Realtime
publishers

Security Management Tactics
for the Network Administrator

The Essentials Series

Controlling and Managing Security with Performance Tools

Mike Danseglio

Copyright Statement

Controlling and Managing Security with Performance Tools

There are as many facets of computer security as there are attackers trying to get through your firewall today. And that's a lot. Each system that you're responsible for needs to be protected—individually and as part of the whole. For example, to comply with many government and industry regulations, you can't just lock down the network perimeter or the desktop computer. Holistic systems to implement, manage, and monitor the system security and configuration must be put in place and then regularly audited with the collection, storage, and analysis of system logs. Records must also be kept and regularly reviewed that track changes to systems to ensure continuous compliance with corporate and industry policy.

In the previous article, you read about using network inventories and maps to identify the resources on your network. That article also called out a technique for gathering the necessary data using an existing performance management infrastructure. In this article, I'll show you how to extend that technique beyond enumeration into the realm of systems management. You'll see why this is a valuable approach to consider, especially in smaller businesses and companies whose IT budgets are tightening daily.

Why Performance Tools?

It doesn't seem intuitive, at first glance, to consider performance management tools as useful for security management tasks. After all, performance management is all about measuring memory use and CPU cycles, restricting disk use, starting and stopping virtual machines, and so forth. That's the common perception. In fact, many administrators' knowledge of performance management is limited to the built-in Windows Task Manager (see Figure 1) or the free Process Monitor tool from Microsoft. But these are not true performance management solutions.

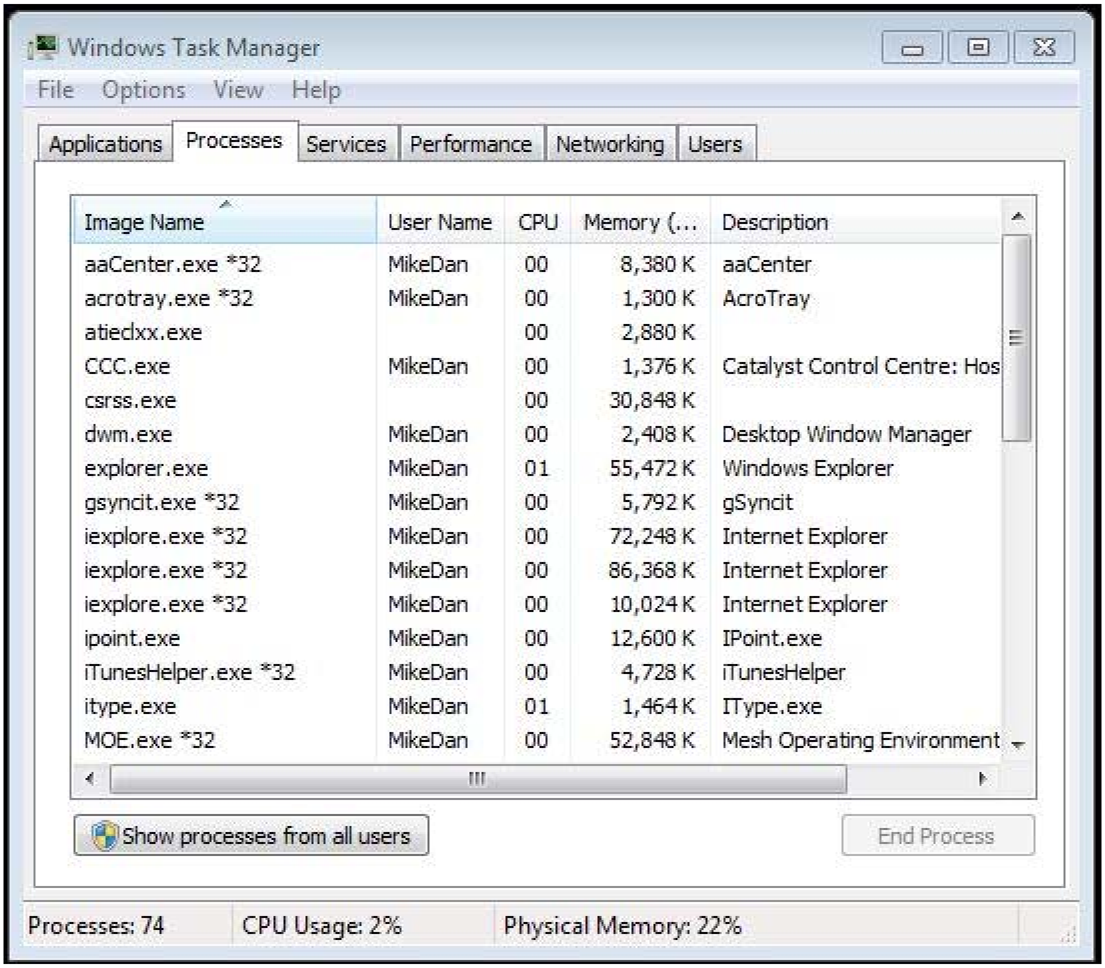

Image Name	User Name	CPU	Memory (...	Description
aaCenter.exe *32	MikeDan	00	8,380 K	aaCenter
acrotray.exe *32	MikeDan	00	1,300 K	AcroTray
atiedxx.exe		00	2,880 K	
CCC.exe	MikeDan	00	1,376 K	Catalyst Control Centre: Hos
csrss.exe		00	30,848 K	
dwm.exe	MikeDan	00	2,408 K	Desktop Window Manager
explorer.exe	MikeDan	01	55,472 K	Windows Explorer
gsyncit.exe *32	MikeDan	00	5,792 K	gSyncit
iexplore.exe *32	MikeDan	00	72,248 K	Internet Explorer
iexplore.exe *32	MikeDan	00	86,368 K	Internet Explorer
iexplore.exe *32	MikeDan	00	10,024 K	Internet Explorer
ipoint.exe	MikeDan	00	12,600 K	IPoint.exe
iTunesHelper.exe *32	MikeDan	00	4,728 K	iTunesHelper
itype.exe	MikeDan	01	1,464 K	IType.exe
MOE.exe *32	MikeDan	00	52,848 K	Mesh Operating Environment

Processes: 74 CPU Usage: 2% Physical Memory: 22%

Figure 1: Task Manager is not a performance management solution.

