10.1. Recovery and Availability

You should be familiar with the following tools available for managing disaster recovery and availability.

Tool	**Description**
Windows Server Backup	Windows Server Backup provides backup and recovery for Windows Server 2008 and above (2008 R2, 2012, 2012 R2, etc.) It allows you to manage backup and recovery from either the command line using **Wbadmin** or the Windows Server Backup console snap-in.
Windows Recovery Environment	Windows Recovery Environment is a partial version of the operating system and a set of tools that you can use to recover the operating system or the full server (you must have a backup created earlier using Windows Server Backup). The following tools are included in the Windows Recovery Environment: • **Windows Complete PC Restore** allows you to restore the operating system or full server using an existing backup. • **Windows Memory Diagnostic Tool** to check the computer's RAM. This tool requires you to restart the system and to run a valid version of Windows Vista (and above: Windows 7, Windows 10) and Windows Server 2008 (and above: 2008 R2, 2012, 2012 R2, etc.) **Command Prompt** opens a command prompt window with Administrator privileges that provides full access to your file system and volumes. To access the Windows Recovery Environment tools, use the **System Recovery Options** dialog in the Install Windows wizard.
Shadow Copies	Volume Shadow Copy Services (VSS or simply Shadow Copy) automatically makes copies of files at regular intervals. Using shadow copies, you can do the following: • Recover deleted files or folders.

	- Recover a previous version of a modified file. - Compare a file with a previous version of that file.
Clustering	Clustering allows you to connect a group of independent computers to increase the availability to applications and services. Each clustered server is called a node. The nodes are connected physically by cables and use software to monitor and maintain the connections. If a node fails, another node begins providing the services of the failed node (this is called *failover*). Failover clustering allows users to experience a minimum of interruptions.
Network Load Balancing	Network Load Balancing (NLB) allows you to load balance network traffic (sent to a cluster virtual IP address) among multiple servers in an NLB cluster. To use NLB, install NLB on a server and add two or more machines to the NLB cluster. Each machine uses two IP addresses: a unique address and the cluster address. This allows the DNS server to respond to clients by sending them to a single IP address. Each server in the cluster runs an algorithm to determine which server responds to the next request. You can have up to 32 machines in an NLB cluster. NLB is a dynamic method for load balancing in that if a server fails (or if a server is added to the cluster), NLB recognizes the change and compensates for it through convergence, a process whereby the server is removed from (or added to) the cluster.

10.2. Windows Backup

Windows Server Backup provides backup and recovery for Windows Server 2008. It replaces the **NTbackup.exe** backup utility in previous Windows versions. Windows Server Backup allows you to manage backup and recovery from either the command line or the Windows Server Backup console snap-in.

You should know the following facts about Windows Server Backup:

- Windows Server Backup uses Volume Shadow Copy Server (VSS) and block-level backup to back up and recover the system.
- Full backups take less time than they did in previous Windows versions.
- As you restore a specific item from an incremental backup, you do not need to run every backup on which the item was restored. You need only select the date on which you backed up the version of the item.
- To install and use Windows Server Backup, you must be a member or either the Administrators group or the Backup Operators group. Alternatively, you can receive permissions to use Windows Server Backup through delegation.
- You can recover the operating system to the same machine, or in the event of a hardware failure, to a new machine.
- Windows Server Backup automatically manages disk usage. It will automatically reuse the space of old backups when it creates new backups.
- You cannot use Windows Server Backup to recover backups created with **NTbackup.exe**. To recover these backups, download the version of **NTbackup.exe** for Windows Server 2008. This tool can only be used to restore previously-created backups, not perform backups.

Windows Server Backup provides three ways to run backups:

- Windows Server Backup MMC snap-in. Using the snap-in, you can run wizards for scheduling backups. It also allows you to connect to other computers and manage backups. To do so, click the **Action** menu and select **Connect to Another Computer**.
- **Wbadmin** from the command prompt. It allows you to perform the same operations as the snap-in from the command line.
- PowerShell cmdlets for Windows Server Backup. The cmdlets allow you to write scripts to perform backups.

***Note**: Because there is no GUI for the Server Core installation of Windows Server 2008 (and above: 2008 R2, 2012, 2012 R2, etc.), you must administer Windows Server Backup either remotely using the Windows Server Backup snap-in or from the command line using the **Wbadmin** command. The PowerShell cmdlets are not supported because PowerShell does not run on server core.*

When you create a backup, you need to specify the volumes to include. Windows Server Backup allows you to select the following types of volumes (***Note**: These volumes must be NTFS-formatted and on a locally attached disk)*:

- **Full server**, which includes all the volumes. Best practice dictates that you choose this option as it allows you to recover the full server.
- **Critical volumes** contain the operating system. This option allows you to recover the operating system or system state.
- **Non-critical volumes** contain files, applications, and data.

