www.uTools.nl

Session: What's new in 2003 compared to 2000

Level: 300

English version, release: 24 Nov 2003.
Written by Edward Willemsen.

Contents

1. Common

This session is meant to inform Microsoft Technical skilled people about most of the new features within Microsoft Windows Server 2003 compared to Microsoft Windows 2000 Server. Basic knowledge of the previous Windows platform is required to understand the new features.

For the ease of readability Microsoft Windows 2000 Server will be abbreviated as W2K and Microsoft Windows Server 2003 will be abbreviated as W2K3.

2. Functional Levels

In W2K you could use the domain in Windows 2000 Mixed mode or Windows 2000 Native mode.

Domain Functional Level	Supported DCs
Windows 2000 Mixed	Windows NT 4.0 Windows 2000 Windows Server 2003
Windows 2000 Native	Windows 2000 Windows Server 2003
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003
Windows Server 2003	Windows Server 2003

In W2K3 these modes are extended to four domain functional levels en three forest functional levels.

Forest Functional Level	Supported DCs
Windows 2000	Windows NT 4.0 Windows 2000 Windows Server 2003
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003
Windows Server 2003	Windows Server 2003

The forest functional level decreases the Global Catalog replication traffic. This is established through a new replication algorithm.

The forest functional level also enables the possibility to rename a domain or a forest.

2.1. LDP.EXE

Not new but very useful in determining the functional level of the networks domain controllers:

- Start the Ldp.exe file.
- On the Connection menu, click Connect.
- Specify the domain controller you want to query, or leave the space blank to connect to any domain controller.
- After you connect, the RootDSE information for the domain controller appears. The forest, domain, and domain controllers are included.

The following is an example of the Windows Server 2003 domain controller, the domain mode is Windows Server 2003 and the forest mode is Windows 2000.

```
1> domainFunctionality: 2=(DS_BEHAVIOR_WIN2003)
1> forestFunctionality: 0=(DS_BEHAVIOR_WIN2000)
1> domainControllerFunctionality: 2=(DS_BEHAVIOR_WIN2003)
```

The domain controller functionality represents the highest possible functional level for this domain controller, not at the function level that the domain controller is operating.

3. Trust relationships

The different kind of trusts relationships which can be establish using an W2K3 environment.

External trust.
Incoming trust.
Outgoing trust.
Two-way trust.
Shortcut trust.
Cross-forest trust.

Cross-forest trusts are not transitive.

4. Active Directory Services service

The W2K3 directory partition is extended with an extra partition type. The W2K partitions are the following:

Schema-partition;
Configuration-partition;
Domain-partition.

Every change within the partition is followed by a complete replication of this new data to all Domain Controllers within a forest. This takes huge amount of bandwidth and time. The new partition type in W2K3 is names Application directory partition. This partition is replication on a as-necessary basis to pre-defined domain controllers. Later in this session will be explained how Microsoft DNS is using this new partition type.

The schema can be prepared using a new utility ADPREP. Use ADPREP /Forestprep to prepare a schema master. Use the ADPREP /Domainprep command to prepare an infrastructure master.

5. Group Policy Object

Group Policy Objects, GPOs, can be assigned using WMI, Windows Management Instrumentation, dependencies. A useful practice it to determine the amount of free disk space before applying a published of assigned application.

Another new feature is the possibility to implement Software Restriction Policies. This enables the Administrator to restrict the execution of code. The restriction methods are the following: Hash, Certificate, Path or Internet Zone. Hash is applied with the highest priority, Internet Zone with the lowest.

GPOs can be cross-forest assigned.

There are new tools available for the management of GPOs. The most important tools are the following:

RSoP utility
Resultant Set of Policies utility enables the possibility to determine the active policy for an Active Directory object. The utility provides logging and planning modes.

DSAdd
Tool to add computers, contacts, groups, OUs or users.

DSGet
Displays selected attributes of an Active Directory object.

