Enforce settings,

Block inheritance

Deny apply group policy

Child group also called shadow group

Set security permissions on the group

You need to make sure that branch office administrators are able to create and manage their own GPOs respectively.

1. Modify the manageby tab on the OU and add the administrator
2. Run the delegation wizard (right to link GPO to administrator)

ADML- Active Directory Multiligual files

You need to use the French version of Administration templates

You create a folder on the PDC emulator for the subsidiary domain in the path %systemroot%\SYSVOL \domain\Policies\PolicyDefinitions\FR.

B. Copy the ADML files from the French local installation media for Windows Server 2008 R2 to the FR folder on the subsidiary PDC emulator.

Each ADML file represents the language you wish to support

ADMX represent the structure

Your partner company has an Active Directory forest that contains a single domain. The company has servers that run Windows Server 2008 R2 and client computers that run Windows 7.

You need to configure your partner company's domain to use the approved set of administrative templates.

What should you do?

B. Copy the ADMX files from your company's PDC emulator to the PolicyDefinitions folder on the partner company's PDC emulator.

Your company has an Active Directory forest that contains Windows Server 2008 R2 domain controllers and DNS servers. All client computers run Windows XP SP3.

You need to use your client computers to edit domain-based GPOs by using the ADMX files that are stored in the ADMX central store.

What should you do?

B. Upgrade your client computers to Windows 7.

Explanation/Reference:

Prerequisites for Administering Domain-Based GPOs with ADMX Files

To complete the tasks in this section, you should have at least:
A Windows Server 2008, Windows Server 2003, or Windows 2000 domain that uses a DNS name server.
A Windows Vista–based computer to use as an administrative workstation.

Since the client machine must be running at least Vista, "B" is the best answer.

Windows Server 2008 R2 and Windows 7 provide a new set of administrative template files in the ADMX format. XML

Your company purchases a new application to deploy on 200 computers. The application requires that you modify the registry on each target computer before you install the application.

The registry modifications are in a file that has an .adm extension.

You need to prepare the target computers for the application.

What should you do?

A. Import the .adm file into a new Group Policy Object (GPO). Edit the GPO and link it to an organizational unit that contains the target computers.

Reason: An ADM template is a file that is designed to be used within Group Policy to define a Registry setting and its' value

---

Look at auditing in group policy

Look at security template…..importing the security template to a gpo …link gpo to OU

Your company has an Active Directory forest that contains client computers that run Windows Vista and Windows XP.

You need to ensure that users are able to install approved application updates on their computers.

Which two actions should you perform?

(Each correct answer presents part of the solution. Choose two.)

A. Set up Automatic Updates through Control Panel on the client computers.
B. Create a GPO and link it to the Domain Controllers organizational unit. Configure the GPO to automatically search for updates on the Microsoft Update site.
C. Create a GPO and link it to the domain. Configure the GPO to direct the client computers to the Windows Server Update Services (WSUS) server for approved updates.
D. Install the Windows Server Update Services (WSUS). Configure the server to search for new updates on the Internet. Approve all required updates.

Answer: CD
Section: Configuring Group Policy

Create a Gpo to assign application to a particular OU that has computer accounts

---

Each location has a child organizational unit named Sales. The Sales organizational unit contains all the users and computers from the sales department.

The offices in London, Chicago, and New York are connected by T1 connections. The office in Madrid is connected by a 256-Kbps ISDN connection.

You need to install an application on all the computers in the sales department.

Which two actions should you perform?

(Each correct answer presents part of the solution. Choose two.)

A. Disable the slow link detection setting in the Group Policy Object (GPO).

o specify settings for Group Policy slow link detection for computers, use the **Group Policy slow link detection policy** setting in the **Computer Configuration\Administrative Templates\System\Group Policy** item of the Group Policy Object Editor. The unit of measurement for connection speed is Kbps.

To set this for users, use the **Group Policy slow link detection policy** setting in **User Configuration\Administrative Templates\System\Group Policy**.

D. Create a Group Policy Object (GPO) named OfficeInstall that assigns the application to the computers. Li the GPO to each Sales organizational unit.

Answer: AD
Section: Configuring Group Policy

Explanation/Reference:
Need to create a GPO to assign the software to computers.

Since the Madrid office is connected via a slow link, the slow link detection setting would stop distribution to that site.