***Note**: Windows Server Backup does not allow you to back up individual files or directories.*

Windows Server Backup can save backups to the following storage types:

Storage Type	**Description**
Local disk	Backups to local disk are saved on a separate, dedicated disk. • Backups on disk can be used to recover the full server, critical volumes, non-critical volumes, individual files and folders, and applications and their data. • Disks used for backup are not visible in Explorer and cannot be used for saving data. • Windows Server Backup formats the disks as part of the preparation for performing backups. • You can store a maximum of 512 backup copies on a disk. This number varies according to the storage capacity of the disk and the extent of the changes in each backup. If you need to store more backup copies, use multiple disks.

External disk	Backups to external disks are much the same as backups to a local disk. • Backups to an external disk can be used to recover the full server, critical volumes, non-critical volumes, individual files and folders, and applications and their data. • Disks are reformatted prior to use, and are not visible in Explorer. • Best practice dictates that you use USB 2.0 or IEEE 1394 disks with 2.5 more times capacity than the set of items you back up. • You can use multiple disks for automatic backup storage. When you create the schedule, all the disks must be attached and available. However, you do not have to leave the disks attached after the backups begin. Best practice dictates that you use only one connected drive at a time. When you want to use a new disk, detach the current disk and attach another disk from the series. This allows you to rotate the disks for offsite disaster protection or other reasons. If you want to force the backup to go to a specific disk among several attached disks, detach or disable the other disks in the backup series.
Shared folder	Backups to a shared folder are saved to a network share. • Backups to a shared folder can be used to recover the full server, critical volumes, non-critical volumes, individual files and folders, and applications and their data. • Backups stored on a shared folder are not saved consecutively. Rather, each backup operation overwrites the previous backup. If a backup operation fails, you may be left without a backup. You can avoid this by storing your backups in subfolders of the shared folder. • If you enable IPSec in your domain, you must save the backup to a shared folder on an IPSec boundary computer. If not, you cannot access the shared folder when you use a Windows Setup Disk to access the Windows Recovery Environment.

DVD	Backups can be stored on DVD. However, this backup media has more limitations than other media. - Backups stored on optical or removable media only allow you to recover volumes, not applications or specific files. - When the DVD backup contains all critical volumes, you can use the backup to perform a system restore. - Backups to DVD are compressed, so it's likely that the backup size on the DVD is smaller than the actual size of the volume. - Backups to DVD can span multiple DVDs if necessary. When one DVD reaches capacity, the system prompts you to insert the next DVD. - When you create a backup to DVD, the destination has to be larger than 1 GB in size, or it is blocked from the list of available devices.

Note*: You cannot back up to tape. Windows Server Backup does not support backups to tape devices.*

10.3. Backup Operations

The table below describes the types of backups you can perform using Windows Server Backup.

Backup Type	Description
Automatic backup	You can create automatic backups using the Backup Schedule Wizard in the Windows Server Backup console or using the **wbadmin enable backup** command. • By default, automatic backups run once a day. You can modify the schedule to take backups more often, but you cannot schedule automatic backups less frequently than once a day. • When you create the backup, you need to determine whether to back up the full server or specific volumes. By default, volumes that hold operating system components (the system volumes) are included, and you cannot exclude them. However, you can include or exclude data volumes as needed. • You can only use local or external disks for the backup. If you want to back up to a different medium, choose a method other than automatic backups. • When you use the wizard, you can only use local or external disks. However, you can save scheduled backups to a volume when you use the **wbadmin enable backup** command. • Use **wbadmin disable backup** to stop the automatic daily backups.
Manual backup	You can run backups manually by using the Backup Once Wizard or the **wbadmin start backup** command. • You can save backups to local disk, DVD, removable media, or a shared folder.

