

Auditing User logon and logoff, from the event logs on the domain controllers

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-04/0925.html

From: Paul (*pwilkins_at_utk.edu*)

Date: 04/08/04

Date: 8 Apr 2004 11:48:57 -0700

I'm trying to build statistics on computer lab usage based on the log on, log off events registered on AD domain controllers.

On individual machines it's pretty easy to determine what's a logon and what's a logoff. Logon is event id 528, type 2 and logoff is 538 type 3. Getting that same info from the DC's appears more complicated. 528 applies to only local logons, so can't use that. I've found that anyone logging on always generates an event id 673, or kerberos ticket granted. But what about logoffs? Logging off generates 538's, but the problem is that I see a bunch a 538's when a users logs in too. Is there a way to accurately figure out when someone logs off?