Security Pro VIP

May 2007

Contents:

Enterprise Event Logging for SMBs

These 6 tools solve your tough log collection and management needs

By John Howie

In recent articles, I described various tools you can use to ease the pain of event log collection and management (see the *Windows IT Pro* Web-exclusive article "Collecting and Analyzing Event and System Logs," March 28, 2006, InstantDoc ID 49492, and the *Windows IT Security* article "Security Log Collection," November 2006, InstantDoc ID 93330). Small-to-midsized businesses (SMBs) have many free or inexpensive tools to choose from. However, SMBs with sophisticated needs might want to consider a log collection and management suite from one of the many vendors that provide tools designed for enterprises. Here are some enterprise-class tools you might want to explore.

GFI EventsManager 7.0

GFI EventsManager 7.0 (http://www.gfi.com/eventsmanager) boasts some impressive features and is a great improvement over its predecessor, GFI LANguard Security Event Log Monitor 5.0. EventsManager supports Windows event logs, syslog, and World Wide Web Consortium (W3C) log files such as Microsoft IIS logs, but not Internet Authentication Service (IAS) logs.

EventsManager provides rule-based event log management that can be quickly deployed to filter out unwanted events and concentrate on those events that are pertinent to your situation. The latest version has an optimized, multithreaded event-processing engine designed to improve event scanning performance and to support plug-ins. GFI claims the product can process an impressive 6 million events per hour.

You can establish scanning profiles, which are used to configure rules for categories of assets. For example, you can configure different sets of rules for servers and workstations and apply the rules quickly. A generic profile can be applied to all assets and then supplemented with targeted profiles.

EventsManager makes the often cryptic and nearly unreadable Windows event log entries more user friendly. It provides extensive reporting capabilities, including many predefined reports ranging from account usage and management reports to policy change and application management reports to trend reports. EventsManager can notify systems administrators and operators via a variety of real-time alerts, including email messages, network messages, and Short Message Service (SMS) alerts via a gateway. In addition, EventsManager has event-filtering capabilities that include preconfigured event queries as well as a query builder that lets you build your own queries to retrieve events of interest from consolidated logs. It also lets you color-code significant events. GFI EventsManager 7.0 requires Microsoft SQL Server 7.0 or later or Microsoft SQL Server Desktop Engine (MSDE) to store collected events.

Even if you've considered and discounted previous versions of EventsManager, I recommend you take another look, if you're in the market for an enterprise event manager. The product is priced from $800 for 3 nodes to $32,000 for 500 nodes. Custom pricing is available for more than 500 nodes and for consultant licenses.

Total Event Log Management Suite

Dorian Software Creations offers a set of tools under the name Total Event Log Management Suite (http://www.doriansoft.com/totalsolution/index.htm). One tool in the suite is Event Archiver 6.0, which collects Windows event logs and stores them in a central location or database; it doesn't support IIS or IAS text log files or syslog. Event Archiver uses an agentless technology; a central server pulls event logs from monitored systems. Event Archiver lets you group several computers together into administrative domains to which you can apply policy settings that can automatically archive specific and different types of events for each group of computers. Event Archiver predefines more than 100 events that you can choose for collection. Collected log files can be stored in ODBC-compliant databases, and Event Archiver supports the SQLOLEDB Provider for large database import operations.

You analyze stored logs by using another tool in the suite, Event Analyst 5.0. This tool lets you search for specific events in stored event-log files or databases. You can create HTML-based reports from consolidated logs by using prepackaged reports or dynamic, filter-based queries.

A third tool in the suite, Event Alarm 4.0, is a Windows service that runs in the background and monitors Windows event logs and syslog messages generated by network devices. It's agentless and can monitor remote systems. A feature called False Positive Reduction lets you choose to ignore certain events that are known to be irrelevant in your environment. Like Event Archiver, Event Alarm comes with more than 100 predefined events that administrators can easily select to monitor. When events of interest are logged to a database, Event Alarm can notify systems administrators and operators via a number of means, including an email message, a network message, forwarding details of the event to a syslog server, and broadcasting over the network to administrators running Dorian Software Creations' proprietary notification utility.

The last tool in the suite is Event Rover. This tool lets you filter and sort Windows event log entries into a tree view for easier analysis. The tool can export log data to HTML-format reports. Event Rover links to Dorian Software Creations' Web site, http://www.eventlogs.com, at which you can research the meaning behind individual entries in the Windows event log.

The Event Log Management Suite is priced at $1,499.99 for five servers, 25 workstations, and an unlimited number of syslog devices or for 10 servers and an unlimited number of syslog devices. The price rises to $2,199.99 for 15 servers and an unlimited number of syslog devices. For pricing of other combinations of servers and workstations, contact Dorian Software Creations directly.

Sentry II

Engagent's Sentry II (http://www.engagent.com/newsite/products/product_sentryII.htm) is actually much more than simply a Windows event log, SNMP trap, and syslog management package. It can proactively monitor TCP/IP and Windows services, other running processes, and system performance. Sentry II monitors Windows systems from Windows 95 through Windows Server 2003, with support for both 32-bit and 64-bit OSs. Sentry II can also monitor UNIX and Linux servers and network devices by using SNMP traps and capturing syslog events, but it doesn't provide support for IIS and IAS text log files. It uses agents running on Windows 2003, Windows NT Server, or Windows 2000 Server to monitor systems.

Sentry II monitors events and can notify systems administrators and operators in real time via email, SMS, pager, SNMP, syslog, pop-up, and custom-program alerts when critical events are logged. Collected events can be stored in either a Microsoft Access or SQL Server database. Reports about archived events can be generated in PDF, HTML, Microsoft Excel, Microsoft Word, and other formats. Sentry II also lets you search consolidated event logs by such items as event identifier, username, event source, and description, and print, email, or export the results to a document. Contact Engagent directly for pricing information.

