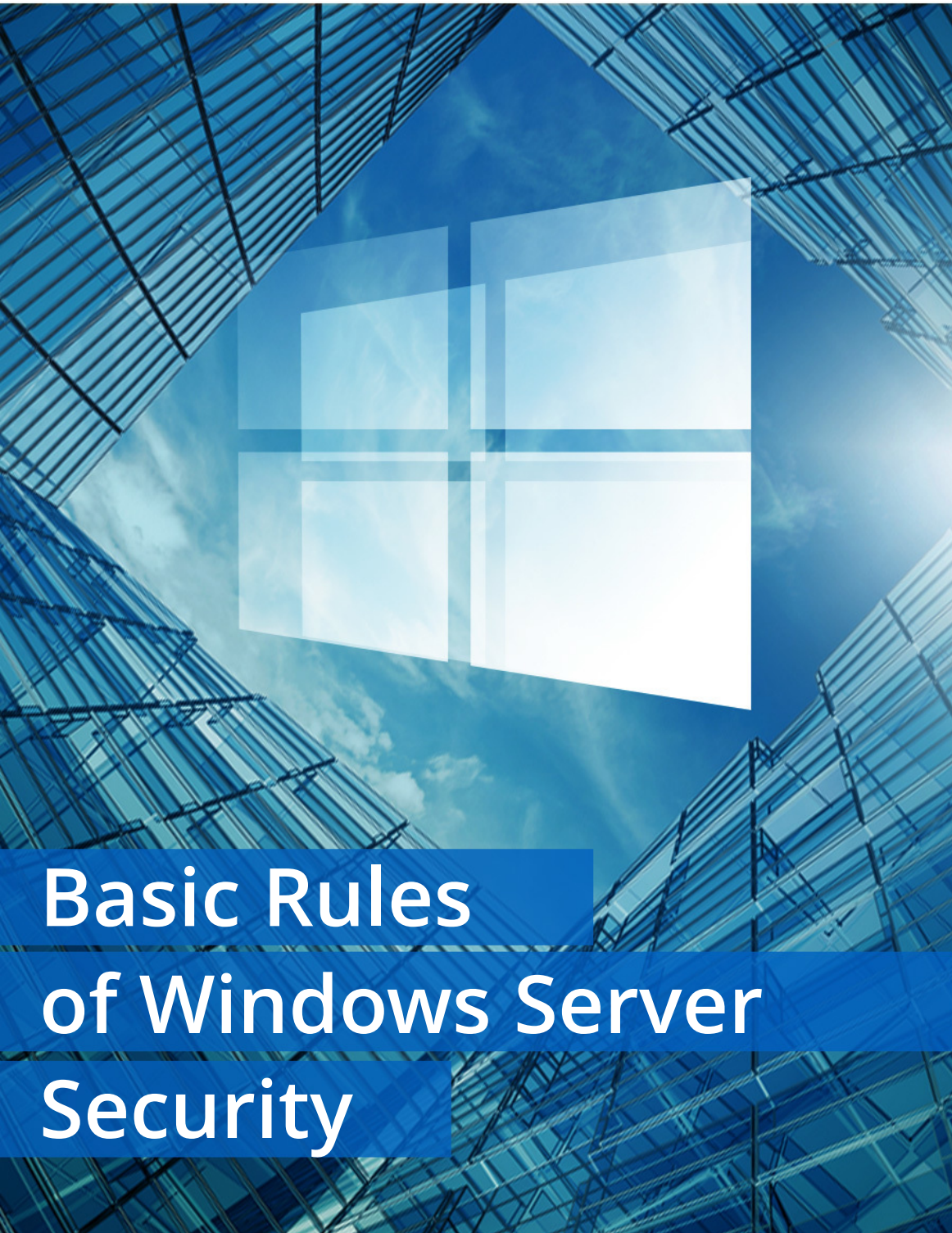


May 2015

netwrix

SysAdmin Magazine



Basic Rules of Windows Server Security

Security News:

PCI DSS v3
Implementation
Hurdle

Top Tips for Windows Server Security

Useful How-tos for Windows Server

PowerShell
to Secure
Windows Server

Quick Reference Guides:

Windows Server Auditing
DNS Auditing

Contents

3 **Basic Rules of Windows Server Security**
by Russell Smith

5 **Ten Simple Ways to Prevent Security Breaches in Windows Server 2012**
by Krishna Kumar

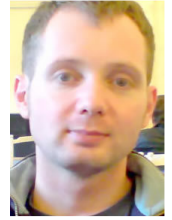
8 **PCI DSS v3's Number One Implementation Hurdle**
by John O'Neill Sr.

11 **Windows 10 Technical Preview: New Security Features**
by Krishna Kumar

13 **How to Detect Who Created a Scheduled Task on Windows Server**

- 15** [How to Detect Unauthorized Software Installation on Windows Server - Who? What? When?](#)
- 17** [Monitoring Event Logs with PowerShell](#)
by Russell Smith
- 19** [Secure PowerShell Remoting Using Constrained Endpoints](#)
by Russell Smith
- 22** [Quick Reference Guide: Windows Server Auditing](#)
- 23** [How to Monitor Deletion of DNS Records](#)
- 24** [Quick Reference Guide: Exchange Server Auditing](#)