Look at passwords default 42 (password may have expired if you cannot get in and you are not locked out..then change to does not expire

---

Group Policy preferences, new for the Windows Server 2008 operating system, include more than 20 new Group Policy extensions that expand the range of configurable settings within a Group Policy object (GPO). These new extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC), under the new Preferences item. Examples of the new Group Policy preference extensions include folder options, mapped drives, printers, scheduled tasks, services, and **Start** menu settings.

Group Policy preferences provide better targeting, through item-level targeting and action modes. Additionally, rich user interfaces and standards-based XML configurations provide you with more power and flexibility over managed computers when you administer GPOs.

In addition to providing significantly more coverage, better targeting, and easier management, Group Policy preferences enable you to deploy settings to client computers without restricting the users from changing the settings. This capability provides you with the flexibility to decide which settings to enforce and which settings to not enforce. You can deploy settings that you do not want to enforce by using Group Policy preferences.

You need to restore the Default Domain Controllers Policy Group Policy object (GPO) to the Windows Server 2008 R2 default settings.

What should you do?

A. Run dcgpofix.exe /target:dc.

Explanation/Reference:
Dcgpofix restores the default Group Policy objects to their original default state after initial installation of a domain controller. The Dcgpofix tool recreates the two default Group Policy objects and creates the settings based on the operations that are performed only during Dcpromo.

The Dcgpofix tool is intended for use only as a last-resort disaster-recovery tool.

To run Dcgpofix
Type the following at the command prompt: **dcgpofix [/ignoreschema][/target: {domain | dc | both}]**
Where:
/ignoreschema is an optional parameter. If you set this parameter, the Active Directory schema version number is ignored.

You need to back up all of the group policies in a domain.

The solution must minimize the size of the backup.

What should you use?

B. the Group Policy Management console

Applies To: Windows Server 2008 R2

To back up a Group Policy object

In the Group Policy Management Console (GPMC) console tree, open **Group Policy Objects** in the forest and domain containing the Group Policy object (GPO) to back up.
To back up a single GPO, right-click the GPO, and then click **Back Up**. To back up all GPOs in the domain, right-click **Group Policy objects** and click **Back Up All**.
In the **Backup Group Policy object** dialog box, in the **Location** box, enter the path for the location in which you want to store the GPO backups, or click **Browse**, locate the folder in which you want to store the GPO backups, and then click **OK**.
In the **Description** box, type a description for the GPOs that you want to back up, and then click **Back Up**. If you are backing up multiple GPOs, the description will apply to all GPOs you back up.
After the operation completes, click **OK**.

http://technet.microsoft.com/en-us/library/cc770536.aspx

Your network contains an Active Directory domain named contoso.com. The domain contains five domain controllers.

You add a logoff script to an existing Group Policy object (GPO). You need to verify that each domain controller successfully replicates the updated group policy.

Which two objects should you verify on each domain controller?

(Each correct answer presents part of the solution. Choose two.)

A. \\servername\SYSVOL\contoso.com\Policies\{GUID}\gpt.ini
B. \\servername\SYSVOL\contoso.com\Policies\{GUID}\machine\registry.pol
C. the uSNChanged value for the CN={GUID},CN=Policies,CN=System,DC=contoso,DC=com container

D. the versionNumber value for the CN={GUID},CN=Policies,CN=System,DC=contoso,DC=com container

Answer: AD
Section: Configuring Group Policy

Explanation/Reference:
Group Policy has two configurations – the computer and the user configuration. In order to track changes to each configuration, the GPO must track a version number for each configuration. With only one version number, the way two versions are tracked is to split the version number into two numbers.
The top 16 bits of the version number corresponds to the user configuration version. The lower 16 bits of the version number corresponds to the computer configuration version. When looking at the version entry in the gpt.ini file what you are then seeing is:
Version = [user version number top 16 bits] [computer version number lower 16 bits]

This number can be found in the editor and in the gpt.ini file

---

You are an administrator at ABC.com. Company has a network of 5 member servers acting as file servers. It has an Active Directory domain. You have installed a software application on the servers. As soon as the application is installed, one of the member servers shuts down itself. To trace and rectify the problem, you create a Group Policy Object (GPO). You need to change the domain security settings to trace the shutdowns and identify the cause of it. What should you do to perform this task?

