Microsoft made incremental changes to security auditing in Windows Server 2012. These enhancements include the ability to audit removable drive usage, to create expression-based audit policies, and to retrieve more detailed and meaningful audit log entries.

Contents of this article

Depending upon your industry, security auditing may be one of those “nice to have, but I’ll get around to it someday” things, or it may simply be mandated by law and therefore require your compliance.

To this latter point, we’ve had the ability to audit events in Windows Server for several years now. For instance, the workflow for auditing file system access events in Windows Server 2008 R2 looks like this:

- Specify your auditing scope in a Group Policy Object (GPO)
- Mark selected file system resources for auditing
- Review security audit entries in the Windows event logs

Windows 7 and Windows Server 2008 R2 introduced Global Object Access Auditing, which made it leagues easier to audit multiple file system and/or Registry resources for audit tracking on a per-computer basis.

Windows Server 2008 R2 also gave us Advanced Security Audit Policy, which greatly broadens and deepens the types of audit policy we can create.

Windows Server 2012 doesn’t give us any ground-breaking new features like we saw in Windows Server 2008. Instead, we find that Microsoft tweaked existing functionality to give us administrators even more flexibility with our in-box auditing policy.

Of course, large enterprises should be concerned with setting audit policy by using Group Policy. Instead, these shops should take a look at Microsoft System Center 2012 Audit Collection Services.

In this blog post I want to walk you through the security auditing enhancements in Windows Server 2012; in a nutshell, these improvements are as follows:

- We can now audit removable devices
- We can now create expression-based audit polices
- We can reduce audit volume and glean additional data from audit events

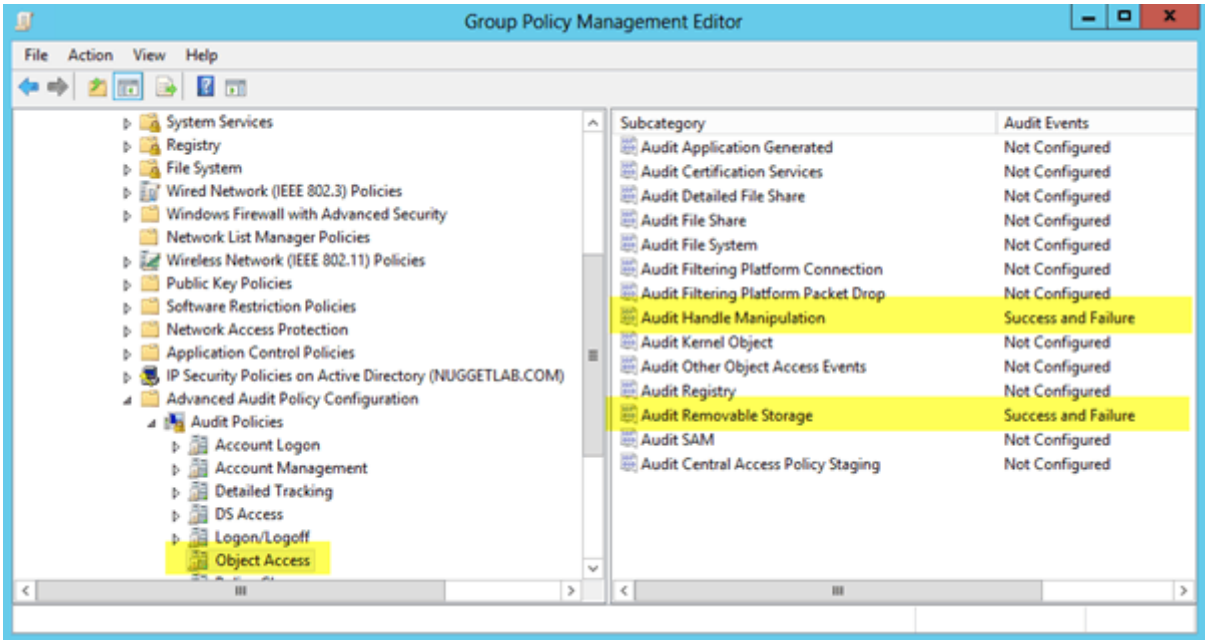
Let's take a look at each of those enhancements in turn.

Auditing removable drives

Removable storage, such as USB flash drives or external hard drives, can represent a very real security risk for an enterprise. For instance, how can we prevent a disgruntled employee from transferring sensitive data to his or her USB thumb drive?