The reality is that performance management solutions are software suites that are deeply integrated within an entire infrastructure. These solutions tie in to core pieces of every system and component. The tight integration enables rich data reporting from across a workgroup, a data center, or a worldwide enterprise. And most performance management solutions have reporting tools that can give both instant summaries and detailed reports of what's happening on all systems.

You can probably already surmise that, when the solution is configured to retrieve security data as well as performance data, the solution's functionality is extended to become a great security dashboard and reporting tool. That's the case with most performance suites today. Many IT professionals want centralized security analysis and reporting across an enterprise, so most software vendors in this space have enabled their systems to provide this feature—either through simple customization or right out of the box.

How Do I Configure Security with These Tools?

The feature that enables these solutions to work for security may already be obvious to you. The tools that you use for performance management don't just report on performance. They enable you to control it.

Most performance management solutions have technology that enables, for example, restriction of virtual machine memory use per virtual machine. As an administrator, you first define the memory utilization parameters for a group of systems. Then the performance management tools configure the target systems to conform to your definition. The performance management system then verifies that the parameters have been applied, and reports success back to the reporting console. Finally, the settings are monitored over time to ensure compliance. When a situation occurs where the settings are not applied or adhered to, or a defined threshold is reached, the system takes action—often in the form of an administrative alert.

Alerts, monitoring, configuration management… this sounds very much like a security management solution. So why can't we use this same technique to configure security settings? Well, we can!

As I mentioned earlier, most performance management tools are already being extended to configure any part of a network—operating systems (OSs), routers, switches, and so on. For example, one common tool in the industry is largely billed as an enterprise-wide performance monitoring and management suite. Its marketing material mostly illustrates examples with virtual machine, OS, and switch management, with various plug-in modules to extend functionality. But a brief look at the interface shows that the solution is much more of a generic configuration framework for configuring and monitoring heterogeneous systems. This same solution allows you to load configurations, execute custom scripts, and even back up, restore, apply, report on, and enforce configuration sets. On top of all that, the suite still does a great job of performance management (even providing a Web-based version of the Task Manager that Figure 1 shows). This is exactly what you want in a security solution.

The one facet that makes these solutions work is that most technology today can be managed through automated processes and controls. This automation spans the range of devices, OSs, applications, and even data. Virtually anything within the IT domain is subject to some level of automated management. And because a great deal of the management interfaces and techniques are almost identical, the tools allow some overlap and extension.

Let's consider a very common example: disabling automatic logon for Windows computers. Most organizations have a standard for servers that disables automation logon to ensure that only administrators log on to the system. The user-centric control for this setting is within Control Panel. But all this control does is change a registry value:

```
Location: \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon
Name: AutoAdminLogon
Value: 0=disable, 1=enable
```

This type of configuration change and enforcement is what performance management tools already do. They can usually be configured to set registry values like this and monitor for unauthorized changes.

That last point is actually a big differentiator. There are a number of solutions in the IT space that enable server configuration automation. But many of them have limited reporting and monitoring capabilities. Although these configuration monitoring techniques may not be central to performance management (performance monitoring is far more important than configuration monitoring in that space), security management absolutely relies on auditing including configuration monitoring, reporting, and change-control alerting.

How Do I Audit With These Tools?

Audit reports are critical to any organization impacted by government or industry compliance regulations. Most likely, your industry is impacted by one or more regulations, no matter where you work. And in the regulatory compliance space, proving consistent compliance with policy is often more important to an auditor than the policy itself.

This is where performance management tools really shine. They are spectacular at monitoring system configuration over time and providing reports of virtually any detail level. This is a result of the deep integration mentioned earlier, and the flexible reporting framework that the tools provide.

> **Auditing Without Configuration Management**
>
> You should remember that using a performance management solution for system auditing can be done without using the same system for configuration. So if you use, for example, Group Policy to configure your Windows systems, you can still use these tools to audit that configuration. It is often easier to use the same tool for both tasks, but you're not restricted to that approach.

There are typically two ways to audit security with performance management tools. The preferred method is to use *built-in security analysis* functionality or a vendor-supplied add-on to report on security compliance. Many vendors supply a combination of customizable configurations and audit reports that validate the settings you choose. These can be changed to suit your specific security requirements and then deployed simply and reliably.

The other method is to use *custom scripts* to apply and validate configurations. These scripts are often written in configuration-oriented languages such as PowerShell. Many can be found on the Internet as samples or nearly-complete examples. If your performance management solution doesn't have security management available as a vendor-supplied option, you can almost certainly extend it to this task with custom scripting that applies and verifies the security configuration.

Summary

Performance management and monitoring tools are amazingly flexible pieces of engineering. They perform their intended tasks very well, usually with little overhead and simplified administration. These powerful tools can also be repurposed to apply and report on security configurations. And using an existing technology in a new way like this can help many organizations get more bang for their existing IT buck.

When you consider your IT security needs, remember that auditing is a key requirement for most organizations. If your performance management solution can be extended to report on, and enforce, audit requirements, your annual audit process will be far less painful.