ELM Log Manager

Another tool is TNT Software's ELM Log Manager 4.0 (http://www.tntsoftware.com/products/elmlogmanager.aspx), which can monitor Windows event logs, Microsoft ISA Server log files, IIS log files, SQL Server error log files, and a number of other application log files, including custom log files, backup-software log files, antivirus log files, and static HTML files. ELM Log Manager also supports syslog and SNMP traps. ELM Log Manager uses an agent to collect logs and stores them in a SQL Server 7.0 or later database, or MSDE. You can manage default retention periods to optimize database usage. You can configure ELM Log Manager to fire off an alarm if a specific event is detected a certain number of times within a user-defined period, but you can also send an alarm if an event is not detected a certain number of times in a user-defined period—a unique feature.

A central console lets administrators view and search collected logs for events of interest. The tool ships with predefined reports that let administrators quickly identify computer and user account creation and management activities, privilege elevation by users, logon and logoff activity, object access to files and registry subkeys, and Group Policy activity. ELM Log Manager can also notify systems administrators and operators in real time via email, executed command scripts, network alerts, IM, syslog, SNMP, SMS, and several other methods.

TNT Software offers other tools that SMBs might find interesting, including ELM Event Log Monitor 4.0 and ELM Enterprise Manager 4.0. ELM Event Log Monitor provides a subset of ELM Event Log Manager's features for businesses that don't require all the features that ELM Event Log Manager provides. ELM Enterprise Manager contains all the features of ELM Log Manager and many more, including real-time monitoring of applications and services. Contact TNT Software directly for pricing information.

EventTracker

Prism Microsystems' EventTracker (http://www.eventlogmanager.com) uses an agent-based architecture for log management and claims to be able to handle as many as 700 events per minute with its standard agent and 7,000 events per minute with its high-performance agent. EventTracker also supports an agentless architecture for Windows systems, which is useful when performance isn't a concern. EventTracker supports Windows event logs, IIS, and syslog, and with additional tools, Linux and Sun Solaris systems. EventTracker doesn't support IAS or SNMP traps.

In addition to monitoring for security-related events, EventTracker can report the starting and stopping of applications (useful for license tracking), memory usage, disk space, CPU utilization, and services. EventTracker can notify systems administrators and operators in real time of critical events via email, pager, and custom command script. EventTracker is integrated with Prism's EventTracker Knowledge Base, which contains information about events that can be generated by various devices and event sources. EventTracker also supports plug-ins to monitor Web sites and networks for such things as unauthorized intrusion by looking for unusual or unexpected traffic patterns. Unusual traffic patterns could include network traffic associated with a hacker attempting to port-scan remote systems, browse the network for unsecured shares, or log on to local accounts. EventTracker relies on a trusted configuration profile—in other words, permitted or legitimate traffic—to identify potential attacks. EventTracker provides rich reporting capabilities with standard report templates and support for customized reports. One strong feature of EventTracker is its ability to warehouse encrypted and signed events in a centralized location. Contact Prism Microsystems directly for pricing information.

LogCaster for Security Auditing & Systems Management

RippleTech's LogCaster for Security Auditing & Systems Management (http://www.rippletech.com/products/logcaster.htm) uses an agent-based architecture. The agent collects important system information, filters it, and passes it back to the LogCaster Server, where it is stored in a SQL Server 2005, SQL Server 2000, or MSDE database. The LogCaster Server can also collect syslog events. The LogCaster agent collects Windows event logs and processes each entry based on predetermined event rules to filter out unwanted events. The agent can process text files, including tab-delimited and comma-separated-values (CSV) files, using rules similar to those used to filter the event logs. The ability to process text files lets you configure LogCaster to monitor IIS, IAS, and other log files.

You use the LogCaster Management Console to configure LogCaster agents deployed on monitored systems and to view filtered events in real time. One nice feature is LogCaster Server's ability to deploy the agent to remote systems. The LogCaster agent can report changes in status to running services and applications as well as monitor system performance. You can use the included templates to quickly configure monitoring rules. LogCaster can notify administrators by email, pager, SMS, broadcast message, and other means. It also provides strong reporting features and has a wizard that helps you quickly create custom report templates. This tool goes one step further by providing rich logs of its own activities, which let you verify that LogCaster is working correctly and diagnose problems. Contact RippleTech directly for pricing information.

Still More to Choose From

Each tool I've described can be downloaded for evaluation before purchase. The list is not exhaustive, however—other solutions are available that might interest you. For example, you might want to consider Microsoft Operations Manager (MOM) 2005, or the forthcoming Microsoft System Center Operations Manager 2007, which comes with a new tool called Audit Collection Services (ACS). For more information about MOM 2005 Workgroup Edition, see the *Windows IT Security* article "MOM for SMBs," January 2007, InstantDoc ID 94361, and "MOM Management Packs," January 18, 2007, InstantDoc ID 94671. I will describe Ops Manager 2007 and ACS in a future article. Secure Vantage Technologies (http://www.securevantage.com) provides management packs and reporting solutions for MOM 2005 and Ops Manager 2007's ACS.

InstantDocID #95511

Vista's ActiveX Installer

Take charge of ActiveX-control downloads with this new service

By Russell Smith

One of the problems associated with least privileged user accounts in Windows XP is that when users browse to a Web site that requires them to download an ActiveX control to display the Web page contents, they don't have the authority to install the control. An ActiveX control from a rogue Web site can be used for malicious purposes. Therefore, ActiveX controls should always be installed with caution from trusted sources only, preferably by an administrator who understands the risks. In practice, this means that users with limited privileges must wait until a support technician with administrative privileges has time to install controls for them. Hardly an ideal situation, but preferable to running Microsoft Internet Explorer (IE) with administrative privileges, in most cases.