DSMod
Enables the possibility to modify an existing Active Directory object.

DSMove
This tool can be used to move or rename Active Directory objects.

DSQuery
Enables the possibility to create lists of computers, groups, OUs, servers or users by using a specified search criterion.

DSRm
Utility that can be used to delete an Active Directory object.

The DSQuery output can be redirected to most of the other DS* tools. Here are some useful examples:

Disable all all user account how haven't logon the last 3 months (13 weeks): dsquery users -inactive 13 | dsmod user -disabled yes >> MonthlyDisabledAccounts.txt
Delete all computers that haven't been active for 52 weeks: dsquery computer -inactive 52 | dsrm >> YearlyCleanupRemovedComputers.txt
Find user accounts who haven't change their password the last 30 days: dsquery user -stalepwd 30 | dsget user -desc -dn >> PasswordNotChanged.txt

The refreshment of group policies, which could be done through SECEDIT /REFRESHPOLICY, is no longer part of the SECEDIT utility. Refreshment can be established through the new GPUPDATE.EXE command. The SECEDIT utility is still available and unique in it's functionality. Using SECEDIT a security template can be applied completely or just partly.

Folder redirection can be applied to a single location for a site, domain or OU. In W2K3 it can also be applied using security groups.

6. DNS

As mentioned before the usage of DNS is changed. To be more precise, the use of Active Directory Services Integrated zones has been changed. The standard Primary (master) and Secondary (slave) zones still use a text file for their data. The ADS Integrated zone is placed in the new partition type: application directory partition.

When creating an integrated zone there must be chosen between the new different methods of DNS database replication. These methods are the following:

- To all DNS server in the Active Directory forest.
- To all DNS server in the Active Directory domain.
- To all domain controllers in the Active Directory domain. (Default within a Windows 2000 forest).
- To all domain controllers specified in the scope of the following application directory partition.

Custom DNS partitions can be created using the following command:

DNSCMD <servername> /createdirectorypartition <fqdn>
This command created the source database.

DNSCMD <servername> /enlistdirectorypartition <fqdn>
This will create a replication partner for the database.

DNSCMD can be installed using the Suptools.msi within the Support\Tools folder on the Windows Server 2003 CD-ROM.

The default names of Active Directory Integrated zones are DomainDNSZones and ForestDNSZones. These names are self-explaining considering the replication methods.

Beside the usual Primary, Secondary en Active Directory-Integrated zones a new zone is created, the Stub zone. A Stub zone records authoritative DNS servers within a domain. A Stub zone can contain three types of records: SOA, NS and A. These records a read-only, all changes occur from within the original primary zone. Simply put, a Stub zone doesn't know the answer, but he knows who to ask. Stub zones can be used when a problem cannot be solved using traditional delegation or within environments with disjoint namespaces. The information within the Stub zone is depending on the replication of NS records, which occurs automatically within an Active Directory forest. This is not the matter with two split-brained forests, were permission is required for replication.

Conditional Forwarding makes it possible to redirect queries to a specific DNS within another namespace. This feature enables a simple method for name resolution between

two forests, without the use of establishing secondary zones. The DNS server compares the queried name to the list of domain name conditions. It uses the longest domain name condition matching the queried name.

7. Terminal Services

In W2K Terminal Services has to be installed completely before remote desktop can be used using the Remote Administration mode. Within W2K3 Remote Desktop can be activated with by checking a single check box. The installation of Terminal Services is not needed, which use fewer resources.

Windows Server 2003 Terminal Services can be used within a NLB, Network Load Balanced, cluster environment. This feature needs a Terminal Services Session Directory database in which it can store and manage it's session information. Best practice is to place this database server outside the NLB cluster. The functionality can be installed using the default Add/Remove Windows Components program. The servers within the NLB Cluster must be added to the database servers Session Directory Computers local group.

Note

Cluster Services is integrated within the Windows Server 2003 Enterprise and Datacenter Editions. The CLB, Common-Object Load Balancing, functionality is dropped.