A. Link the GPO to the domain and enable System Events option
B. Link the GPO to the domain and enable Audit Object Access option
C. Link the GPO to the Domain Controllers and enable Audit Object Access option
D. Link the GPO to the Domain Controllers and enable Audit Process tracking option
E. Perform all of the above actions

Answer: A

You are an administrator at ABC.com. Company has a network of 5 member servers acting as file servers. It has an Active Directory domain. You have installed a software application on the servers. As soon as the application is installed, one of the member servers shuts down itself. To trace and rectify the problem, you create a Group Policy Object (GPO). You need to change the domain security settings to trace the shutdowns and identify the cause of it. What should you do to perform this task?

A. Link the GPO to the domain and enable System Events option
B. Link the GPO to the domain and enable Audit Object Access option
C. Link the GPO to the Domain Controllers and enable Audit Object Access option
D. Link the GPO to the Domain Controllers and enable Audit Process tracking option
E. Perform all of the above actions

Answer: A
Section: Configuring Group Policy

Use Group Policy to Set Your Application and System Log Security

1. In the Active Directory Sites and Services snap-in or the Active Directory Users and Computers snap-in, right-click the object for which you want to set the policy, and then click **Properties**.
2. Click the **Group Policy** tab.
3. If you must create a new policy, click **New**, and then define the policy's name. Otherwise, go to step 5.
4. Select the policy that you want, and then click **Edit**.

   The Local Group Policy MMC snap-in appears.
5. Expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
6. Double-click **Event log: Application log SDDL**, type the SDDL string that you want for the log security, and then click **OK**.
7. Double-click **Event log: System log SDDL**, type the SDDL string that you want for the log security, and then click **OK**.

Your network contains an Active Directory domain named contoso.com. All domain controllers and member servers run Windows Server 2008. All client computers run Windows 7.
From a client computer, you create an audit policy by using the Advanced Audit Policy Configuration settings in the Default Domain Policy Group Policy object (GPO).
You discover that the audit policy is not applied to the member servers. The audit policy is applied to the client computers.
You need to ensure that the audit policy is applied to all member servers and all client computers.

What should you do?

A. Add a WMI filter to the Default Domain Policy GPO
B. Modify the security settings of the Default Domain Policy GPO
C. Configure a startup script that runs auditpol.exe on the member servers.
D. Configure a startup script that runs auditpol.exe on the domain controllers.

Answer: B
Section: Configuring Group Policy

Your network contains an Active Directory domain.

You need to back up all of the Group Policy objects (GPOs) Group Policy permissions, and Group Policy links for the domain.

What should you do?

A. From Windows PowerShell, run the Backup-GPO cmdlet.
B. From Windows Server Backup, perform a system state backup
C. From Windows Explorer, copy the content of the %systemroot%\SYSVOL folder.
D. From Group Policy Management Console (GPMC), back up the GPOs

Answer: A
Section: Configuring Group Policy

Your network contains a single Active Directory domain. Client computers run either Windows XP Service Pack 3 (SPP·) or Windows 7. All of the computer accounts for the client computers are located in an organizational unit (OU) named OU1.

You link a new Group Policy object (GPO) named GPO10 to OU1.

You need to ensure that GPO10 is applied only to client computers that run Windows 7.

What should you do?

A. Enable block inheritance on OU1.
B. Create a new OU in OU1. Move the Windows Xp computer accounts to the new OU
C. Modify the permissions of OU1.
D. Create a WMI filter and assign the filter to GPO10

Answer: D
Section: Configuring Group Policy

Explanation/Reference:
Creating WMI and Group Filters

Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista

When the network includes client computers that run a variety of Windows operating systems, two computers in the same OU might require different settings to achieve the same configuration. For example, a computer that is running Windows XP might require a different setting than a computer that is running Windows 7 or Windows Vista. Two GPOs would be required in that case, one to apply to computers that are running Windows XP, and one to apply to computers that are running the later versions of Windows.

There are also times when you cannot rearrange the computers in your AD OU hierarchy to let you link a GPO to OUs that contain only the computers to which you want the GPO to apply. So Group Policy also supports using access control lists (ACLs) to prevent the GPO from applying to any computer or user account that is not granted permissions to the GPO.

There are two frequently used techniques used to make sure that GPOs only apply to the correct computers:

- ***Add a Windows Management Instrumentation (WMI) filter to the GPO***. A WMI filter enables you to specify criteria that must be matched before the linked GPO is applied to a computer. By letting you filter the computers to which the GPO applies, this reduces the need to further subdivide your OUs in Active Directory. This technique is dynamic, in that the filter is evaluated when the computer attempts to apply the policy. So if you are filtering based on the version of Windows then upgrading the computer from Windows XP to Windows 7 requires no changes to your GPO, because the filter will automatically recognize the change and filter the computer's access to the GPO accordingly.