To be sure, we had Removable Storage Access Policy in Windows Server 2008 R2 to deny usage of removable devices. However, in 2008 we had no way to track attempts to use removable drives.

As you can see in Figure 1, we have audit policies that target and track removable drive access attempts.**Failure** audits generate Event 4656, and **Success** audits generate Event 4663.



Auditing removable device access

The two policies in question are **Audit Removable Storage** and **Audit Handle Manipulation**; these are located in the Group Policy path **Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Object Access.**

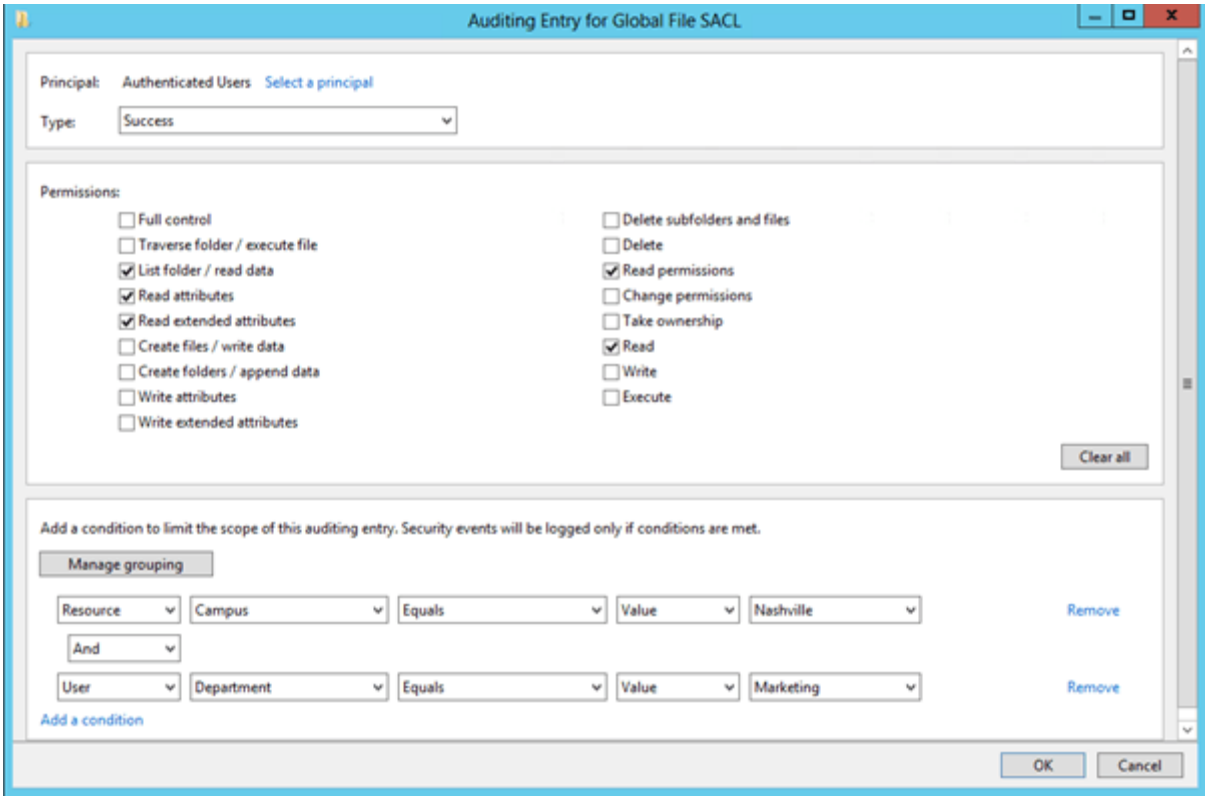
Using expression-based audit policies

Dynamic Access Control (DAC) is a new feature in Windows Server 2012 that enables us administrators to granularly control access to filter server resources by using expression-based logic.

For instance, we can share out a folder that grants access to marketing department employees located in the Los Angeles office for files that are marked as high-priority. This security access method is powerful, flexible, and makes it easier to manage hundreds or thousands of shared folders.

We can also apply conditional logic to our Global Object Access Auditing policy. Create a GPO, navigate to**Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Global Object Access Auditing**, and double-click the **File system** policy. Enable the policy and click **Configure**.

As you can see in Figure 2, the **Advanced Security Settings for Global File SACL** dialog box allows us to define audit entries that embrace claims and resource properties.