This is where Windows Vista's ActiveX Installer Service comes in. This service—in Vista Ultimate, Business, and Enterprise editions only—can be used in conjunction with Group Policy to determine whether a least privileged user is allowed to install an ActiveX control package (i.e., an .ocx, .dll, or .cab file) from a particular URL. If ActiveX Installer Service finds the URL on the allowed list in Group Policy, the service will install the control on the user's behalf. Although Installer Service has some limitations (which I discuss below), it does give users and their administrators some control over ActiveX objects, so I believe it's worth using. Let's look at how to set up Installer Service to install Adobe Flash Player for users who request it.

Background and Moving Ahead

I should note that pre-Vista, IE isn't totally without control over ActiveX components. In XP Service Pack 2 (SP2) with IE 6.0 or later, it's possible to run as an administrator and block installation of all ActiveX controls. For each IE security zone, you can configure whether an administrative user can download and run signed or unsigned ActiveX controls. Also, you can define a list of "administrator approved" ActiveX controls in Group Policy that local administrators can run. These Group Policy settings are fine for restricting administrative users, but they don't help when it comes to allowing least privileged users to install controls. These users are barred from installing controls no matter what policy is set.

To make use of ActiveX Installer Service, you must install it because it's an optional Windows component. In the Ultimate, Business, or Enterprise edition of Vista, log on with an account that has administrative privileges, open Control Panel, and select Programs. Select *Turn Windows features on or off*. You'll see ActiveX Installer Service at the top of the list. Select its check box as shown in Figure 1, then click OK.

Allowing Flash Player

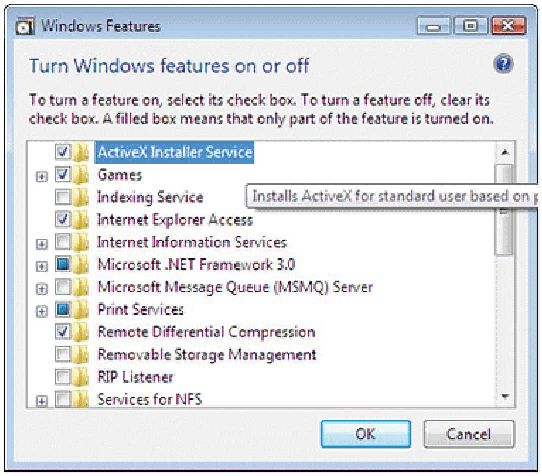
Before you can actually set a policy that specifies which URLs least privileged users can download ActiveX controls from, you need some information about those Web sites and controls. To get that information, you can generate an event related to a URL and control and look in the event description.

To cause an event, first log on to Vista with a user account that's a member of the built-in users group only. You shouldn't have any administrative privileges.

For the purposes of this article, we're going to work with Flash Player, so go to the Adobe Flash Player Download Center at http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash. (If you already have this control installed on your system, you can use IE's *Manage Add-ons* tool to remove it.)

Click the button to install Flash Player 9 on your computer. Vista's User Access Control (UAC) will prompt you to enter an administrator username and

Figure 1: Turning on ActiveX Installer Service



Windows Features

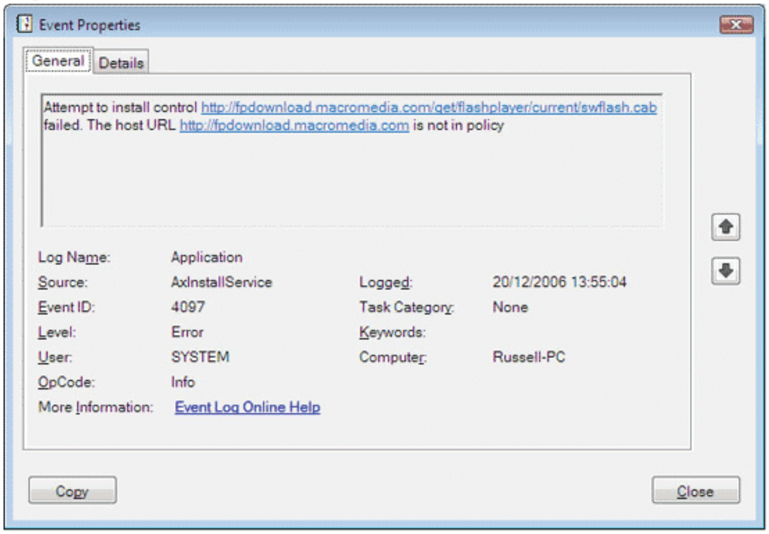
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ ActiveX Installer Service
- ⊞ ☑ Games
- ☐ Indexing Service
- ☑ Internet Explorer Access
- ⊞ ☐ Internet Information Services
- ⊞ ■ Microsoft .NET Framework 3.0
- ⊞ ☐ Microsoft Message Queue (MSMQ) Server
- ⊞ ■ Print Services
- ☑ Remote Differential Compression
- ☐ Removable Storage Management
- ☐ RIP Listener
- ⊞ ☐ Services for NFS

Installs ActiveX for standard user based on p

Figure 2: Event 4097



Attempt to install control http://fpdownload.macromedia.com/get/flashplayer/current/swflash.cab failed. The host URL http://fpdownload.macromedia.com is not in policy

```
Log Name:          Application
Source:            AxInstallService          Logged:          20/12/2006 13:55:04
Event ID:          4097                      Task Category:   None
Level:             Error                     Keywords:
User:              SYSTEM                    Computer:        Russell-PC
OpCode:            Info
More Information:  Event Log Online Help
```

password for the Internet Explorer Add-on Installer. At this point, click Cancel on the UAC prompt. Now, you have your event.