	- When backing up to shared folder or local disk, you can recover individual folders and files. When backing up to DVD or removable media, you can only restore full volumes. - To use a shared folder, DVD, or removable media, you must select **Different options** in the **Backup options** page. Otherwise, the settings used for automatic backups will be used (and only local disks will be supported). - Best practice dictates that you use manual backups only to supplement regularly scheduled backups.
Scheduled backup	To run backups automatically but avoid running them on the default at-least-once-a-day schedule, use Task Scheduler and the **wbadmin start backup** command. You can do this by either running the command through a series of scheduled tasks or by launching a batch file. However, make sure that this custom schedule doesn't conflict with any regular backup schedule or one of the backup operations will fail. Using the **wbadmin start backup** command allows you to have full control over the types of data you wish to back up. For example, when you create a comma-delimited list of volumes to back up using the **-include** switch, you do not have to include system volumes as you do with other types of backups. Use the **-backupTarget** switch to designate the storage location for the backup.
System state backup from command line	If you want to create a backup of the system state, use the **wbadmin start systemstatebackup** command (this backup option type is not available through snap-in). A system state backup can only be saved to a locally attached disk (the disk can be either internal or external), not a DVD or shared folder. When recovering data from a system state backup, you can only recover the system state and system applications. You cannot recover volumes or files from a system state backup. While you can't configure a scheduled backup for system state backups, you can still script the **wbadmin start**

	systemstatebackup command and use the Task Scheduler to perform backups on a schedule.

Be aware of the following when using Server Backup:

- Configuring backups to disk using **Wbadmin** requires you to know the disk ID. Use **wbadmin get disks** to view information, including the disk ID, for installed disks.
- After you create the first backup, best practice dictates that you perform a test recovery.
- You can monitor the status of a backup or recovery using the following sections in the snap-in:
    - **Messages**
    - **Status**
    - **Scheduled Backup**

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

10.4. Restore Operations

To perform a system recovery, you can use the following wizards or tools:

Recovery Type	**Description**
Files and folders	To recover files or folders you can use either the Recovery Wizard or **wbadmin start recovery**. You should know the following about recovering files and folders: • You can't recover files and folders from DVD, removable media, or a system state backup. You can only recover files and folders from backups stored on a hard disk or in a shared folder. • When you recover files or folders, you can select **Original Location** or **Another Location** to save the objects to a different storage location. • When backup finds duplicate files, you can select from the following three options: o **Create copies so I have both versions of the file or folder** o **Overwrite existing files with recovered files** o **Don't recover those files or folders**
Volumes	To recover volumes, you can use either the Recovery Wizard or **wbadmin start recovery**. You should know the following about recovering volumes: • You can restore a volume from a shared folder, disk, DVD, or removable media backup. • When you restore a volume, the restore operation overwrites the data on the destination volume. Make sure the destination does not contain data that you may need later before performing the restore.

Applications	To recover applications, you can use either the Recovery Wizard or **wbadmin start recovery**. You should know the following about recovering applications and their data: • To be able to recover an application, the application must have a VSS (Volume Shadow Copy Service) writer. This allows the application to register with Windows Server Backup. The VSS writer must be running when you create the backup. • You cannot recover an application from a DVD or removable media backup. • If you are recovering from your most recent backup and the application supports "roll-forward" of the application database, the **Do not perform a roll-forward recovery of the application database** option appears. Select this option if you do not want Windows Server Backup to roll-forward the application database currently on the server. • When you recover an application, you can copy the application to a different location, but you cannot recover the application to a different computer of a different name.
Backup catalog	The backup catalog stores information about the backups, such as the volumes backed up and where those backups are located. • The backup catalog is stored in the same location as your backups. • If the catalog becomes corrupted, you receive an alert, and an Event is registered in the Event log. You cannot perform more backups until you either restore the catalog using an available backup or delete the catalog. • If you delete the catalog, you can't use the Windows Server Backup snap-in to access the backups. You can use either the Catalog Recovery Wizard or **wbadmin restore catalog** to recover a corrupt catalog. In fact, you only see the Catalog Recovery Wizard in Windows Server Backup if the catalog is corrupted.

Operating system or full server	To perform a recovery of the operating system or a full server recovery, you need to use a Windows Setup disc and a Windows Server Backup backup. • To begin the recovery, boot the computer from the Windows Setup disc and select the **Repair your computer** option. • Restoring only the critical volumes restores volumes that contain operating system files, but not volumes that contain user data only. • Restoring the entire PC restores critical and non-critical volumes. • When you restore volumes, existing disks are repartitioned and reformatted, resulting in all existing data on the disks being lost. You can keep disks by excluding them from the restore process. This keeps the existing data, but does not restore those disks from the backup. You can also use the **wbadmin start sysrecovery** command to recover the volumes that contain the operating system's state, but you can only use it when you also use the Windows Recovery Environment.
System state	You can recover a computer's system state using the **wbadmin start systemstaterecovery** command line command.
Backup created with Ntbackup	In the event that you need to recover backups created with **Ntbackup**, you can download a version of **Ntbackup** for use with Windows Server 2008 and above (2008 R2, 2012, 2012 R2, etc.). However, you can only recover backups created with **Ntbackup**; you cannot create new backups with **Ntbackup**.

When you perform a recovery to a new disk, best practice dictates that the new disk be as big as the disk on which the backups were stored. For example, if you saved your backups to a 1 TB disk, the new disk must be 1 TB even if the backed up volumes came from a 100 GB disk.

10.5. Domain Controller Restore

The first step in a recovery strategy for domain controllers is to perform the proper backups while everything is working correctly. In addition to performing regular full server backups, you should perform regular system state backups. Restoring from a system state backup, when possible, is faster than restoring from a full server backup. Be aware of the following when performing a system state backup:

- Use **Wbadmin start systemstatebackup** to take a system state backup. You cannot use the Windows Server Backup console to do only a system state backup.
- The backup can only be saved to a local drive, not to a shared folder or a disc.
- The backup cannot be saved to the same drive as the system state data. While this is possible by making a registry change, doing so leads to problems under certain circumstances.
- To perform system state backups on a schedule, create a Scheduled Task that runs **Wbadmin**.

You might need to restore a domain controller if the Active Directory database on the domain controller is corrupt or lost, or if the entire server fails. When restoring Active Directory, there are two types of restore:

Restore type	**Description**
Nonauthoritative	A *nonauthoritative* restore returns the domain controller and the Active Directory database to its state at the time of backup. After the domain controller returns online, Active Directory replicates the database with other domain controllers on the network. Any changes that took place since the backup are replicated to the restored domain controller. Nonauthoritative restores are the default method for restoring Active Directory, and the most common use of a nonauthoritative restore is to bring an entire domain controller back from a serious failure.

Authoritative	An *authoritative* restore returns a designated object or container of objects to its state at the time of the backup. For example, imagine a junior administrator accidentally deletes an OU that contains a large number of users. If you restore the server from backup, the default nonauthoritative process doesn't restore the deleted OU because the domain controller is updated to the current status of its replication partners, which means that the OU is deleted. When you perform an authoritative restore, you prevent specific objects from the backup from being overwritten by Active Directory replication. With the authoritative restore, the Update Sequence Number (USN) is incremented so that it is higher than the existing USN of the (deleted) object in the Active Directory replication system. Use authoritative restore to restore specific objects in Active Directory.

The following table lists several methods for performing a domain controller restore. If possible, use the first method in the table.

Method	**Description**
DCPromo (only on 2008 R2 and below)	If the server boots but Active Directory is corrupt, you can use **dcpromo**. 1. Run **dcpromo** to remove Active Directory from the domain controller. The server becomes a member server. 2. Run **dcpromo** again to install Active Directory. Active Directory data is copied from another domain controller on the network. If you are unable to remove Active Directory, run **dcpromo /forceremoval**. The disadvantage of using **dcpromo** is that the entire Active Directory database must be replicated across the network from another domain controller. However, you can use

	the **Install from Media** option to copy the database from media to reduce network traffic.
Restore system state	If the server boots but Active Directory is corrupt, you can restore the system state data from a recent backup. After the backup is restored, Active Directory replication copies only the changed data to the restored domain controller. To use this method to restore a domain controller: 1. Reboot the server in Directory Services Restore Mode (DSRM). Use one of the following methods: o Reboot the server. Following the BIOS screen, press F8. Select Directory Services Restore Mode (DSRM) from the menu. o At a command prompt, type: ***bcdedit /set safeboot disrepair*** ***shutdown -t 0 -r*** 2. Run ***Wbadmin start systemstaterecovery*** to restore the system state data. 3. Restart the server in normal mode. If you used bcdedit to start the server in DSRM, type the following at a command prompt: ***bcdedit /deletevalue safeboot*** ***shutdown -t 0 -r*** following the restart, allow time for Active Directory replication to occur.
Critical volume or full server restore	If you are unable to reboot the server, you will need to perform a critical volume or full server restore. This restore rebuilds the entire server, along with the Active Directory database. Use the ***Wbadmin start recovery*** command to start the restore. A full server restores not only restores Active Directory, but data on all other volumes as well.

Note*: To enter DSRM, you must supply the recovery mode password. You set this password during the domain controller installation. If you need to set or change the password, use the following steps:*

1. Open an elevated command prompt by clicking **Start**, then right-clicking **Command Prompt** and selecting **Run as administrator**.
2. Type ***ntdsutil***
3. Type ***set dsrm password***
4. Type ***reset password on server <servername>***
5. Enter the password.
6. Confirm the password.
7. Type ***quit***, then ***quit*** again.

10.6. Active Directory Restore

If you need to restore lost Active Directory data, use the following methods:

Method	**Description**
LostAndFound container	When you delete an OU, all objects within the OU are also deleted. However, if you have multiple domain controllers, objects might have been added to the OU on one controller after that OU had been deleted on another domain controller. In this case, following Active Directory replication, the new objects are placed in the LostAndFound container. • Use the **View** menu to show the **Advanced Features** to see the LostAndFound container. • Move objects out of the LostAndFound container and into the necessary OUs. • Objects added to the OU before it was deleted are lost and must be restored.
Authoritative restore	To restore Active Directory data, such as deleted objects, perform an authoritative restore. Use the following process: 1. Restart the domain controller in Directory Services Restore Mode (DSRM). 2. Perform a nonauthoritative restore of a system state backup that holds the deleted objects. 3. Run the **Ntdsutil** command. 4. At the **Ntdsutil** prompt, use the **authoritative restore** command, followed by the LDAP name of the object you want to mark as authoritative. 5. Type **quit** exiting Ntdsutil, and then restarting the domain controller. Active Directory replication will copy the authoritatively restore object back to other domain controllers. It will also copy

	changes made on other domain controllers back to the restored database.
View snapshots	With Windows Server 2008 and later, you can take snapshots of the Active Directory database. You can use these saved snapshots to see how Active Directory looked at the time that the snapshot was taken. • Snapshots use the Volume Shadow Copy Service (VSS). • Snapshots are read only; you cannot restore data from a snapshot. Instead, you open a snapshot and manually record object information. To make and use snapshots: 1. Take regular snapshots of the Active Directory database. You can schedule a task to run **Ntdsutil snapshot** on a regular basis, or you can even take regular system state backups. Using **Ntdsutil snapshot** offers several advantages, so the remaining steps describe this process. 2. Run the **Ntdsutil mount** command to mount (make active) a database snapshot. You can mount multiple snapshots. 3. Run the **Dsamain** command to expose a snapshot as an LDAP server. This step allows you to connect to and view the snapshot. With **Dsamain**, you specify the path to the snapshot, along with a port number that will be used to connect to the snapshot. 4. Run the **Ldp** tool or Active Directory Users and Computers using the specified port to view the snapshot data. You can also use third-party tools, such as **ADExplorer** from Sysinternals.

When you restore Active Directory objects with an authoritative restore, it is possible that group membership will not be restored, even though the group and all user accounts exist following the restore.

- The problem occurs because group membership involves a link in the group object (the **Member** attribute, called a *forward-link*) and a corresponding link in the user object (the **MemberOf** attribute, called a *back-link*).
- Starting with Windows Server 2003, a feature called linked-value replication (LVR) enables restoring these links. To take advantage of LVR, the forest functional level must be Windows Server 2003 or higher.
- LVR allows for the replication of individual attributes instead of the entire object.
- The steps you take to restore group memberships depend on the forest functional mode at the time of the backup.

Functional mode	Description
Windows Server 2003 or 2008	If the forest functional mode has always been in Windows Server 2003 or 2008, then LVR is enabled. Group memberships are restored automatically, and no additional steps are required.
Windows 2000	In Windows 2000 forest functional mode, back-links are not restored. To restore back-links: o Manually make the necessary changes. o Run the updated version of **Ntdsutil** available on a Windows Server 2003 R1 or later server to perform the authoritative restore. This version of **Ntdsutil** creates an LDIF file that contains back-link information. Run the **Ldifde** command using this file to restore the back-links.
Windows 2000 updated to Windows Server 2003 or 2008	If the forest is at the Windows 2000 functional level, LVR is enabled when you upgrade to Windows Server 2003 or 2008 functional level. However, doing so does not automatically update group memberships. Only groups edited after upgrading the functional level can have their memberships automatically restored. o If all groups were edited following the change, no additional action is necessary.

	o To restore back-links for groups whose membership has not changed since the update to the functional level, run the **Ldifde** with the LDIF file to restore the back-links.

When you perform a system state backup, all Active Directory data, including Group Policy information stored on the Sysvol folder, are backed up. To simplify Group Policy management, you can back up and restore only Group Policy data using the Group Policy Management console.

