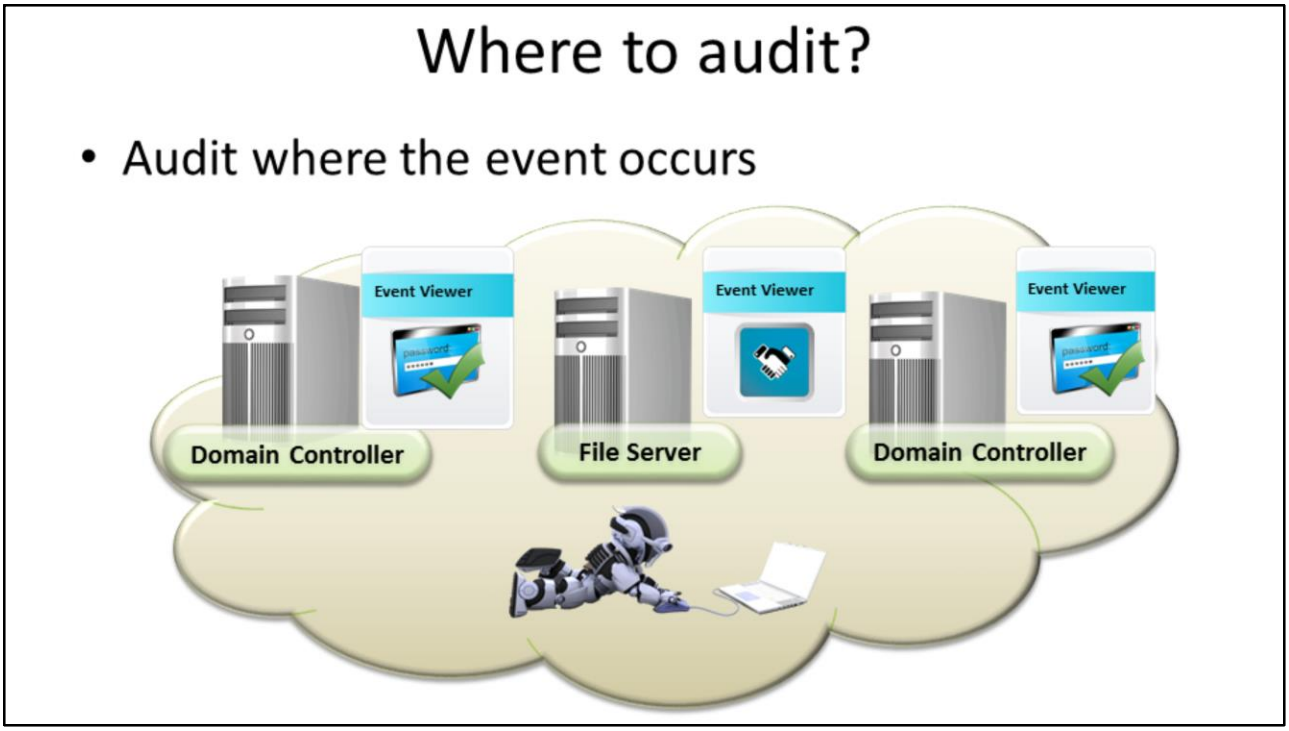
Active Directory Auditing

For the free video please see
http://itfreetraining.com/certificate/active-directory-auditing

This video will look at the concepts you need to understand in order to use Auditing in Windows. Once you understand the concepts of Auditing, the next two videos will look at Auditing for the file system and objects in Active Directory.



Where to audit?

- Audit where the event occurs

Where to audit?
Before you start setting up your network for auditing, it is important to locate the best place to audit. For example, if a user accesses the network via a VPN and the VPN server is a read only Domain Controller, the logon event will be stored in the read only Domain Controllers event log. Likewise, if the user accesses a file server, a logon event will not be stored on the file server, however an event will be stored on the file server indicating that a connection was made to that file server. So when auditing the network it is important to understand that you are auditing the correct locations to get the right information. You may also need to audit multiple servers in order to obtain the information that you are after.