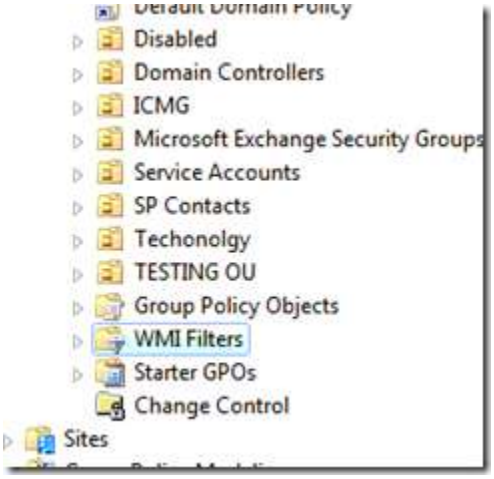
- Grant or deny the **Apply Policy** security permission in the ACL for the GPO. If you put your computers in security groups, you can then grant the **Apply Policy** permission to only the groups that should use the GPO.

http://technet.microsoft.com/en-us/library/cc754488(v=WS.10).aspx

---

WMI filter

We go out to our Domain Controller and Open Group Policy Management Console and select WMI Filters:



The right hand side content area should be blank…

If you r familiar with SQL then this should be really straight forward for ya…

- Your basically running WMI query but the format is just like a SQL query

“Select * from Win32_OperatingSystem where Caption = "Microsoft Windows 7 Enterprise " OR Caption = "Microsoft Windows 7 Professional "”

Click Ok

Your company has a single Active Directory forest with a single domain. Consultants in different departments of the company require access to different network resources. The consultants belong to a global group named TempWorkers. Three file servers are placed in a new organizational unit named SecureServers. The file servers contain confidential data in shared folders. You need to prevent the consultants from accessing the confidential data.

What should you do?

A. Create a new Group Policy Object (GPO) and link it to the SecureServers organizational unit. Assign the Deny access to this computer from the network user right to the TempWorkers global group.
B. Create a new Group Policy Object (GPO) and link it to the domain. Assign the Deny access to this computer from the network user right to the TempWorkers global group.
C. On the three file servers, create a share on the root of each hard disk. Configure the Deny Full control permission for the TempWorkers global group on the share.
D. Create a new Group Policy Object (GPO) and link it to the domain. Assign the Deny log on locally user right to the TempWorkers global group.
E. Create a new Group Policy Object (GPO) and link it to the SecureServers organizational unit. Assign the Deny log on locally user right to the TempWorkers global group.

Answer: A
Section: Cooper Exam D

Explanation/Reference:
You would want to do this at the OU level using a GPO rather than at the domain level.

Your network contains an Active Directory forest named adatum.com.
All client computers used by the marketing department are in an organizational unit (OU) named Marketing Computers. All user accounts for the marketing department are in an OU named Marketing Users.

You purchase a new application.

You need to ensure that every user in the domain who logs on to a marketing department computer can use the application. The application must only be available from the marketing department computers.

What should you do?

B. Create and link a Group Policy object (GPO) to the Marketing Computers OU. Copy the installation package to a shared folder on the network. Assign the application.

Explanation: Has to be done with a GPO assigned to the Marketing Computers. The GPO must point to a shared location where the users/computers have permissions.

These are some powerful policy settings that allow you to configure five settings for **Application**, **Security**, **Setup**, and **System** event logs. These categories and their policy settings are located under **Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service**.

The **Log File Path** policy setting, when enabled, allows you to provide a specific location where the Event Log service writes its log file. You must provided path and filename when relocating where Windows writes the log file.

Next is the **Maximum Log file size** policy. When enabled, this policy allows you to specify the maximum size of the event log. It supports sizes between one megabyte and two terabytes and uses one-kilobyte increments.

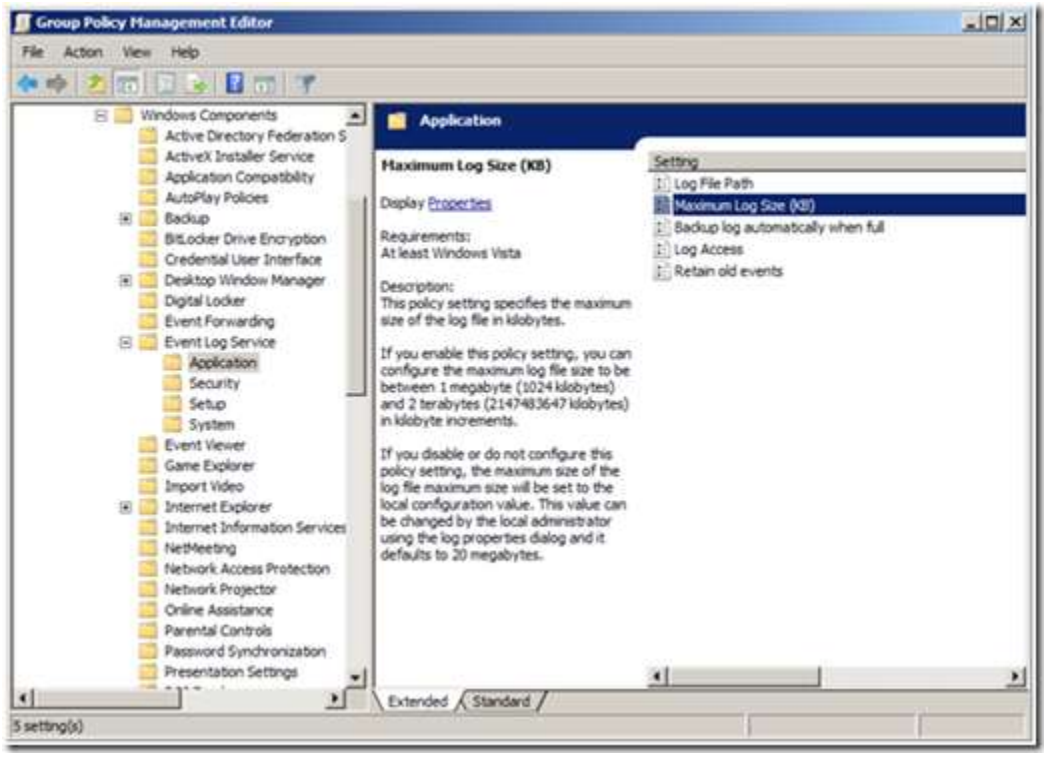


Figure 1 Event Log Service Policy Settings

The next two policy settings are related. The Event Logging service uses the **Retain old events** and **Backup log automatically when full** policy settings when the event log reaches the maximum file size (defaults to 20 MB or the value specified in the **Maximum Log size** policy setting). With the **Retain Old Events policy** setting enabled, the Event Logging service stops writing new events to the event log when the log file reaches or exceeds the maximum value and you lose all new events. With this policy setting disabled, new events overwrite old events. When you enabling the **Backup log automatically when full** and the **Retain old events** policy settings, the Event Log service closes the current event log, renames it, and then creates a new log. The **Backup log automatically when full** policy setting *works* only when you enable **Retain old events** policy setting.

