Windows Server 2003 Security Guide v2.1 Release Notes

April 26, 2006

MSCG-001R-2003-RN

Contents

---

1. Windows Server 2003 Security Guide Download

- Download Center: http://go.microsoft.com/fwlink/?linkid=14846
- TechNet online: http://go.microsoft.com/fwlink/?linkid=14845

---

2. Changes in This Version

Version 2.1 corrects some errors in the tools and templates, which accompany this guide, and updates some links and minor typographical errors in the guide. The *Optional-File-Permissions.inf* in the Security Template files has been updated. Some registry settings and registry paths have been updated in the security template .INF files. In chapters 4 and 5, the Local Service account has been granted the 'Change the System Time' user right in some of the baseline policy security templates. In chapter 11 the default algorithm for EFS has been updated in line with new product and service pack releases.

Version History

Version 2.0 provides specific recommendations about how to harden computers that run Microsoft Windows Server 2003 with Service Pack 1 (SP1) in three distinct enterprise environments—one in which older operating systems such as Windows NT 4.0 and Windows 98 must be supported, one in which Windows 2000 is the earliest version of the Windows operating system in use, and one in which concern about security is so great that significant loss of client functionality and manageability is considered an acceptable tradeoff to achieve maximum security. These three environments are respectively referred to as the Legacy Client (LC), Enterprise Client (EC), and Specialized Security – Limited Functionality (SSLF) environments throughout this guide.

Guidance about how to harden computers in these three environments is provided for a group of distinct server roles. The countermeasures that are described and the tools that are provided assume that each server will have a single role. If you need to combine roles for some of the servers in your environment, you can customize the security templates that are included in the downloadable version of the guide to create the appropriate combination of services and security options. The server roles that are referenced in this guide include the following:

- Domain controllers that also provide DNS services
- Infrastructure servers that provide WINS and DHCP services
- File servers
- Print servers
- Web servers that run Microsoft Internet Information Services (IIS)
- Internet Authentication Services (IAS) servers
- Certificate Services servers
- Bastion hosts

The tools for hardening Windows Server 2003 computers have been updated. The security templates provided in previous versions of this guide contained information to configure specific system services. This service configuration is now done by the Security Configuration Wizard (SCW), which is a component of Windows Server 2003 with Service Pack 1. The corresponding service configuration information is not included in this guide. Detailed instructions on using the SCW and configuring services with it are provided in Chapter 2.

Version 1.3 corrected permissions on System Services in the Security Templates. Changes were also made to "Removable Storage Service Start-up Mode to Manual" section in Chapter 3, and "IPSec Filters for Domain Controllers" section in Chapter 4. The explanation of the "Background Intelligent Transfer Service (BITS) Server Extension" in Chapter 8 was clarified.

Version 1.2 updated several URLs and the title pages. Changes were also made to the "Domain Controller IPSec Guidance" section in Chapter 4, and the "Hardening IAS Servers Overview" section in Chapter 9.

Version 1.1 added some bookmarks to the PDF files to make it easy to locate specific chapters or sections of the content.

Version 1.0 of the Windows Server 2003 Security Guide. This was the first version of this guide, released on Thursday, April 24th, 2003.

---

3. Unresolved Issues and Resolutions - Managing Bastion Hosts After Lockdown

Ensure that the bastion hosts and the High Security - Bastion Host.inf security template are configured to enable the functionality your environment requires before applying the security settings. The recommended configuration included in this guide disables many system services, making it very difficult to manage or reconfigure bastion hosts that have been locked down. For example, the Windows Installer service is disabled, making it impossible to reconfigure a bastion host using the Add or Remove Programs applet in Control Panel. Administrators can work around some of these limitations by temporarily enabling and restarting services as required. Restart the bastion host after completing any management tasks to ensure the Bastion Host Local Policy (BHLP) takes effect.

---

4. Copyright and license agreement