**Types of events to Audit**

|  |  |
| --- | --- |
| **Event** | **Example** |
| Account Logon | An account is authenticated by a security database. When a user logs on to the local computer, the computer records the Account Logon event. When a user logs on to a domain, the authenticating domain controller records the Account Logon event. |
| Account Management | An administrator creates, changes, or deletes a user account or group; a user account is renamed, disabled, or enabled; or a password is set or changed. |
| Directory Service Access* Directory Service Changes
* Directory Service Replication
* Detailed Directory Service Replication
 | A user accesses an Active Directory object. To log this type of access, you must configure specific Active Directory objects for auditing.The subcategories are new to Windows Server 2008. If you enable Directory Service Access, you enable all of the subcategories. Note that you still need to modify the system access control list (SACL) on the specific objects for auditing to take place.You can also modify individual subcategories using the Auditpol command-line utility:Example: **auditpol /set /subcategory:"directory service changes" /success:enable** |
| Logon | A user logs on or off a local computer, or a user makes or cancels a network connection to the computer. The event is recorded on the computer that the user accesses, regardless of whether a local or domain account is used. |
| Object Access | A user accesses a file, folder, or printer. The administrator must configure specific files, folders, or printers to be audited, the users or groups that are being audited, and the actions for which they will be audited. |
| Policy Change | A change is made to the user security options (for example, password options or account-logon settings), user rights, or audit policies. |
| Privilege Use | A user exercises a user right, such as changing the system time (this does not include rights that are related to logging on and off) or taking ownership of a file. |
| Process Tracking | An application performs an action. This information typically is useful only for programmers who want to track details about application execution. |
| System | A user restarts or shuts down the computer, or an event occurs that affects Windows Server 2003 security or the security log. |

**References**

* Windows Server 2008 Auditing AD DS Changes Step-by-Step Guide
<http://go.microsoft.com/fwlink/?LinkID=112104&clcid=0x409>