Log off as the standard user and log back on as an administrator. (You could probably use Fast User Switching—FUS—here, but I prefer during testing not to use it, especially when making changes to Group Policy. In my experience, depending on which policy I'm modifying, a log on or off or even a reboot might be required. The results are more consistent when you log off and on, even if it takes a little longer.)

Open the Event Viewer (type *event* in the Search box on the Start menu, and the Event Viewer will appear under Programs), and search the application event log for event ID 4097. Figure 2 shows the event information, which gives you two important pieces of data: the name of the ActiveX control file and the host URL. The control filename—swflash.cab—tells you that this is a file that ActiveX Installer Service can handle. (Remember that Installer can install controls packaged as .ocx, .dll, or .cab files.) The host URL—http://fpdownload.macromedia.com—is what you need to configure ActiveX Installer Service to allow to install the control.

In a corporate environment, you'd configure an Active Directory (AD)-based Group Policy Object (GPO) in order to set up Installer for multiple machines, but for the purposes of testing, I'll describe configuring the local computer policy to enable standard users to install Flash Player.

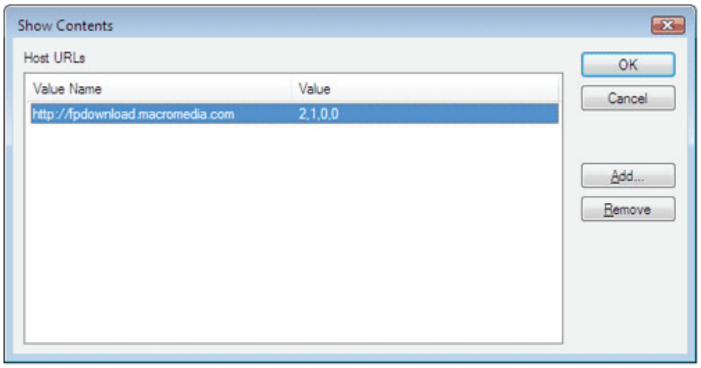
At the Start menu, type *gpedit.msc* in the Search box, and click Enter. Under Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\ActiveX Installer Service, click *Approved Installation Sites for ActiveX Controls*, select Enabled, and click Show. In the Show Contents dialog box, click Add and enter the host URL http://fpdownload.macromedia.com as the value name and 2,1,0,0 as the value. Click OK. Figure 3 shows the resulting dialog box.

The first three digits of value 2,1,0,0 tell ActiveX Installer Service how trusted, signed, and unsigned controls should be handled. A 0 means *don't install*, a 1 means *prompt the user before installing*, and a 2 means *silent install*. Thus, in the value 2,1,0,0, the 2 tells Installer that it can silently install trusted controls, the 1 tells Installer to prompt the user before installing digitally signed controls, and the 0 ensures that unsigned controls won't be installed.

The fourth digit of value 2,1,0,0 tells ActiveX Installer Service how to handle HTTP Secure (HTTPS) certificate errors. The default value is 0, which means that there can be no certificate errors when installing a control. The other possible values are listed in Table 1. If an ActiveX control is hosted from an HTTPS URL, the non-0 settings lower the security requirements for resolving problems with certificate errors.

Click OK in the *Approved Installation Sites for ActiveX Controls* dialog box and close Group Policy Editor (GPE). To make sure that the policy takes effect immediately, we need to force a policy update. Open

Figure 3: Setting a policy for handling ActiveX controls



Value Name	Value
http://fpdownload.macromedia.com	2,1,0,0

a command prompt and type

```
gpupdate /force
```

It will take a few seconds for the policy to be refreshed.

Tests and Caveats

After the command has completed, log back on as the standard user and try again to install Flash Player. Open IE and go once again to the Adobe Flash Player Download Center Web site. Attempt to install the control again and notice the difference in behavior. This time, an ActiveX Installer Service prompt will ask you for permission to install the control. Grant the permission, and after a few seconds, you should see that the process has been successful from the flash animation in the Web browser window. No administrative privileges required.

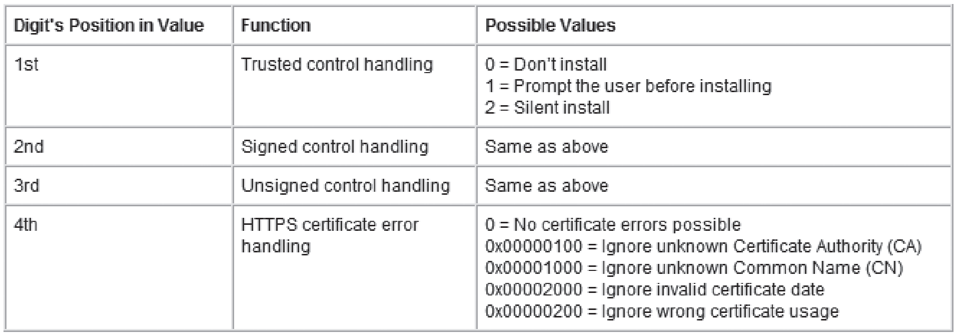
You should confirm that if you as the standard user browse to another site that prompts for the download and installation of an ActiveX control, Vista applies its standard security restrictions. For example, if you browse as the standard user to http://www.apple.com/quicktime/player/win.html, UAC will prompt you for administrative credentials because the host URL isn't defined in a policy. Cancel the UAC request and (after logging off as the standard user and logging back on as an administrator) check the application event log again for event ID 4097. Note the different host URL for Apple QuickTime.

The policy that you've just configured should let a standard user install any ActiveX controls that are in the required package format and that are hosted at the Adobe URL the policy specifies. However, in my testing, I've experienced problems installing certain controls even if they're packaged in one of the supported formats. For example, ActiveX Installer Service installation of the Adobe Shockwave Player (which is in the correct format and is at the same Adobe URL as Flash Player) prompts for credentials, which defeats the point of Installer. The lesson here is that you need to test every potential ActiveX control that you want Installer to approve for installation on your network.