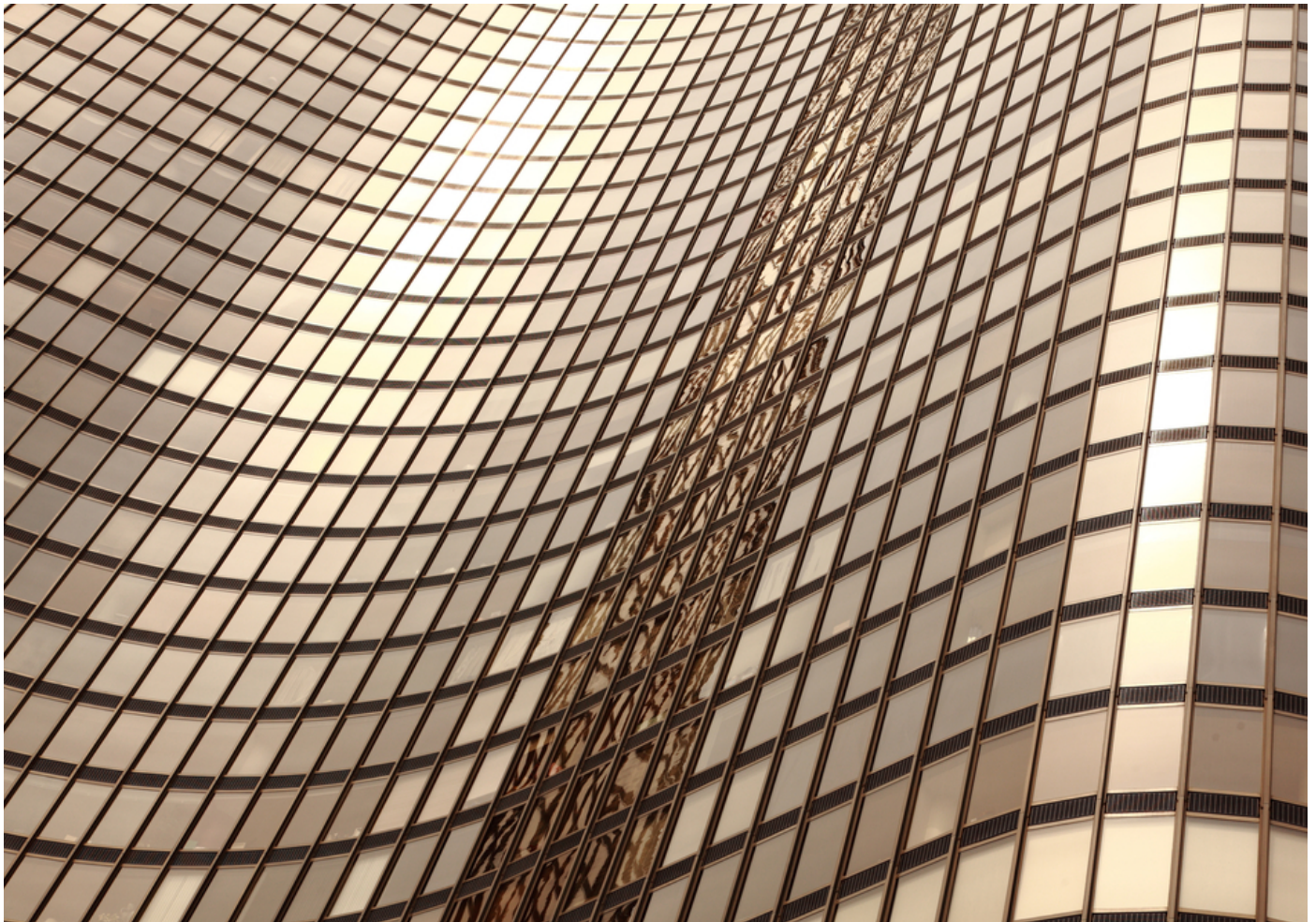
Basic Rules of Windows Server Security



by Russell Smith

Specializing in the management and security of Microsoft-based IT systems, Russell is the author of a book on Windows security and a contributing author and blogger.

While Windows Server is considered to be secure out-of-the-box, like any part of your IT infrastructure, it needs to be patched, monitored and configured in an ongoing effort to ensure that it isn't left exposed to attack. Let go through some of the tools and best practices that can help you keep Windows Server protected.



Configure Baseline Security

To keep the attack surface to a minimum, Windows Server's modular design allows you to add server roles and features as required. Nevertheless, Windows Server is configured to provide interoperability and backwards compatibility with legacy systems out-of-the-box, and though this is convenient and makes Windows Server easier to use, it can leave systems vulnerable.

Small businesses that have limited IT resources can use the Security Configuration Wizard (SCW) to lock down Windows Server. SCW is installed by default in Windows Server 2012 R2, and can be found on the *Tools* menu in Server Manager. The wizard creates security policies based on a series of questions you answer about your server, which then can be applied to the local device, or converted to a Group Policy Object (GPO) and used to configure one or more servers if you have Active Directory.

Windows Server is configured to provide interoperability and backwards compatibility with legacy systems out-of-the-box, and though this is convenient and makes Windows Server easier to use, it can leave systems vulnerable.

Microsoft's free Security Compliance Manager (SCM) tool comes bundled with a series of templates for securing Windows Server and client devices. SCM gives administrators more control over the settings applied than SCW, and allows you to create custom security baselines, and compare settings between templates.

Separate Administrative Duties and Least Privilege Security

Virtualization technologies make it easier than ever to separate out server roles, so you should make sure that domain controllers don't host other server roles or applications, and are never used to perform everyday administration tasks. Installing server roles and applications on separate servers gives you more control over

administrative privileges, and helps to improve security by ensuring access to critical systems can be appropriately restricted.

In a similar vein, domain administrator accounts should only be used where absolutely necessary. Using domain administrator accounts to manage workstations for example, makes it considerably easier for an attacker to get access to those credentials, at which point you can consider your entire Windows infrastructure owned.

Auditing solutions provide critical and detailed information about who changed what, when and where, and includes "before" and "after" configuration data so you can easily understand what has changed.

