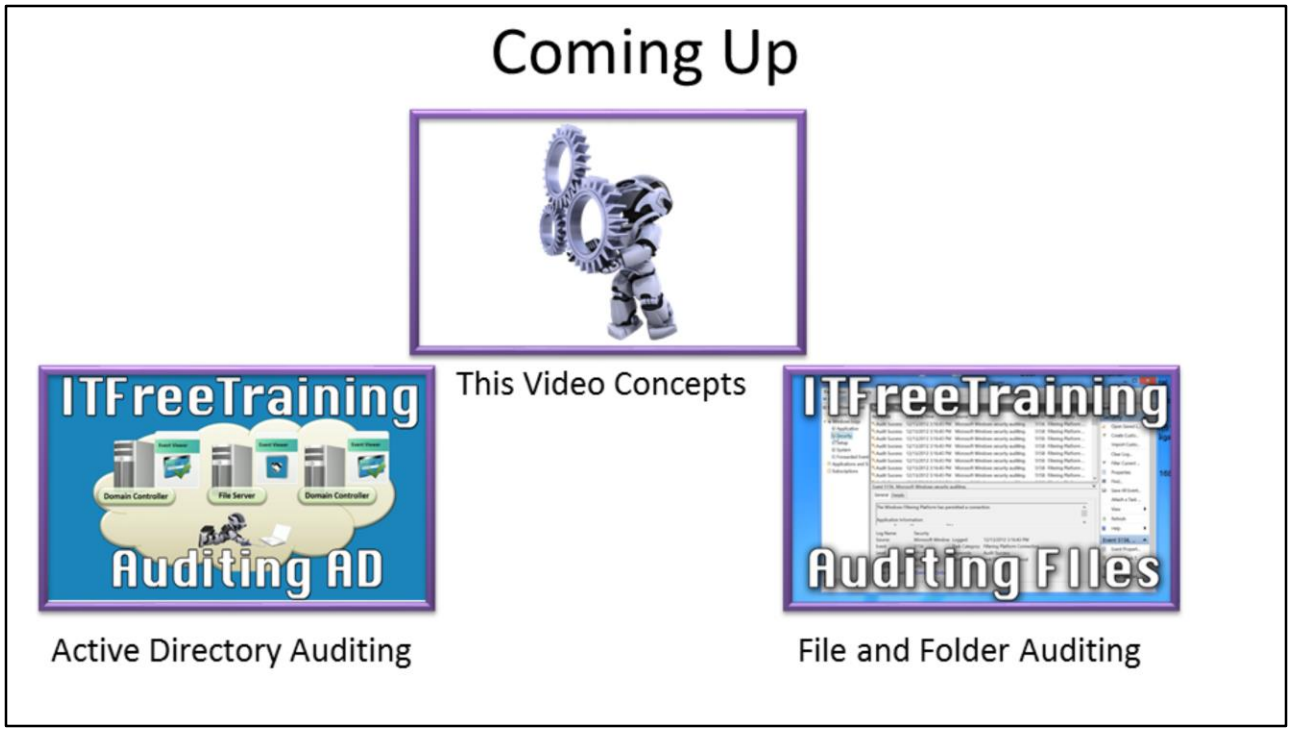
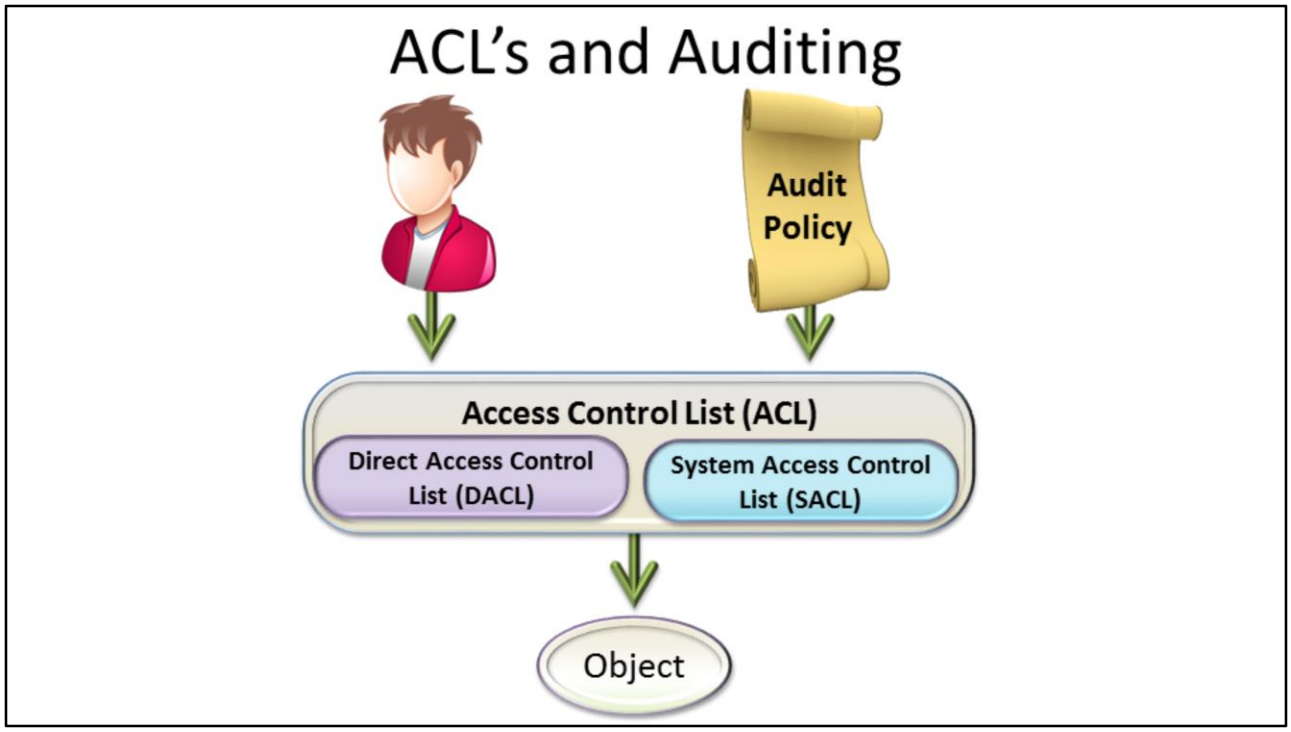
Windows Auditing