If the fact that you're trusting the hosting company and any controls it decides to publish at the given URL, rather than any one specific ActiveX control, gives you pause, you'll need to look for a different solution. However, in my opinion, ActiveX Installer Service is a huge improvement over managing ActiveX controls in previous versions of Windows. See the *Windows IT Pro* article "Deactivate ActiveX to Protect Your SBS Network," January 2006, InstantDoc ID 48400, for instructions about how to manage ActiveX downloads in pre-Vista Windows.

InstantDocID #95515

Table 1: ActiveX Control Handling



Digit's Position in Value	Function	Possible Values
1st	Trusted control handling	0 = Don't install 1 = Prompt the user before installing 2 = Silent install
2nd	Signed control handling	Same as above
3rd	Unsigned control handling	Same as above
4th	HTTPS certificate error handling	0 = No certificate errors possible 0x00000100 = Ignore unknown Certificate Authority (CA) 0x00001000 = Ignore unknown Common Name (CN) 0x00002000 = Ignore invalid certificate date 0x00000200 = Ignore wrong certificate usage

Toolbox: Icacls

New search and save features beef up this ACL tool

By Jeff Fellinge

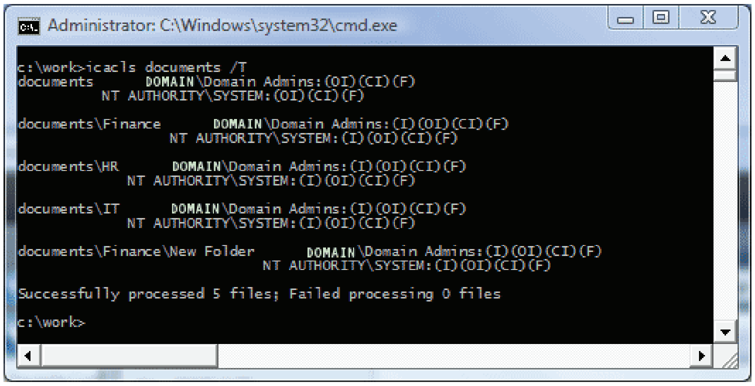
A command-line tool to audit and modify file permissions makes a valuable addition to any systems administrator's toolbox. In Windows Vista and Windows Server 2003 Service Pack 2 (SP2), Microsoft included an updated version of its Cacls tool (cacls.exe) called Icacls (icacls.exe). Icacls helps you review, set, save, and restore folder and file permissions using user or group names or SIDs. Let's take Icacls out for a spin by using it to review, set, save, and restore rights on a set of folders.

Using Icacls

Unlike Cacls, Icacls lets you save the ACL configurations of a folder and its subdirectories to a file and restore them later. Icacls offers the ability to search a set of directories for any rights that a particular SID has. You can grant or deny rights based not only on a user or group name but also on a SID. If you need to change more than just a few permissions or to repeatedly audit a set of folders, you'll find that Icacls is a time-saver. Using Icacls also reduces the chance of error, because you can make your changes in a text file (or a program such as Microsoft Excel) and then execute all the changes after you've double-checked your settings.

For demonstration purposes, we'll use a set of folders named HR, Finance, and IT contained in a parent directory called Documents. You'll need to create domain local groups named HR-Author, HR-Reader, Finance-Author, Finance-Reader, IT-Author, and IT-Reader, into which you'll add users who need either modify (i.e., author) or read-only (i.e., reader) access. This is a common permission model and will demonstrate the usefulness of Icacls.

Figure 1: Using Icacls to check your Documents folder's ACLs



```
c:\work>icacls documents /T
documents       DOMAIN\Domain Admins:(OI)(CI)(F)
            NT AUTHORITY\SYSTEM:(OI)(CI)(F)

documents\Finance       DOMAIN\Domain Admins:(I)(OI)(CI)(F)
                    NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

documents\HR       DOMAIN\Domain Admins:(I)(OI)(CI)(F)
               NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

documents\IT       DOMAIN\Domain Admins:(I)(OI)(CI)(F)
               NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

documents\Finance\New Folder       DOMAIN\Domain Admins:(I)(OI)(CI)(F)
                                NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

Successfully processed 5 files; Failed processing 0 files

c:\work>
```

Breaking Folder Inheritance

To set permissions on a subdirectory that are different from the permissions on the parent directory, you must first break folder permission inheritance. To do this, use the GUI to check for and remove any unwanted inherited ACLs and access control entries (ACEs) affecting the Documents folder.

Next, set the inheritance behavior of the ACEs that you add to the Documents folder. Right-click the Documents folder and click Properties. Click the Security tab, then the Advanced button. Select the Permissions tab, click Edit, and review the listed permissions entries. You should see entries labeled Domain Admins, Folder Operators, SYSTEM, and possibly others. Clear the *Include inheritable permissions from this object's parent* check box in the Edit dialog box. Click the Copy button to copy the permissions entries. Now you've broken inheritance but have preserved the ability for the original groups, such as Domain Admins, to access the folder. Next, individually remove any permissions that you don't want for the Documents folder by clicking the name of the ACE and then clicking Remove.

Reviewing ACLs

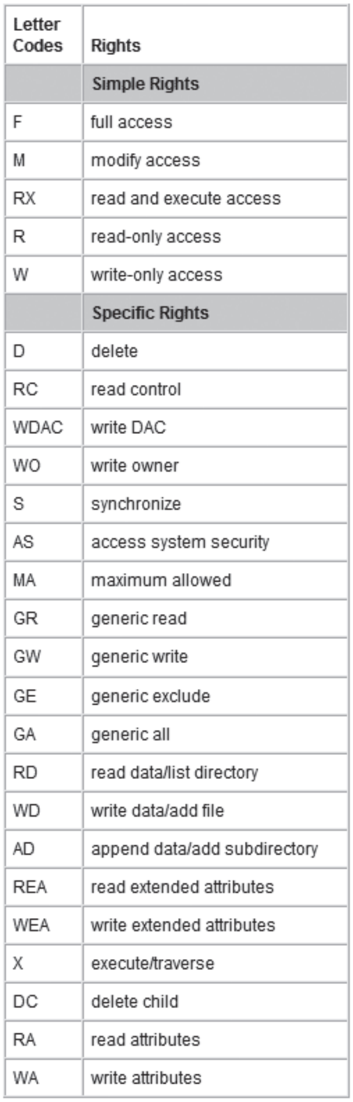
Now that you've broken inheritance and removed any unwanted permissions, run the command

```
icacls documents /T
```

to review the Documents folder's ACLs, as Figure 1 shows.

Icacls lists all the rights of the Documents folder and—because you specified the /T parameter—its subdirectories (i.e., \Finance, \HR, \IT). At the end of each ACE (e.g., in documents\HR DOMAIN\Domain Admins: (I)(OI)(CI)(F)), you can see a list of the inheritance properties and the simple and specific rights. If the ACE is inherited from its parent, you'll see (I) listed before all of the other rights. We broke inheritance at the Documents level, but subdirectories under Documents still inherit from Documents.

Table 1: Icacls Letter Codes for Simple and Specific Rights



Letter Codes	Rights
	Simple Rights
F	full access
M	modify access
RX	read and execute access
R	read-only access
W	write-only access
	Specific Rights
D	delete
RC	read control
WDAC	write DAC
WO	write owner
S	synchronize
AS	access system security
MA	maximum allowed
GR	generic read
GW	generic write
GE	generic exclude
GA	generic all
RD	read data/list directory
WD	write data/add file
AD	append data/add subdirectory
REA	read extended attributes
WEA	write extended attributes
X	execute/traverse
DC	delete child
RA	read attributes
WA	write attributes

Icacls also lets you set and observe the inheritance behavior of an object. For example, the applied inheritance *This folder, subfolders, and files* is denoted as (OI)(CI), which means that Object Inherit (OI) and Container Inherit (CI) are enabled. Icacls also uses the Inherit Only (IO) and Non-Propagate (NP) inheritance flags. You can set these inheritance properties when you use Icacls to define an ACE.

(F) represents Full access and (M) represents Modify access. Table 1 lists all the codes Icacls uses to define simple and specific rights.

Useful Commands to Get You Out of Trouble

Before you write a series of Icacls commands to set the permissions and inheritance for the subdirectories, back up the current ACLs using Icacls' Save feature. Run the command

```
icacls documents\* /save
 acl-documents /T
```

to back up the ACLs of the Documents directory and its subdirectories to a file named acl-documents located in the directory in which you ran the Icacls command. It's a good idea to back up the ACLs because if you make a mistake when you're tweaking them, you can quickly restore them to the point at which you saved them. To restore the ACLs, use the /restore parameter:

```
icacls Documents /restore
 acl-documents
```

You can also reset the permissions by running the command

```
icacls documents /reset /T
```

This command essentially enables permission inheritance at the folder level that you specified and wipes out any custom permissions on underlying directories. In addition to resetting any permissions work you've done on the Documents folder and its subdirectories, this command also re-enables inheritance, so use it with care.

Setting Permissions

Now, let's set permissions to allow a group to read from a specific folder. To grant the *read and execute access* (RX) right for the HR-Reader group to the Documents/HR directory, run the following command:

```
icacls documents\HR /grant
 "Domain\HR-Reader":
 (OI)(CI)(RX)
```

where *Domain* is the name of your domain.

This command adds a new ACE to the directory, but you could use the optional /grant:r parameter to replace previously set explicit rights. Also, this command adds the (OI) and (CI) inheritance flags so that any new folders or files placed into the HR directory inherit these rights. You can easily test whether the inheritance flags are working by creating a new subdirectory under the HR folder and running the command

```
icacls documents/HR /T
```

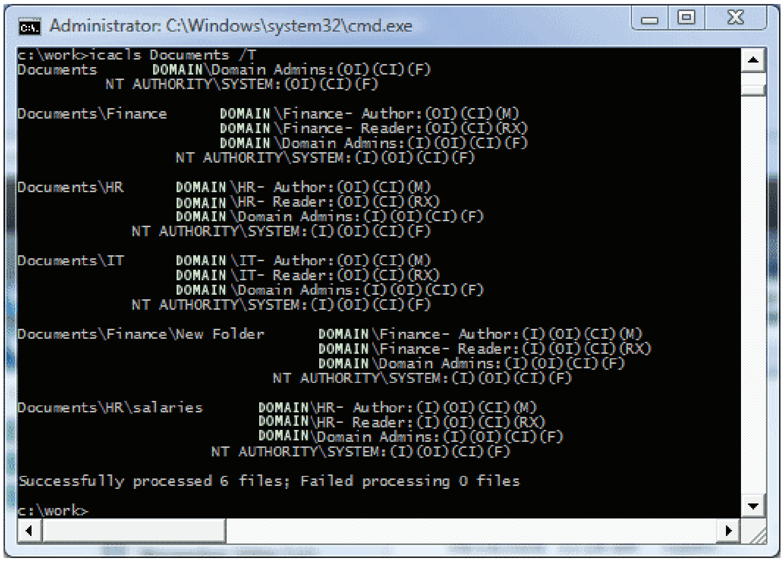
which shows you that the HR-Reader group has inherited the *read and execute access* (RX) right to the new folder that you created. If you omit the (OI)(CI) inheritance flags, your ACE will apply only to the folder on which you set it.

