standard System State restore.

Overview

A Windows Server running Active Directory Domain Services must be booted into Directory Service Restore Mode (DSRM) in order to restore the System State. DSRM is similar to Windows Safe mode and has no Active Directory services running.

DSRM mode behaves very differently from normal boot mode.

Requirements

There are many requirements for System State restore to an Active Directory Domain Controller, most of which revolve around the limitations of DSRM mode.

> ⚠ Active Directory restore can not be performed if the backup is older than the tombstone lifetime set in Active Directory. This is a Microsoft limitation. See the following article for more information: Useful shelf life of a system-state backup of Active Directory

Enable the built-in administrator account (applies only to Windows Small Business Server and Essentials Server family)

1. In normal boot mode, enable the built-in “administrator” account, which is disabled by default
    a. Assign a password. For all examples on this page, we will use *dsrm-password* as our password.
    b. See this Technet article for details: What Username and Password Do I Need to Use for Directory Services Restore Mode (DSRM) in SBS 2008?

> ⓘ The DSRM password can be reset using the following procedure: How To Reset the Directory Services Restore Mode Administrator Account Password

Boot into DSRM mode

1. Restart the computer, and press F8 during the boot phase so that system boot menu is displayed.
2. Select DSRM mode from the boot menu.
    a. See the following Technet articles for more details:
        i. For Windows Server 2008, Windows Server 2008 R2 and up: Restart the Domain Controller in Directory Services Restore Mode Locally
        ii. For Windows Server 2003, Windows Server 2003 R2: Restart the domain controller in Directory Services Restore Mode locally
3. Log on to Windows
    a. Username: *.\Administrator*
    b. Password: *dsrm-password*

Reconfigure the log-on user for all ZCB Services

ZCB uses two services to control backup and restore, named **ZWC Service** and **ZCB Service**. In a standard environment, these services are configured to run as the *amandabackup* user. The *amandabackup* user is not available in DSRM mode. All ZCB services must be reconfigured to run under the Local System account.

The **ZWC-Database** service will also exist, but it runs as the Local System account by default.

To reconfigure the log-on user:

1. Open Services.msc
2. Right click the ZWC Service and click **Properties**.
3. Visit the Log On tab
4. Change the log-on user to the Local System account.
5. Restart the service.
6. Repeat for ZCB Service and, if necessary, for ZWC-Database.

The ZWC Service and ZCB Service log on settings will be reverted back to *amandabackup* as part of the restoration process. If you must perform multiple DSRM restores for some reason, please remember to change the log-on user for these services before you begin each time.

Restore the System State

Restoration can begin once the requirements are met. As shown above, the server must be in DSRM mode and the services reconfigured.

The restoration process, shown below, depends on where your backups are stored.

Scenario #1: Backup archives are stored on directly attached storage

1. Simply open ZCB and proceed with restoration of the chosen System State backup to the Original Location.
2. Use the Monitor or Report pages to observe the restore progress and result.

Scenario #2: Backup archives are in the Cloud.

1. The DNS server must be set manually, unless there are multiple Domain Controllers (DNS Servers) in your environment.
    a. Change the DNS setting of your primary network interface to a public DNS server, such as OpenDNS: 208.67.222.222 or Google: 8.8.8.8.
    b. This setting will be reverted back by the restoration process.
    c. This step is required because the "Preferred DNS Server" setting of the local network adapter points to itself by default on a Domain Controller. However, the DNS service is not running in DSRM mode.
2. Open ZCB and proceed with Restoration of the chosen System State backup run to Original Location.
3. Use the Monitor or Report pages to observe the restore progress and result.

Scenario #3: Backups are only on CIFS/NFS share.

There are two options:

1. Ensure that the local **administrator** user account on the domain controller can access the network device using the *dsrm-password* pass word.
    a. Map the share using different credentials.
    b. Test and ensure correct security permissions to the network share before the restore begins.
2. If you are not able to access the network share in DSRM mode, reboot to normal mode and copy the backup data from the network share to the local drive.
    a. Then use the "Restore Catalog from Local Directory" option in ZCB (Tools menu > Restore Catalog) to restore the backup set.

Once completed, open ZCB and proceed with Restoration of the chosen System State backup run to Original Location. Use the Monitor or Report pages to observe the restore progress and result.

Scenario #4: Backups are on a Windows Share.

This scenario is a bit challenging when there is a single domain controller, as it requires connecting to the network share when the domain controller is not available.

It is much simpler to copy the backup archive from the network share to the local drive, and then use the "Restore Catalog from Local Directory" option in ZCB (Tools menu > Restore Catalog) to restore the backup set. Once complete, open ZCB and proceed with Restoration of the chosen System State backup run to Original Location. Use the Monitor or Report pages to observe the restore progress and result.

If the above (moving the backup data to local system) is not possible, please continue with the directions below.