For the free video please see
http://itfreetraining.com/70-640/windows-auditing

Windows has a comprehensive auditing feature allowing you to track files and object access. In this video and the next 2 videos, auditing is looked at for Active Directory and file and folders access.

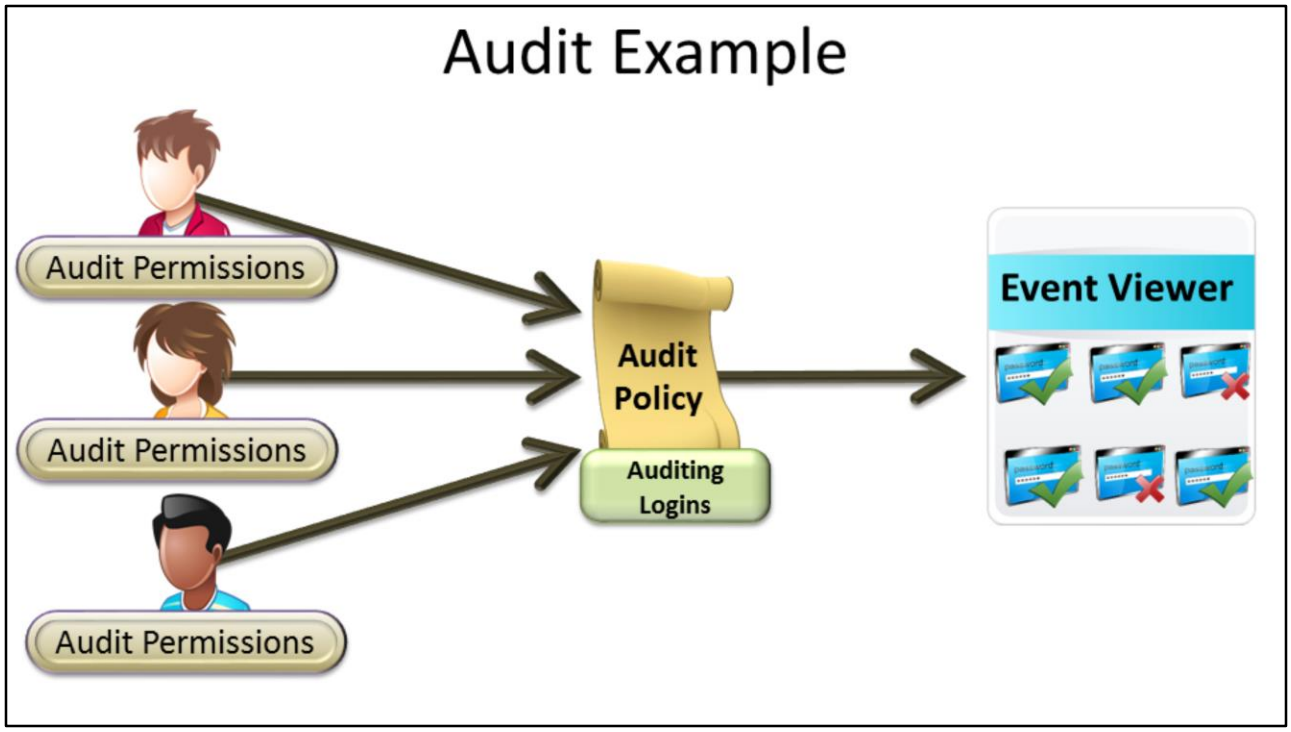


Coming Up
This video: Auditing concepts
Next video: Active Directory Auditing
Video after this: File and Folder Auditing



ACL's and Auditing

An Access Control List or ACL defines the permissions of an object in Windows. The ACL is divided into two parts. These are the Direct Access Control List (DACL) and System Access Control List (SACL). The DACL is used for permissions like read and write. The SACL is used for auditing permissions like success and failure. Since two systems are used for permissions and auditing, this requires two sets of ACLS. This means that an object can be audited by the auditing system even though there may not be any read permissions defined for that object.



Audit Example

The SACL on an object will determine if this object is audited. However, if the results are recorded in the event viewer, this will be determined by the audit policy. If the audit policy is configured to record events of that audit type, these events will be recorded in the event viewer. Thus, in order for auditing to work, the SACL must be configured to audit events for that object and also the Audit Policy must be configured to allow auditing to occur. By having a system like this, it allows an administrator to quickly change what is audited without having to change the permissions of objects. As auditing puts more load on the system, many administrators will only use auditing when required.

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