

Re: File Access Auditing on Exchange 2003 Server

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-06/0380.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 06/28/05

Date: Tue, 28 Jun 2005 09:26:31 -0500

Auditing of object access can make a huge amount of entries in the security log even when you have not enabled auditing on any folders yet. One thing to check is that in Local Security Policy [secpol.msc], or whatever appropriate security policy, that the security option for audit:audit the access of global system objects is disabled. I can tell you right now that keeping track of read activities will generate a huge amount of events. When you do audit a folder it is best to audit absolute minimum number of permissions for absolute minimum number of users/groups and avoid auditing for everyone, users, authenticated user groups but instead use a global/local group of just the users you want to track. The free MS tool Event Comb can help in tracking object access events and it can search by text string such as for filename or user name. The link below may help. --- Steve

<http://www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.aspx>

"Jimmy" <Jimmy@discussions.microsoft.com> wrote in message
news:9F05E958-9BFE-40E7-939F-F2A4BAB5BD89@microsoft.com...

> *Our company has an Exchange 2003 SP1 server runs on Windows 2003 Std. It*
> *will*
> *update to SP1 in a few weeks. The server also does file sharing for all*
> *our*
> *40+ users.*
>
> *We want to enable auditing to keep track of read/write activities on the*
> *file shares. I did attempt turn on Success/Failure of Object Access in*
> *Local*
> *Security Policy. I didn't turn on auditing on any File System yet. Then I*
> *discovered a lot of Exchange object access (ID 562) were tracked in*
> *security*
> *log. Size increase is more than 6MB for merely an hour. That makes*
> *auditing*
> *impractical to implement.*
>
> *Did I do anything wrong on the setup or this is a necessary evil of*
> *auditing*
> *on E2K3?*
>
> *Jimmy*

microsoft.public.windows.server.security: Re: File Access Auditing on Exchange 2003 Server

>