- You can back up a single GPO or multiple GPOs at the same time into the same backup file.
- Starter GPO data is backed up separately from the GPO backup. To back up everything, you will need to back up the GPOs as well as the starter GPOs.
- Restoring a GPO creates the GPO and restores its settings.
- To move a GPO from one domain to another, or to copy GPO settings from one GPO to another, import the settings from the GPO backup. Using backup and import to migrate GPOs does not copy the DACL for the GPO. You will have to manually configure GPO permissions.
- To move a starter GPO to another domain, export the starter GPO as a .cab file, then import it in the other domain. You cannot use the backup feature to move a starter GPO to another domain.
- To restore the settings in the Default Domain Policy and the Default Domain Controller GPOs, run the **Dcgpofix.exe** tool.

10.7. Restartable Active Directory

Restartable Active Directory is the ability to stop and restart Active Directory Domain Services without shutting down the domain controller. This allows you to apply updates to the domain controller or perform offline defragmentation of the AD DS database. It also allows services that do not depend on AD DS, such as DHCP, to continue functioning and responding to user requests. Restartable AD DS is available on all domain controllers that run Windows Server 2008, regardless of functional level.

Restartable AD DS makes it possible for a domain controller to be in any of the three states described in the table.

State	Description
AD DS Started	This is the state in which Active Directory is running and fully functional.
AD DS Stopped (only on 2008 R2 and below)	This is the state in which Active Directory is stopped. A domain controller in this mode has the following characteristics: • The Active Directory database (Ntds.dit) on the local domain controller is offline. • The domain controller cannot service domain logon requests. o Another domain controller, if available, can be contacted for logon using domain credentials. o If another domain controller is not available, you can log on to the domain controller in DSRM using the DSRM password. • The server is joined to a domain, allowing Group Policy and other settings to continue to be applied to the domain controller. • The domain controller cannot replicate with other domain controllers. • You can run the **dcpromo /forceremoval** command to remove AD DS from a domain controller in this state.

Directory Services Restore Mode	This state is almost identical to the Directory Services Restore Mode in Windows Server 2003. The one exception is that you can run the **dcpromo /forceremoval** command to remove AD DS from a domain controller running in DSRM. This is the state in which you must run the machine to restore Active Directory objects using the **Ntdsutil** utility.

You should know the following about restartable AD DS:

- You cannot start a Windows Server 2008 DC in the AD DS Stopped state, but you can restart it into DSRM.
- Services such as File Replication Service (FRS), Kerberos Key Distribution Center (KDC), and Intersite Messaging that depend on AD DS shut down before AD DS stops. If they are running when you stop AD DS, they restart when you restart AD DS.
- If the domain controller is a DNS server, it cannot respond to Active Directory-integrated zone queries while AD DS is stopped. To prevent DNS lookup failures, provide redundancy by configuring member computers, application servers, and domain controllers to point to multiple DNS servers.

10.8. Offline Defragmentation

Offline defragmentation is the process of taking the Active Directory database offline, reorganizing the data within the database to make it more efficient, and returning unused disk space to the operating system.

- Online defragmentation occurs automatically (by default every 12 hours) when garbage collection runs. However, free space remains within the database file and is not returned to the system for use.
- Over time, the size of the database can grow to be much larger than the size of the objects within the database.
- The only way to return unused space from the directory database to the file system is through offline defragmentation.

To perform offline defragmentation, you run **Ntdsutil** to compact the database file to an alternate location, then copy the compacted file back to its original location in the **%systemroot%\NTDS** folder. Use the following steps:

1. Stop the AD DS service by stopping the Active Directory Domain Services service in the Services console. (Restarting the domain controller in Directory Services Restore Mode is not required.)
2. Open a command prompt as an administrator. quitRun **Ntdsutil** with the **compact** command. This copies the database file to a different location. As it copies, free space is removed from the database file. Use the following commands to compact the database:
   ```
   ntdsutil
   activate instance ntds
   files
   compact to <path>
   quit
   quit
   ```
3. Delete any log files saved in the **%systemroot%\NTDS** directory.
4. As a precaution, copy the existing Ntds.dit file to a new location.
5. Copy the compacted file you created in step 2 to the **%systemroot%\NTDS** directory.
6. You can verify the integrity of the new file using the following commands:
   ```
   ntdsutil
   ```

```
   activate instance ntds
   files
   integrity
   quit
   ```

7. If all checks pass, restart the Active Directory Domain Services service. If the checks fail, you can copy the **Ntds.dit** file back from the alternate location.

If you want to move the log or database files, use the **move** command with **Ntdsutil**. Using the **move** command updates the registry with the new file location. Do not simply copy the files to a different location. The following commands show an example:

```
Ntdsutil
activate instance ntds
files
move db to <path> or move logs to <path>
```

***Note**: Use these same commands and processes to manage database files on an AD LDS installation. To stop the AD LDS instance, stop the service that was created during the instance installation.*

10.9. System Monitoring Tools

The table below describes tools that you can use to view and monitor system events and information.

Component	**Description**
Event Viewer	Use Event Viewer to view system and error messages generated by the operating system and other programs. Through Event Viewer, you can: • View events from multiple event logs. • Save useful event filters as custom views that can be reused. • Configure event subscriptions to collect and view a set of events stored in multiple logs on multiple computers. Events from remote computers are sent to another computer where they can be viewed and stored. • Attach a task to an existing instance of error to notify you of when a particular error occurs. This is useful if you notice an error that occurs in random intervals. To manage logs and read events from the command prompt, use **Wevtutil**.
Network Monitor	Network Monitor is a protocol analyzer. Use Network Monitor to capture, view, and analyze network traffic. Network Monitor offers the following features: • Network Monitor captures packets (or packet fragments) and their contents. • You enable packet capturing on specific network interface cards. When enabled on a NIC, Network Monitor captures all traffic sent to and from that NIC. • You can use the p-mode (promiscuous mode) to capture all packets regardless of the destination MAC addresses. • Configure *filters* to specify packets to display or capture.

	◦ A *display* filter shows only the packets specified by the filter. Using a display filter does not affect the data that is in the capture file. ◦ A *capture* filter captures only the packets specified by the filter. If the packet type you are looking for is not in the capture file after using a capture filter, you must reconfigure the filter and recapture. • **Nmcap.exe** is the command-line version of Network Monitor. • You must run Network Monitor as an administrator or as a member of the Netmon users group.
Task Manager	Press **Ctrl + Alt + Delete** to start the Task Manager. Task Manager displays data in the following tabs: • The **Applications** tab allows you to view and, if needed, stop each running application. • The **Processes** tab displays each running process, memory resources in use, and a short description. • The **Services** tab displays each service needed to run active processes and applications. • The **Performance** tab graphs CPU and memory usage. • The **Networking** tab allows you to view the percentage of available network bandwidth your computer is currently using. • The **Users** tab displays each user that is currently logged in to the computer and their login method. You can disconnect users if needed.
Windows System Resource Manager	Windows System Resource Manager (WSRM) allows you to control how CPU and memory resources are allocated to applications, services, and processes on the computer. This prevents one application from consuming more than its allotted CPU and memory limits and starving other applications of CPU and memory. You can run WSRM through the Wsrm snap-in or from the command line with the **wsrm** command.

10.10. Reliability and Performance Monitor

Windows Reliability and Performance Monitor combine the functionality of the following tools that were previously only available as stand-alone tools:

- Performance Logs and Alerts
- Server Performance Advisor
- System Monitor

The table below describes the components of Windows Reliability and Performance Monitor.

Tool	Description
Resource View	The resource view shows you real-time statistics for the following categories: • CPU • Disk • Network • Memory To view details, expand each node. Resource View is a default view of important system information, but it cannot be customized and only shows current statistics (data is not saved).
Performance Monitor	Performance Monitor is a real-time visual display of a PC's overall performance. You track performance by using *objects* and *counters:* • An *object* is a statistic group, often corresponding to a specific type of hardware device or software process (such as physical disk or processor statistics). • A *counter* is a specific statistic you can monitor. For example, for the PhysicalDisk object, you can monitor counters such as %Disk Read Time or %Idle Time. Be aware of the following:

	• Performance Monitor shows real-time statistics. • You can customize the statistics you want to view. • You can save the current statistics, but you cannot use Performance Monitor to capture data over long periods of time. • Performance Monitor displays data in the following forms: line graph, histogram, report (text).
Reliability Monitor	The Reliability Monitor shows you an historical record of system changes and events. Reliability Monitor tracks: • Application installs and uninstalls • Application and Windows failures • Hardware failures Information is reported for each day over a one-year period. Each day is assigned a System Stability Index number. • The System Stability Index number identifies how stable the system is. • 1 is the least stable and 10 is the most stable. • Daily indexes are shown on a chart, with additional detail available for each day.
Data Collector Sets (DCS)	A Data Collector Set (DCS) is a group of objects and counters that can be used to capture system performance statistics over a period of time. A Data Collector Set includes one or more data collectors, which identify the specific objects and counters you want to track. There are four types of data collectors, and you can also create your own. • Use a *performance counter* data collector to save system statistics over time in a log. Logs can be saved to different log formats: o Use text files (comma or tab delimited) to import data into a spreadsheet program.