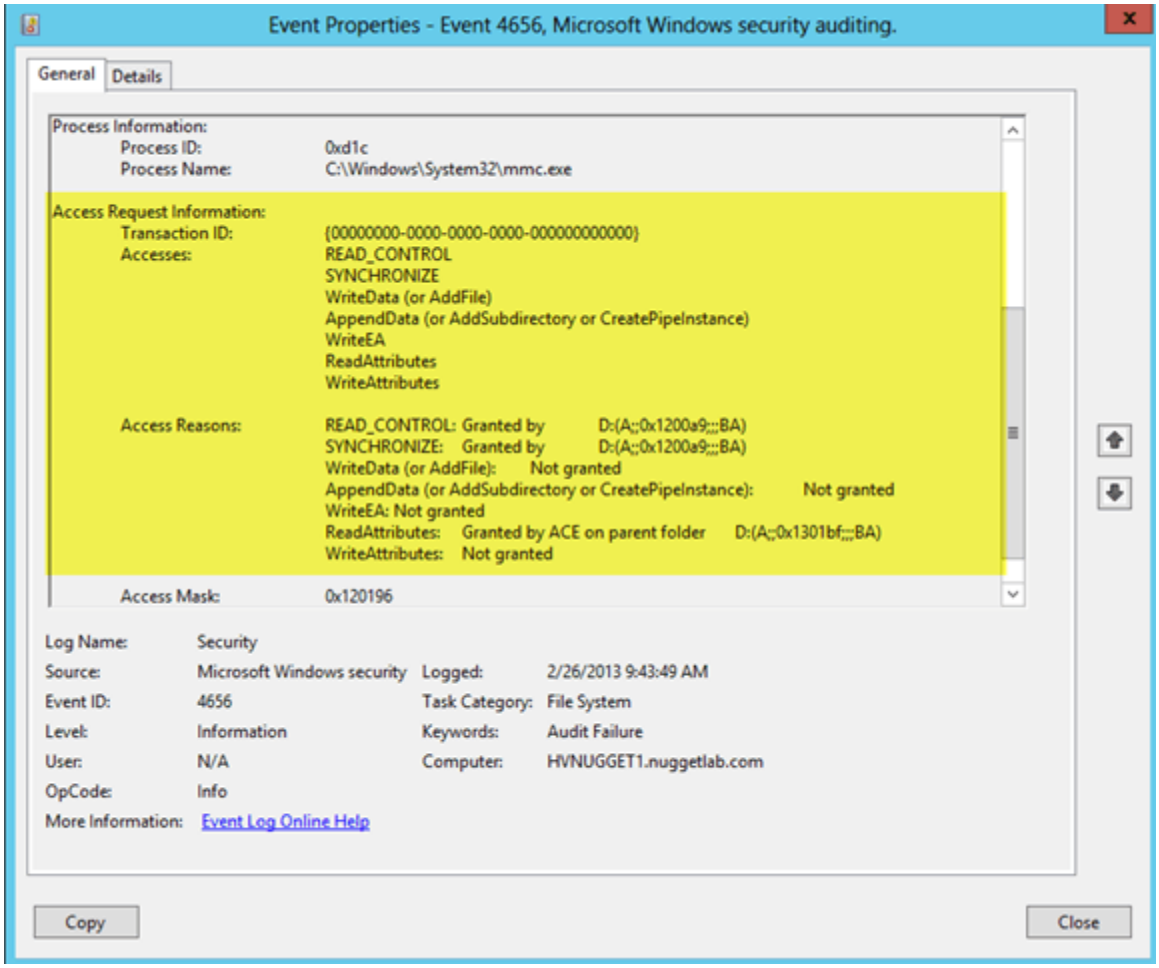
Expression-based audit policy

In the previous screenshot, we monitor successful reads by authenticated users who work from the Marketing department in the Nashville office. That's pretty powerful, isn't it? These expression-based polices give us much more targeted audit log feedback.

Reviewing detailed audit log data

You already know that Windows writes Success and Failure audit events to the Windows Security log. In Windows Server 2012 we still have the trusty Event Viewer tool with which we can review our log entries.

However, Windows Server 2012 gives us more information in logon and object access events. For instance, check out Figure 3. Observe that the audit log entry now provides reasons for access in addition to detailed file attribute data. For my money, this is a very valuable addition to Windows Server 2012.



Detailed audit entry data

Specifically, be on the lookout for the following audit entries if you've configured advanced audit policy in Windows Server 2012:

- File Access Event 4656
- File Access Event 4663
- User Logon Event 4624
- User Logon Event 4626