8. Global Catalog

The usage of a Global Catalog can be minimized within multi-site environments. Within W2K3 Microsoft has implemented a feature called Universal Group Membership Cache. This feature must be implemented per site, so that all Domain Controllers are going to cache the mentioned membership. Doing this will minimize replication traffic.

Domain Controllers and Global Catalog servers can be promoted from media. This way a DC or GC can be backed-up and restored to a different server. This way lots of site replication can be avoided. Although this option is mentioned as new within W2K3, it is also available in W2K SP4. The option to promote from media is visible when DCPROMO.EXE is started in Advanced mode using: DCPROMO /ADV.

9. Disaster Recovery

9.1. ASR

The usage of ERD, Emergency Repair Disk, is changed to a new method of disaster recovery called ASR, Automated System Recovery. This process creates an back-up file and a floppy disk. To recover a server, the server has to be rebooted from the original CD-ROM. During startup, the F2 key must be pressed and the ASR floppy disk must be inserted. The disk contains to files, ASR.SIF and ASRPNP.SIF which contains references to the installed system files.

9.2. EMS

Another new feature is EMS, Emergency Management Services. Using this feature servers can be approached by an VT100 sessions which is connected to the servers serial port. Current recovery possibilities are very limited.

9.3. VSS

The Volume Shadow Copy Service, VSS, can be used to give a user the ability to undelete files or recover older document versions from a network share. The feature is enabled on a per volume basis. On each client, read Windows 2000 Professional (SP3 or higher) and Windows XP Professional, the Shadow Copy Client, aka Previous Version client, software must be installed. This client must be downloaded from the Microsoft Web site, search for ShadowCopyClient.msi. The System Shadow Copy provider uses a copy-on-write mechanism to enable this feature.

(On systems with a file system's cluster size smaller than 16KB the possibility exists that a Shadow Copy may be lost when you Defrayment a volume. KB312067).

10. Other features

SUS, Software Update Services.
MS-BSA, Microsoft Baseline Security Analyzer.
GPMC, Group Policy Management Console.
WSS, Windows SharePoint Services.

Note

When using the Windows Server 2003 Administration Pack on Windows 2000 the minimum required Service Pack must be 3.

11. Appendix A

11.1. How to

Remote Restart

Use Manage Computer MMC and select; Connect to <system>
Select Properties from Computer Manager
Select Advanced
Select Startup & Recovery Settings
Click Shutdown (popup with restart/shutdown appears).

11.2. Resources

11.2.1. GPMC Whitepaper

http://www.microsoft.com/windowsserver2003/docs/MigGPOs.doc

11.2.2. EMS Whitepaper

http://download.microsoft.com/download/5/7/7/577a5684-8a83-43ae-9272-ff260a9c20e2/EMS10.exe

11.2.3. Windows Server 2003 Terminal Server Licensing

http://www.microsoft.com/windowsserver2003/docs/termservlicensing.doc

11.2.4. Migrating NT 4.0 Domains to Windows 2003 Active Directory

http://www.microsoft.com/windowsserver2003/docs/NT4domtoad.doc

11.2.5. Overview Windows Server 2003 Clustering

http://www.microsoft.com/windowsserver2003/docs/ClusteringOverview.doc

11.2.6. Quorums in Windows 2003 Cluster

http://www.microsoft.com/windowsserver2003/docs/ClusterQuorums.doc

11.2.7. Overview Windows Server 2003 Application Services

http://www.microsoft.com/windowsserver2003/docs/Appserv.doc

11.2.8. Remote Administration of Windows Using RDP

http://www.microsoft.com/windowsserver2003/docs/tsremoteadmin.doc

11.3. Feature Packs

http://www.microsoft.com/windowsserver2003/downloads/featurepacks/default.mspx

Here you can find the GMPC, Remote Control Add-on, Shadow Copy Client and much more useful utilities.