After you've set up one group's command the way you want it, you can then create Icacls commands for your remaining groups. The following commands set the permissions for our sample folders and groups:

```
icacls documents\HR
 /grant:r "domain\HR-Reader":
 (OI)(CI)(RX)
```

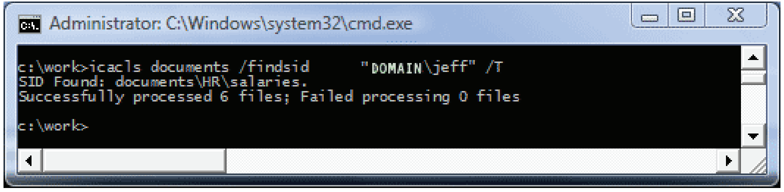
```
icacls documents\Finance
 /grant:r "Domain\Finance-Reader":
 (OI)(CI)(RX)
icacls documents\IT
 /grant:r "Domain\IT-Reader":
 (OI)(CI)(RX)
icacls documents\HR
 /grant:r "Domain\HR-Author":
 (OI)(CI)(M)
icacls documents\Finance
 /grant:r "Domain\Finance-Author":
 (OI)(CI)(M)
icacls documents\IT
 /grant:r "Domain\IT-Author":
 (OI)(CI)(M)
```

Figure 2: Verifying ACE permissions using Icacls



```
c:\work>icacls Documents /T
Documents      DOMAIN\Domain Admins:(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(OI)(CI)(F)

Documents\Finance      DOMAIN \Finance- Author:(OI)(CI)(M)
                       DOMAIN \Finance- Reader:(OI)(CI)(RX)
                       DOMAIN \Domain Admins:(I)(OI)(CI)(F)
                  NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

Documents\HR      DOMAIN \HR- Author:(OI)(CI)(M)
                  DOMAIN \HR- Reader:(OI)(CI)(RX)
                  DOMAIN \Domain Admins:(I)(OI)(CI)(F)
             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

Documents\IT      DOMAIN \IT- Author:(OI)(CI)(M)
                  DOMAIN \IT- Reader:(OI)(CI)(RX)
                  DOMAIN \Domain Admins:(I)(OI)(CI)(F)
             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

Documents\Finance\New Folder      DOMAIN\Finance- Author:(I)(OI)(CI)(M)
                                  DOMAIN\Finance- Reader:(I)(OI)(CI)(RX)
                                  DOMAIN\Domain Admins:(I)(OI)(CI)(F)
                             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

Documents\HR\salaries      DOMAIN\HR- Author:(I)(OI)(CI)(M)
                           DOMAIN\HR- Reader:(I)(OI)(CI)(RX)
                           DOMAIN\Domain Admins:(I)(OI)(CI)(F)
                      NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)

Successfully processed 6 files; Failed processing 0 files

c:\work>
```

Figure 3: Auditing permissions using Icacls



```
c:\work>icacls documents /findsid     "DOMAIN\jeff" /T
SID Found: documents\HR\salaries.
Successfully processed 6 files; Failed processing 0 files

c:\work>
```

Verifying and Auditing Permissions

After you run these commands, you can verify that the ACEs are properly set by again running the Icacls command with the /T parameter. Figure 2 shows the results; you can see that the subdirectories are correctly inheriting permissions. Icacls also includes a parameter called /findsid, which is useful for discovering whether a particular SID has rights to a folder or set of folders. For example, you can see whether the user jeff has rights in the Documents folder or any of its subdirectories by running the following command:

```
icacls documents /findsid
 "Domain\jeff" /T
```

Icacls audits the permissions and reports its findings. As Figure 3 shows, the user jeff has access to the Documents folder and the HR\salaries subdirectory. The /findsid parameter can also be quite useful in determining whether someone inappropriately changed permissions in a large directory structure where manually checking permissions is impractical. For more information about Icacls, see the *Windows IT Pro* article Windows Power Tools: “Icacls: The New and Improved Cacls?” May 2007, InstantDoc ID 95346.

InstantDocID #95657

Access Denied

Answers to your Windows security questions

By Randy Franklin Smith

Using the Correct Certificate Template for Client Certificates

Q: Can Encrypting File System (EFS) certificates and Web application client certificates conflict with one another? In our environment, we use EFS to secure the My Documents folder on laptops. We also have a key business partner whose extranet requires some of our users to install a client certificate for secure Web-based access to logistics information. One such user's client certificate recently expired, so I deleted it and requested a new one from our business partner's Certification Authority (CA). After the CA issued the new certificate, I installed it on the user's workstation and everything appeared to be working fine. A short time later, however, I received a call from the user saying that he couldn't access his encrypted My Documents folder. I knew I hadn't deleted the user's EFS certificate, and I quickly confirmed that by using the Microsoft Management Console (MMC) Certificates snap-in. Luckily, we were able to recover the user's files using the EFS Recovery Agent certificate. Apparently, the client certificate—rather than the EFS certificate that we provide through the domain—had encrypted the user's files. Is that possible, and if so, why? Aren't certificate templates supposed to define what purposes a certificate can be used for?

A: It is possible for the client certificate to encrypt user files, and you're on the right track by thinking about certificate templates. Certificate templates define how a certificate can be used and should prevent what happened in your situation if used correctly. Windows workstations automatically request EFS certificates for users based on the Basic EFS template for protecting encrypted files. The only purpose the Basic EFS template allows is EFS certificate creation.