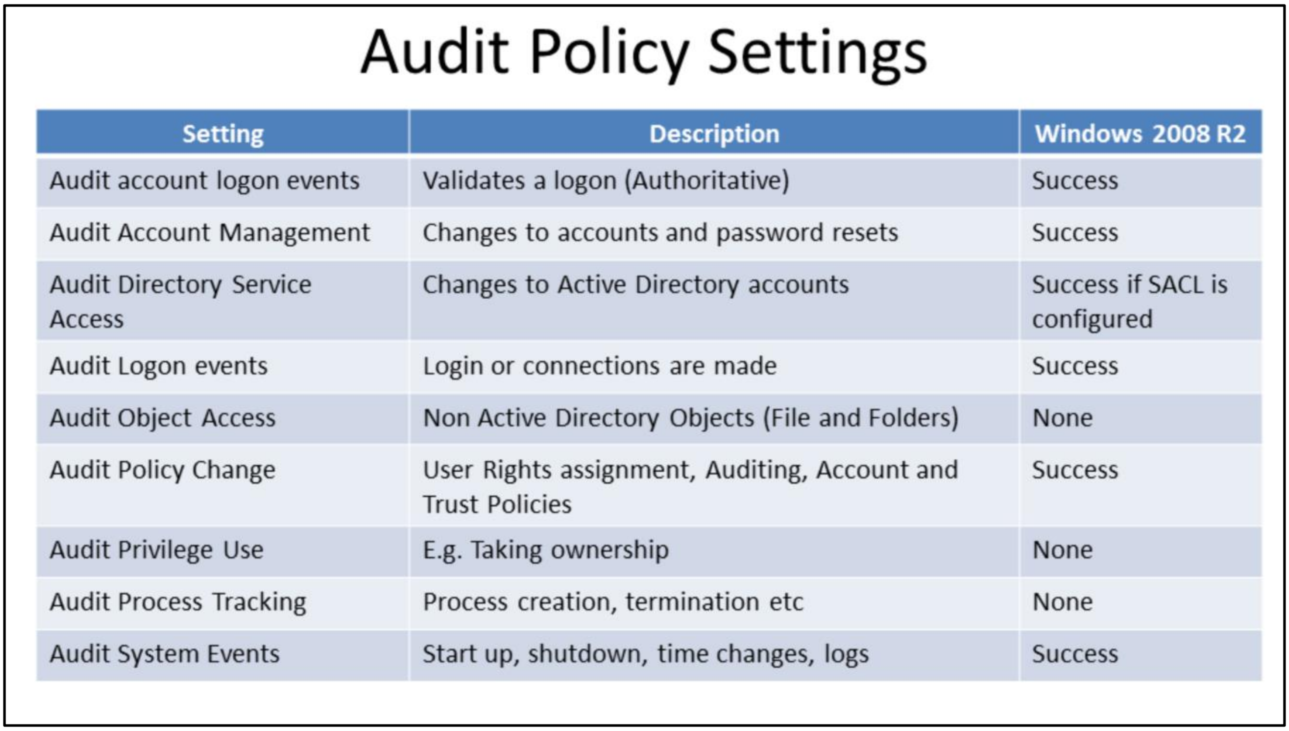
Demonstration

Demonstration

There are 7 auditing settings in Group Policy found under the following location.

Computer Configuration\Polices\Windows Settings/Local Polices\Audit Policy

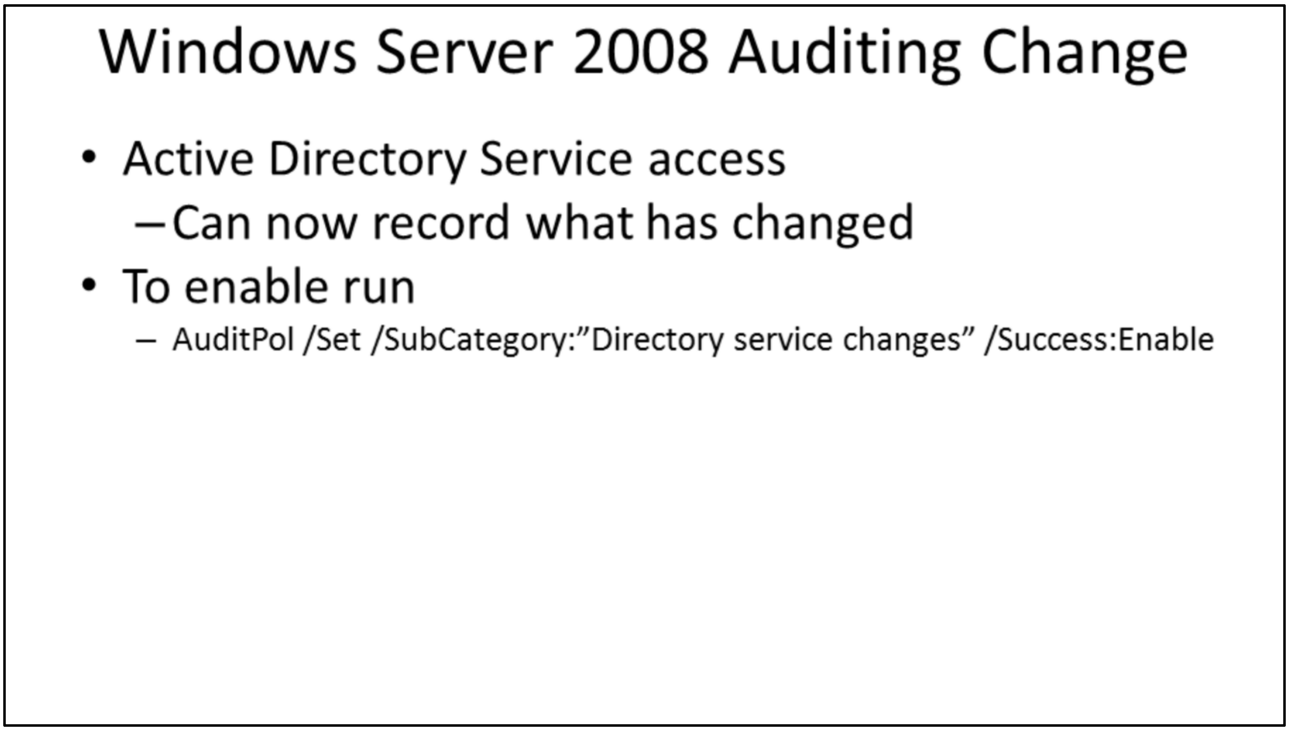
To configure a setting, it is just a matter of opening the setting, ticking “Define these policy settings” enabling it and then selecting which settings you want to audit, that is success and failure.