	o Use binary files to save data that is intermittent. Select a circular file to save all data into a single file, overwriting the contents when the log is full. o Use SQL database files to importing statistics into SQL server in order to perform data comparisons or data archival. • Use an *event trace* data collector to capture events logged by software processes. • Use a *configuration* data collector to monitor the state and changes to registry keys. • Use a performance counter *alert* to configure triggers that take an action when a counter reaches a threshold value. When you configure an alert you specify: o The counter you want to watch. o A threshold limits (a counter value that you want to watch for). o An action to take when the threshold value is reached. For example, you can write an event to a log, send a message, or run a program.

When monitoring Active Directory-related events, be aware of the following:

- The Directory Services object includes multiple counters to monitor Active Directory. This object includes counters for:
    - The Directory Replication Agent (DRA) to monitor replication events such as the number of inbound/outbound packets or objects, and pending replication operations.
    - Directory service (DS) events, such as reads and writes from various databases.
    - LDAP calls, including client sessions, connections, and searches.
    - Security Account Manager (SAM) operations.
- The following trace collectors record information related to Active Directory:
    - Active Directory Domain Services: Core
    - Active Directory Domain Services: SAM
    - Active Directory: Kerberos Client
    - Active Directory: Kerberos KDC

- You can use the preconfigured Active Directory Diagnostics data collector set to monitor common events related to Active Directory. The Active Directory Diagnostics data collector set includes the following collectors:
    - NT Kernel and Active Directory trace collectors to capture events logged by these processes.
    - A performance counter that monitors all counters related to the following objects: directory services, physical disk, processor, memory, network interface, TCP and UDP, IPv4 and IPv6, and others.
    - AD Registry configuration collector, to monitor changes to the registry related to Active Directory.

Note: *Users can only use the Reliability and Performance Monitor if they are part of the Performance Monitor User group.*

10.11. Active Directory Monitoring Tools

The table below describes tools that you can use to monitor and manage Active Directory.

Tool	**Description**
RepAdmin	Repadmin (Replication Diagnostics Tool) is a command-line tool that you can use to diagnose replication problems between Windows domain controllers. The following list shows some of the common switches used with Repadmin • Use **/showrepl** to show the replication partners of a domain controller. • Use **/replicate** to force replication between two domain controllers. List the target system first, followed by the source system. • Use **/syncall** to force replication between all domain controllers in a site. • Use **/showchanges** to view unreplicated changes on a domain controller. You can export this information to text file, run the command again at a later time, and then compare the results. • Use **/showconn** to show connection objects. • Use **/replsummary** to view the replication status for all domain controllers in the forest. The output lists each domain controller with status information. • Use **/showattr** to see the attributes of an Active Directory object. You can launch Repadmin from the command prompt or through its link in the Advanced Tools section of the AD DS server role in Server Manager.
ReplMon	Replmon (short for Active Directory Replication Monitor) is a GUI-based tool that you can use to perform tasks similar to those performed by RepAdmin. In addition, use ReplMon to view a

	graphical representation of the Active Directory replication topology.
Group Policy Results	The Group Policy Results wizard allows you to determine the current, cumulative effects of Group Policy settings that apply to a specific user or computer. • When you run the wizard, you select a computer and a user. • The computer you select must be turned on. The utility contacts the destination computer and queries it for effective Group Policy settings. The destination computer must run Windows XP Professional or later. • You can only select a user account that has been used to log on to the target computer. Group Policy Results creates a report based on the answers you supply during the wizard. The report shows the resultant set of policy for the user and computer you entered in the wizard. • **Gpresult.exe** is the command line version of Group Policy Results. This feature used to be referred to as Resultant Set of Policy (RSoP) logging mode.
Group Policy Modeling	The Group Policy Modeling wizard allows you to calculate the effects that GPOs have on your system before you deploy the GPOs. • When you run the wizard, you select a domain controller in a domain. The domain controller must be running Windows Server 2003 or later. • You can select a target OU, computer, or user account. • You can choose to include or exclude items from the analysis. For example, you can include or exclude specific WMI filters that have been applied, loopback processing, or GPOs linked to sites. • You can analyze the effects of moving a user or computer to a different OU, changing group memberships, or the application of Group Policy over slow links.

	• After working through the wizard, the answers you supplied are displayed in a report as if they were from a single GPO and saved as a query represented by a new item under the Group Policy Modeling node. This feature used to be referred to as Resultant Set of Policy (RSoP) planning mode.

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757