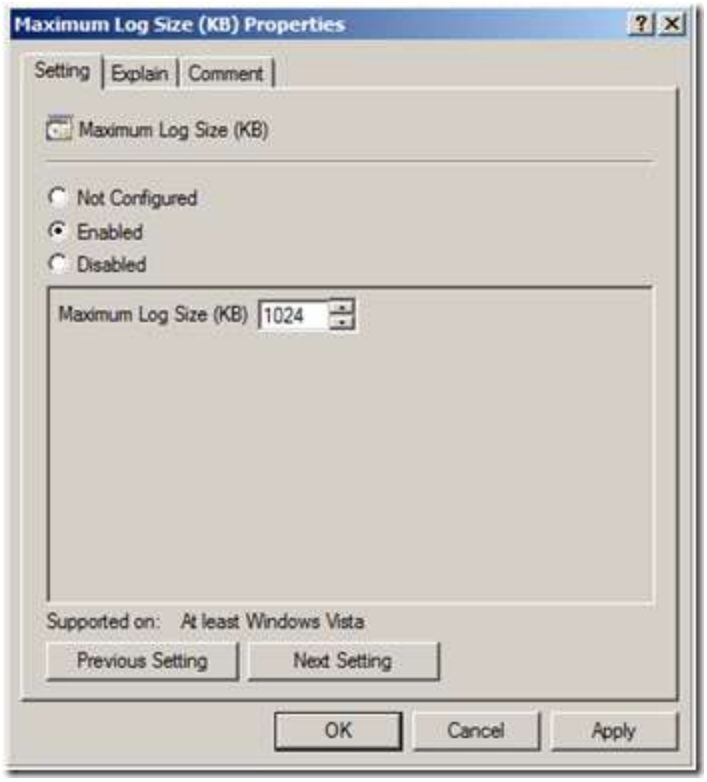
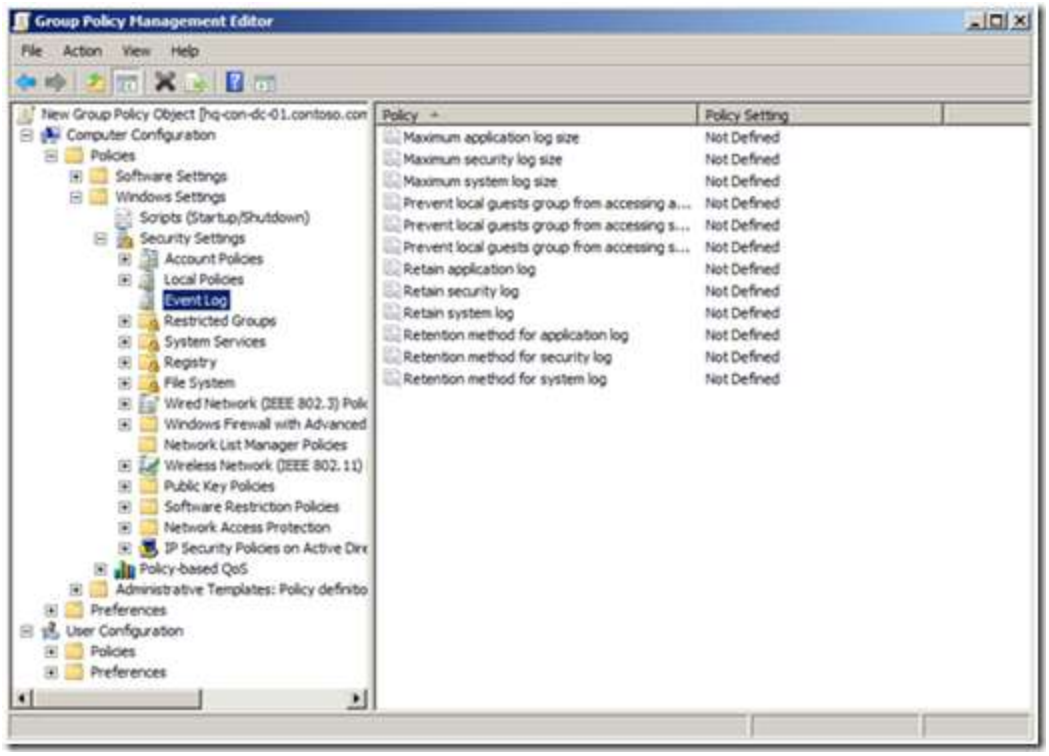


Figure 2 Maximum Log Size Policy Setting

The last setting and one that I think is the most beneficial is the **Log Access** setting. Enabling this setting allows you to enter a security descriptor for the log file. The security descriptor controls who can read, write, or clear the event log. You enter the security descriptor using Security Definition Description Language (SDDL), which is document on MSDN(http://msdn.microsoft.com/library/en-us/secauthz/security/security_descriptor_string_format.asp). Also, my esteemed colleague Jim provides a two-part blog series about SDDL (http://blogs.technet.com/askds/archive/2008/04/18/the-security-descriptor-definition-language-of-love-part-1.aspx and http://blogs.technet.com/askds/archive/2008/05/07/the-security-descriptor-definition-language-of-love-part-2.aspx).

Finally, I should mention that these new policy settings have precedence over the older Windows Server 2003 and Windows XP security policy setting that manage Event Logs. Both settings can exist in the same Group Policy object and apply only to the respective operating systems for the policy setting.



These new policy settings for the Event Logging service provide more flexibility and control from earlier versions. Using Group Policy to control where event logs are written, how large they can grow, how they are preserved, and who can manage them are key to change control and security auditing. You can implement these policy settings in your existing Group Policy objects and they will not affect operating systems earlier than Windows Vista.