Audit Policy Settings

Setting	Description	Windows 2008 R2
Audit account logon events	Validates a logon (Authoritative)	Success
Audit Account Management	Changes to accounts and password resets	Success
Audit Directory Service Access	Changes to Active Directory accounts	Success if SACL is configured
Audit Logon events	Login or connections are made	Success
Audit Object Access	Non Active Directory Objects (File and Folders)	None
Audit Policy Change	User Rights assignment, Auditing, Account and Trust Policies	Success
Audit Privilege Use	E.g. Taking ownership	None
Audit Process Tracking	Process creation, termination etc	None
Audit System Events	Start up, shutdown, time changes, logs	Success

Audit Policy Settings
By default, some auditing settings are configured to audit success events and thus you will have some audit events in the event log even if you do not configure auditing.
Audit account logon events: Audits an event when authentication occurs. For a domain account, this will happen on a Domain Controller. For a local account, this will happen on the computer that the local account is stored on.
Audit Account Management: Auditing when a user performs account management using tools like Active Directory Users and Computers to perform actions like resetting passwords.
Audit Directory Service Audit: Audit any changes to Active Directory Accounts. Includes changes not made with management tools.
Audit Logon Events: This records when a user connects or disconnects from a server. For example, when connecting a map drive to a file server the user needs to logon to the server before the file share can be accessed. This event also records access being denied due to the account being locked. In contrast to Audit Account Logon Event, an event is only recorded when the user is authenticated.
Audit Object Access: This will audit non Active Directory objects, this includes file and folders.
Audit Policy Change: Audits changes to settings like user rights assignment, auditing and trust polices. For example, if you changed a setting and gave a user the” take ownership” right, this setting would record the user rights assignment change in the event log.
Audit Privilege Use: This setting records when privileges are used. An example of a privileges is changing the system time.
Audit Process Tracking: This setting tracks the start and termination of processes in Windows. This setting generates a lot of events so should only be enabled in special circumstances.
Audit System Events: This records events like system start up, shutdown and changes to the system time.



Windows Server 2008 Auditing Change

- Active Directory Service access
  - Can now record what has changed
- To enable run
  - AuditPol /Set /SubCategory:”Directory service changes” /Success:Enable

Windows Server 2008 Auditing Change
Before Windows Server 2008, auditing could only track that a value has changed. It would not tell you what the value was before the change. Windows Server 2008 allows the value of an object before the change to be recorded in the event viewer. This means you can effectively know the value was changed and what the value was before the change.
Due to compatibility reasons the option is not enabled by default, in order to enable it run the following command.

```
auditpol /set /subcategory:”Directory service changes” /success:enable
```

Demonstration
Before auditing can occur in Windows Server 2008 to record changes to Active Directory objects, the following command needs to run. This only needs to be run once for all Windows Server 2008 installs as it makes a change in Active Directory.

```
auditpol /set /subcategory:”Directory service changes” /success:enable
```

When an object is changed, different events are recorded so it is important to find all the events that are related to changes.
For example, when changing an object, this will often log an event for deleting the previous value and then adding a new value. When trying to understand what has been changed, look at a few events around the event that you are interested in case there are multiple events generated for that value change.

References
“MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition” pg 367-375
“Access Control Lists (Windows)” http://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx
“AD DS Auditing Step-by-Step Guide” http://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx