# Windows troubleshooting guideline

Education, School

Lesson 11 Active Directory Maintenance, Troubleshooting, and Disaster Recovery Knowledge Assessment Matching a. authoritative restoref. LDP b. checkpoint fileg. system volume c. Directory Services Restore Modeh. tombstone d. fragmentationi. transaction buffer e. garbage collectionj. Windows PowerShell __h__ 1. This object is created when an object is deleted within Active Directory. __i__ 2. Active Directory changes are written here before they are committed to disk. __j__ 3. This is a new advanced command-line and scripting interface included in Windows Server 2008. __g__ 4.

This volume houses the boot files for a Windows Server 2008 computer. __e__ 5. This describes the process of removing tombstoned objects from the NTDS. DIT file. __a__ 6. You will need to perform this operation if you have inadvertently deleted one or more Active Directory objects. __f__ 7. This is a graphical user interface that will allow you to query Active Directory as part of the troubleshooting process. __b__ 8. This is used as a reference file in case the Active Directory database needs to be recovered from a systemfailureto ensure that no transactions are lost. _c__ 9. To perform many Active Directory maintenance operations, you will need to restart your domain controller in this startup mode. __d__ 10. This can decrease database performance because updates are made to the Active Directory over time. Multiple Choice 1. Which of the following backup types can be initiated by a member of the local Administrators group or a member of the local Backup Operators group on a Windows Server 2008 computer? a. Manual backup b. Scheduled backup c. Full backup d. Differential backup

A manual backup can be rescheduled by a local administrator or member of the local Backup Operators group. Scheduled backups can only be created by members of the local Administrators group. 2. The NTDS. DIT file is based on which databasetechnology? a. Structured Query Language (SQL) b. Oracle c. Extensible Storage Engine (ESE) d. My*SQL The NTDS. DIT file is based on the Extensible Storage Engine (ESE) data storage format, not Microsoft SQL as some people believe. 3. Which of the following commands can be used to configure Active Directory permissions from the command line? . LDP b. Dsacls c. Dcdiag d. ADSI Edit The dsacls. exe command-line utility can be used to list and modify Active Directory permissions for a particular object or container. 4. What runs automatically on a domain controller every 12 hours by default during the garbage collection process? a. Offline defragmentation b. Authoritative restore c. Nonauthoritative restore d. Online defragmentation Online defragmentation on an Active Directory domain controller is also known as the garbage collection process. 5.

Which tool can you use to force a domain controller to start in Directory Services Restore Mode on its next reboot? a. cmd. exe b. bootmgr. exe c. bcdedit. exe d. dcpromo. exe Apart from pressing F8 during the system boot, you can configure a Windows Server 2008 computer to automatically boot into Directory Services Restore Mode by using the bcdedit. exe command-line utility before rebooting the server. 6. Which operation requires the Active Directory Domain Service to be taken offline? a. Offline defragmentation b. Online defragmentation c. Garbage Collection d. Transaction Buffering

Of the operations listed, only an offline defragmentation requires you to take the Active Directory database offline, whether through rebooting into DSRM or by using the new restartable Active Directory feature. 7. Which of the following backup types can be initiated only by a member of the local Administrators group on a Windows Server 2008 computer? a. Manual backup b. Scheduled backup c. Full backup d. Differential backup Unlike manual backups, scheduled backups can only be created by members of the local Administrators group on a Windows Server 2008 computer. 8.

Which backup type will empty the Application log on the server that is being backed up? a. Copy backup b. Differential backup c. Normal backup d. VSS full backup VSS full backup will update each file's backup history and clear the Application Log files. 9. Which of the following volumes hosts the Windows operating system? a. Boot volume b. Shared volume c. System volume d. Host volume The boot volume holds the Windows operating system and the Registry. 10. When performing an authoritative restore of a user object that belongs to multiple Active Directory groups, what is restored by the LDF file that is generated by Ntdsutil? . Optional attributes b. Mandatory attributes c. Back-links d. Security Identifier (SID) In a multi-domainenvironment, back-links need to be manually re-created after an authoritative restore by using the LDIF files generated automatically by ntdsutil. CASE SCENARIOS Scenario 11-1: Consulting for Margie's Travel You are a computer consultant for Margie Shoop, the owner of Margie's Travel. Margie has a single Active Directory domain structure with the domain margiestravel. com. Margie has travel agencies worldwide, at 50 locations in 7 countries. All locations are connected to a satellite array.

Margie has signed a 10-year contract to provide satellite access to her 50 locations. Connectivity to the satellite array varies from 57 Kbps to 128 Kbps. Although her locations vary greatly in the number of computer and user accounts, each location with more than 15 users has its own domain controller, global catalog server, and DNS server, all typically configured on the same computer. The margiestravel. com Active Directory infrastructure has nine sites. Given this information about Margie's Travel, answer the following questions: 1. You discuss performance monitoring with Margie.

During your conversation, you learn no one has ever used Replication and Performance Monitor to check the performance of her domain controllers. Margie wants to know why anyone would even bother. What do you say to her? Replication and Performance Monitor is used to provide one-time and ongoing reports of Active Directory performance counters, which can be used to proactively monitor Active Directory for potential hardware and software issues that might impact client authentication. 2. Margie tells you that some of her domain controllers have multiple hard disks. She tells you that the additional physical hard disks are not being used.

She wants to know if they can be used to improve the performance of Active Directory. What would you tell her? The Active Directory database and log files can be moved to different hard disks within a server to improve performance. 3. Margie sends you to Cairo, Egypt, to troubleshoot a few domain controllers in her Egypt location. You find some event messages concerning replication events, but you would like to see more detailed information than the data in the log now. What can you do? Modify the debugging levels in the Registry to increase the number of events that are logged to the Event Viewer.