Efficiently exploit printers in Windows Server 2003 (Part 3)

In the previous article of this series, I have shown you the most effective way to manage a network printer is to create print queues on one of the network servers and force all print jobs to be Go through that queue. In the second part of this series, we introduced some basic techniques for this

Efficiently exploit printers in Windows Server 2003 (Part 1)
Efficiently exploit printers in Windows Server 2003 (Part 2)

In the previous article of this series, I have shown you the most effective way to manage a network printer is to create print queues on one of the network servers and force all print jobs to be Go through that queue. In the second part of this series, we have introduced some basic techniques for print string protection that you created in Part 1. In this article, I will show you how to verify the use of a network printer.

Why check the printing on the network?

There are several possible reasons why it is necessary to authenticate using a network printer. As we explained in the first part of this series, evaluating printers is a must for your company to test them. You must know who is printing and whether the person is entitled to printing.

A simple example of verification involves managing printer supplies such as ink and paper. We have studied in many companies, where printers are tested so that separate rooms are responsible for providing what they use. Since then, there have been cases in which high-density photo printers are validated for unauthorized use because the supplies are very expensive.

Verify a network printer

We talked a little bit about why to authenticate the network printer, now let's move on to the process of verifying it. If you have ever looked at the server's security logs, you may notice that the printer authentication cannot be performed by default. To enable printer authentication, select the Printers and Faxes command from Start. After you are done, you will see the Printers and Faxes window. Right-click the printer you want to verify, select the Properties command from the right-click menu. The printer properties sheet will appear after you execute the command.

In this section, you must select the Security tab and then click the Advanced button. When you do, Windows will display the properties page of the Advanced Security Settings. Select the Auditing tab, you will see that it is completely empty as shown in Figure A.

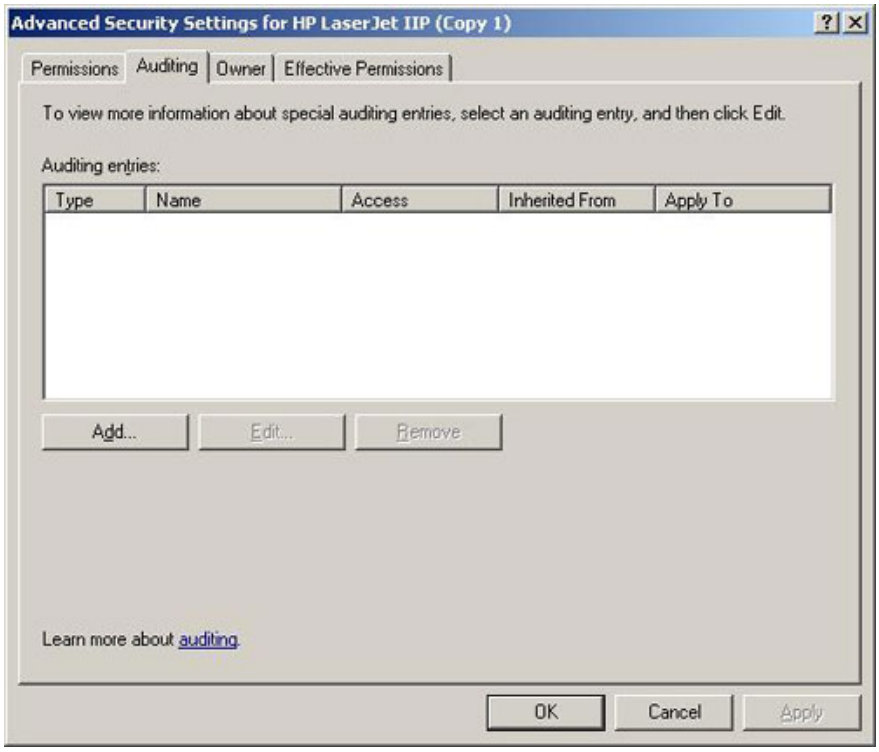

Figure A: Printer authentication is disabled by default

How to set up the printer authentication, the authentication focuses on users and groups rather than focusing on the printer itself. That means you can't ask Windows to create an audit log input any time someone sends a print job to the printer (at least not directly). Instead, Windows will ask for the name of the user or group you want to authenticate. If your purpose is to verify any use of the printer, you can verify the Everyone group.

Keep in mind, click the Add button, you will see a screen asking you to enter the name of the user and the group you want to authenticate, as shown in Figure B. After entering the name of the user and group, we We recommend clicking on the Check Names button. Doing so will ensure that you spell the appropriate names and that the name is valid, the authentication will not perform if you are authenticating a user or group does not exist.

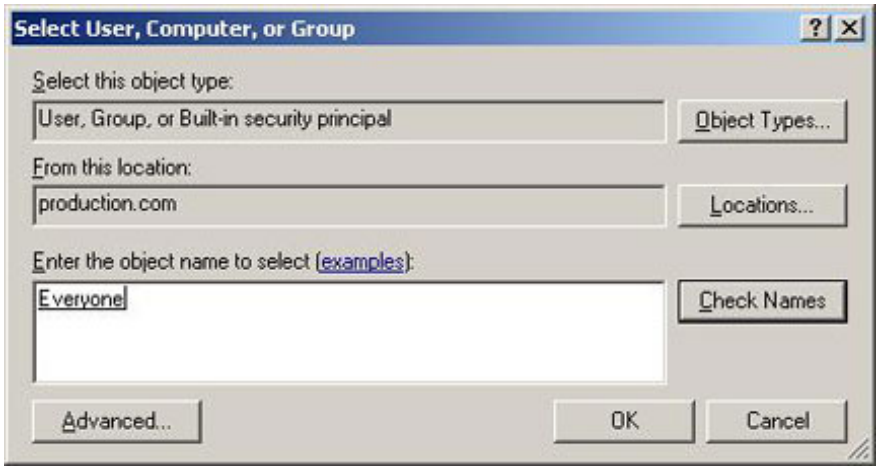

Figure B: Windows requires entering the user name and the groups you want to authenticate

Click OK and you will see an Auditing Entry dialog box, as shown in Figure C. As you can see in the figure, this dialog box allows you to verify both the success and failure of the various printer-related events. To enable authentication, all you need to do is select the events you want to audit and click OK. Before doing that, you have to understand the meaning of these different events.

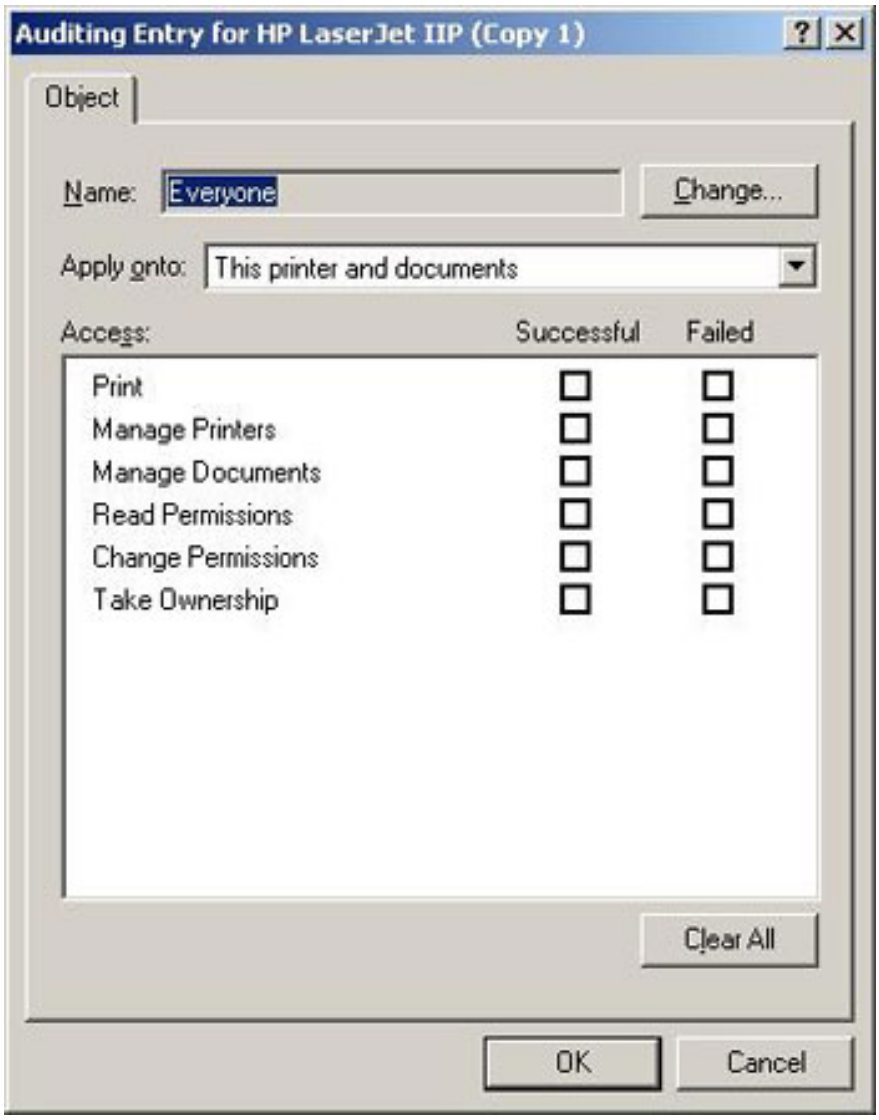

Figure C: The dialog box allows you to control the events you want to audit

In the section below, we will describe what the event you can assess means. As I have done, you should remember that my descriptions acknowledge that you are appraising the success of a particular event. Verifying the failure of events means simply that someone attempting to perform the action will result in a normal event if the user has valid permissions. For example, performing a successful audit on the Print event will create a security log each time someone performs print jobs on the printer. A failure of such an event will create a record any time someone tries to print on the printer, but cannot because they lack the necessary permissions. Remember those things, here are the different facts and their meanings:

• *Print* - The currently *authenticated* user has sent a print command to the printer

• *Manage Printers* - Users change the properties or permissions of the printer

• *Manage Documents* - Users have stopped, restarted, restarted or deleted a print job.

• *Read Permissions* - User reads the printer's security permissions

• *Change Permissions* - Users change the security permissions of the printer

• *Take Ownership* - Users gain ownership of the printer

What must you evaluate?

With all the authentication settings available, you might be wondering what to evaluate. That really depends on the nature of the printer and how secure you need it. If the printer is used for printing checks, you should perform both success and failure assessments for each event. On the other hand, if the printer is a common-use general-purpose printer, you do not have to perform the above successful authentication for the Print event. If you have done so, the event log will increase in size quickly and cannot be managed because the new record will be created each time someone sends a print job to the printer.

I think the vast majority of printers in the average organization may not need to be verified. However, if a printer is used for a variety of financial purposes (such as print checks), or consumes expensive supplies, you may need to verify this printer. In many situations, we recommend that you verify the two success and failure events related to Manage Printer and Change Permission. We also recommend using the Print event validation failure.

Conclude

In this article, we have shown you that it is easy to miss printers when developing network security plans because printers are so often so trivial that they are rarely secured. The phenomenon of bypassing the printer can cause financial waste for the company. Therefore, we recommend configuring sensitive printers using a centralized print queue managed by a Windows server. After all, you can easily perform security for the printer and verify its use or those trying to use it (unauthorized).