If the server is the the only domain controller on the network:

1. Reconfigure the network share containing your backup archives to give both Share and NTFS read permissions to a local **administrator** user on the member server.
    a. This is required because the member server has to query the DC to allow connection to its share, but the DC is not available, since it is booted in DSRM mode.
2. If the local **administrator** user password on the member server is *dsrm-password*, the connection to network share will work.
3. If the chosen password is not *dsrm-password,* map the network drive with the credentials of any local user account (but not **administrato r**) who has appropriate permissions on the member server.

    a. See the following article http://technet.microsoft.com/en-us/library/bb490717.aspx.
4. Assign the same drive letter to the mapped network drive as in the original setup.
    a. Example: If the mapped drive was assigned to Z:\ in normal boot mode, it should also be assigned to Z:\ in DSRM mode.
5. Open ZCB and proceed with Restoration of the latest System State backup run to Original Location.
6. Use the Monitor or Report pages to observe the restore progress and result.

If there are other domain controllers on the network:

1. If the local **administrator** user password on the member server is *dsrm-password*, the connection to network share will work.
2. If the chosen password is not *dsrm-password,* map network drive with the credentials of any local user account (but not **administrator**) w ho has appropriate permissions on the member server.
    a. See the following article http://technet.microsoft.com/en-us/library/bb490717.aspx.
3. Assign the same drive letter to the mapped network drive as in the original setup.
    a. Example: If the mapped drive was assigned to Z:\ in normal boot mode, it should also be assigned to Z:\ in DSRM mode.
4. Open ZCB and proceed with Restoration of the latest System State backup run to Original Location.
5. Use the Monitor or Report pages to observe the restore progress and result.

After the System State Restore

Case #1: Your server is the one and only domain controller in your environment

Restart the server after the System State restore is complete. No further steps are necessary.

Case #2: There are multiple domain controllers in your environment

The Active Directory database exists and is replicated to every domain controller in your environment. Every time any object in the database is updated, the database version number changes. Such changes are synchronized by the replication process that takes place between all domain controllers.

By default, restoring System State on a Domain Controller is a non-authoritative AD restore. The changes made by the restore will not be propagated out to other DCs.

After the restore, once the system boots back to normal mode, Active Directory will be updated (synchronized) to the latest version from other DCs in your environment. The other DCs will propagate AD back to the system, and overwrite the changes to Active Directory that were made by the restore.

For example:

- You accidentally deleted an Organization Unit in AD.
- Synchronization between DCs took place and deletion of this object propagated to other domain controllers.
- You run a System State restore on one of the domain controllers. By default, this is a non-authoritative restore.
- The restored AD database contains deleted objects, but its version is older than the database present on the on other DCs.
- The Domain Controller with the restored Active Directory is rebooted into to normal mode, and synchronization with other DCs will occur.
- The deleted object that were restored will **NOT** appear in AD, because the synchronization process will once again propagated the deletion of this object.

If the goal of your System State restore is anything *except* the restore of a deleted Active Directory object, the default non-authoritative restore is sufficient.

If the goal of your System State restore is to restore a deleted Active Directory object, you must mark this restore as an authoritative restore.

Option A (default): Non-authoritative restore

System State restores are non-authoritative by default. If the goal of your System State restore is anything *except* the restore of a deleted Active Directory object, no further steps are necessary. Simply reboot the system after the System State restore is complete.

Option B: Authoritative restore

Authoritative restore is a process of marking AD objects in the restored database as the authority for other domain controllers. After an authoritative restore, the synchronization process will propagate the changes to other domain controllers.

Follow these steps to perform an authoritative restore:

1. After the System State restore is successful, but *before* you boot into normal mode, launch **NTDSUTIL**.
    a. Click **Start**, click **Run**, type **ntdsutil**, and then press ENTER.
2. In Windows 2008 and up, type **activate instance ntds** at the **ntdsutil** prompt and then press ENTER.
    a. This step is not necessary for Windows 2003.
3. Type **authoritative restore** at the **ntdsutil** prompt and then press ENTER.
4. To restore a subtree or individual object, type one of the following commands, as appropriate, and then press ENTER.

a. To restore a subtree (for example, an organizational unit and all child objects):
   restore subtree *DistinguishedName*
b. To restore a single object:
   restore object *DistinguishedName*
c. *DistinguishedName* is the distinguished name of the subtree or object that is to be marked authoritative

5. For example, if you want to restore a deleted organizational unit named *Marketing NorthAm* in the *corp.contoso.com* domain, type:
   a. **restore subtree "OU=Marketing NorthAm,DC=corp,DC=contoso,DC=com"**
6. Click **Yes** in the message box to confirm the command.
7. At the **authoritative restore** and **ntdsutil** prompts, type **`quit`** and then press ENTER.
8. Restart the domain controller in normal operating mode.

For more information

Please see the following Microsoft Technet articles

- Mark an Object or Objects as Authoritative.
  - Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2
- Mark the object or objects authoritative
  - Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2
- How to Perform an Authoritative System State Restore in SBS 2008/2011 Standard
- Restoring Active Directory from Backup Media