In your case, I think your business partner issued the user a certificate based on the User certificate template instead of the Authenticated Session certificate template. The User certificate template includes EFS, secure email, and client authentication among its purposes. After this certificate was installed, the workstation had two viable EFS certificates and began encrypting new files using your business partner's EFS certificate. If any files on the workstation were created before you installed the new certificate, the user still would have been able to access them, even after you deleted the expired certificate.

There are two lessons to be learned from this situation. First, make sure you define data recovery agent certificates via Group Policy and back them up every time you use EFS. Second, administrators should avoid using the User certificate template to secure Web-based applications, especially for outside business partners such as your user. Instead, ask your business partners to issue certificates based on the Authenticated Session certificate template, which doesn't include EFS as one of its purposes. I also recommend looking into BitLocker Drive Encryption, which is a new feature in Windows Vista. I think BitLocker is far superior to EFS as an encryption solution for most laptop encryption needs. For more information about BitLocker, see the *Windows IT Pro* articles "Vista's BitLocker Drive Encryption," June 2007, InstantDoc ID 95673, and "Security Annoyances," February 2007, InstantDoc ID 94414.

For more information about EFS, see the *Windows IT Security* article "Take a Closer Look at EFS," September 2005, InstantDoc ID 47175. To read more about certificates, see the *Windows IT Security* article "Sharing Information Securely," October 2005, InstantDoc ID 47625.

InstantDocID #95601

Logging Remote Desktop Connections

Q: We believe someone at our company is using another employee's account to access a workstation remotely via Remote Desktop Connection. We know the authorized employee couldn't have accessed the workstation because at that time he was on a 12-hour flight with no Internet access. Can we get a list of all the Remote Desktop logons to our workstations from Small Business Server's (SBS's) Security log?

A: The short answer is no. Your question illustrates why it's so important to enable auditing not only on your domain controllers (DCs), but also on your workstations and member servers.

Assuming the SBS system is your only server, it's also your DC. And if the SBS system's audit policy is configured with default settings, the Security log will have a record of all the successful authentications of domain accounts—including Remote Desktop logons to workstations. (Default audit policy enables only successful account logon events—not failures.) In your DC's Security log, look for event ID 672 (authentication ticket granted) in which the service name is the computer name of the workstation that was accessed. Also look for event ID 680 (account used for logon by) where the workstation name matches that of the accessed workstation. In both events, the description's User Name line will identify the user who was authenticated to the workstation.

However, you must understand that DCs log authentication events—not logon events (there's a difference). Authentication is the same to a DC no matter what type of logon occurs at the workstation. From the DC's Security log you can't determine whether the authentication event was caused by a Remote Desktop Connection logon, a local console logon, or a logon to a shared folder on the workstation. The only way to find out what caused the authentication event is to enable the workstation's logon/logoff auditing. Most Windows workstations don't enable auditing by default, so unless you've already enabled logon auditing for the workstation, no such record exists. Also note that DC Security logs show only authentication events involving domain accounts. Any attempt to log on to a workstation using a local account in the workstation's SAM will show up only in that workstation's Security log, not in the DC's Security log.

InstantDocID #95602

Comparing BitLocker with EFS

Q: How does Windows Vista's BitLocker Drive Encryption compare with Windows XP's Encrypting File System (EFS) for protecting data on a laptop?

A: I was a long-time EFS user, but I recently stopped using it in favor of BitLocker. EFS works on a file-by-file basis, whereas BitLocker encrypts the entire volume and eliminates many of the laptop vulnerabilities that let information leak out of encrypted folders and into unencrypted folders. EFS is also vulnerable to sophisticated attacks that insert malicious code into the startup files in the Windows OS and wait for the user to enter a password and access encrypted files. A laptop equipped with the Trusted Platform Module and BitLocker can mitigate this risk.

BitLocker also supports storing the encryption key on a USB flash drive for added security. You can even use certain USB flash drives that support biometric authentication, such as those from MXI Security, to require two-factor user authentication before allowing access to encrypted drives. Note that only Vista Ultimate and Vista Enterprise support BitLocker.

InstantDocID #95603

Reader to Reader: Tips to Secure Your Backup Tapes

By Gregory W. Smith

As part of a disaster-recovery plan, many companies regularly perform full backups of their network or server data and store the backups offsite. However, after spending the time and resources to secure the data, it's risky to simply store the backups offsite. You need to protect them as well.

As a systems analyst, I've found that many administrators back up to tapes, then protect those tapes with passwords. My primary experience is with Symantec's Backup Exec, so I'll talk specifically about using that product to back up to tapes. However, no matter what backup tool and what backup media you use, you need to make sure the backups are secured with passwords and the data is encrypted.

Backup Exec lets you protect tapes with passwords. The password-protected tapes work seamlessly on the local server, but you're prompted for the password when the tapes are imported on any other server. In Backup Exec versions earlier than 11d, you can't encrypt the backup data, so if the password request is bypassed, the entire backup becomes available.

Fortunately, Backup Exec 11d provides encryption capabilities. All data written to tapes is encrypted with a key you generate, which means that your tapes are much more secure in the event of loss or theft. (Note that if you back up to disks, Backup Exec 11d doesn't encrypt some types of data. However, there are workarounds.)

Encrypting backup data causes a performance hit on the backup job, but this hit can be kept to a minimum if you use software compression rather than hardware compression on your backup jobs. Software compression will compress the data before encryption, whereas hardware compression will compress the encrypted data. Because encrypted data is randomized, applying hardware compression can actually increase the size of the job.

With password-protected, encrypted backup tapes, the disaster-recovery plan must include the password and the encryption key so that the tapes can be restored if needed. The disaster-recovery plan and backup tapes should be kept separate to avoid compromise.

Editor's note: This Reader to Reader item was a winning entry in the Know Your IT Security contest sponsored by Microsoft Learning Paths for Security.

InstantDocID #95723