Monitoring and Auditing

Windows Server has built-in tools for monitoring and auditing, such as Event Viewer and some handy PowerShell cmdlets. While using custom views in Event Viewer is useful for getting an overview of server events, and PowerShell an option if you have the time and resources to create your own solution, the best way to ensure that Windows Server stays secure, and to monitor configuration changes, is to deploy a third-party change auditing solution. Auditing solutions provide critical and detailed information about who changed what, when and where, and includes "before" and "after" configuration data so you can easily understand what has changed. Reporting features allow you to easily understand the changes that are occurring across your Windows Server estate, including applications such as Active Directory and Exchange, and in different easy-to-read formats using pre-configured reports included with the software, so that you can get started quickly. They also go beyond the auditing capabilities native to Windows Server to help better secure your systems by pulling information from a wider variety of sources, and have extra features such as user activity video recording.

Ten Simple Ways to Prevent **Security Breaches** in **Windows Server 2012**



by Krishna Kumar

10+ years in IT Industry specializing in
designing, implementation and
administration

Windows Server is one of the most commonly deployed critical systems in the organization. Most of the applications used in the organization are also Windows based, plus there are other legacy applications built on these Windows platforms. Since these servers are used the most, they need to be configured with tight security. The latest ones, Windows Server 2012 and Windows Server 2012 R2 have some great security features and improvements to protect from security threats and vulnerabilities. These features need to be implemented and configured to prevent against any kind of security breaches occurring in the environment. Given below are ten simple ways to prevent security breaches in Windows Server 2012.



1. Microsoft Security Assessment Tool

Microsoft Security Assessment Tool is a free tool which helps identify and assess security threats providing the guidelines for minimizing risks quickly and efficiently. This single tool can run across the complete environment like a PC server, database or other heterogeneous environment. It has 'a set of hundred questionnaires' which helps understand the security strategy and uses best practices to give the most appropriate recommendations.

2. Microsoft Security Baseline Analyzer

Microsoft Security Baseline Analyzer helps scan the local and remote systems with eight categories of effectiveness, trustworthiness and reliability. It assists with categories such as security, performance, configuration, policy and operation, pre-deployment, post-deployment and other prerequisites. It scans the system for all the defined categories and searches to match the best practice rule specified in the Microsoft Security Baseline Analyzer. It looks into the system recommendations with Error, Warning and Information. Errors are returned when their conditions do not match. Warnings are returned when the conditions are matched at 50-80% and when they are not fixed leading to the error situation. Similarly, information is returned when the conditions are satisfied with the best practice rule.

Microsoft Security Assessment Tool has 'a set of hundred questionnaires' which helps understand the security strategy and uses best practices to give the most appropriate recommendations.

3. Microsoft Security Compliance Manager

Microsoft Security Compliance Manager is a

great tool which helps in deploying, configuring and managing computers in your environment using Group Policy and Microsoft System Center Configuration Manager (SCCM) with Microsoft Security Guide recommendations and industry best practices. It allows configuring computers running from the latest version to the legacy version of Windows Server, Windows client, Microsoft Office applications and Windows Internet Explorer.

Security auditing allows the administrator to monitor various activities on the servers such as user activities, forensic analysis, regulator, compliance, troubleshooting, etc. through audit logs.

4. Active Directory Rights Management (AD RMS)

Active Directory Rights Management can be implanted to protect the documents, presentations, workbooks and other sensitive information from being forwarded, copied, and printed; also, it protects data from leaking. Documents are protected using Information Rights Management, permissions are provided down to file level and these permission are stored in the file itself. Hence, no matter where, when and how a file is been stored and accessed, the appropriate permission restrictions are applied to the file.

5. Applocker

Applocker prevents users from installing and using any unauthorized / unlicensed / outdated applications on the servers to avoid huge damage to the performance and security of the application and save huge amount of administrator's efforts on fixing. Protecting these applications reduces security risks and increases performance.

6. Bitlocker

Bitlocker is a built-in feature to provide full disk encryption and protect against any kind of disk or removable devices data theft. Disk failures are inevitable, but you can extract data from a failed disk. Hence, it is highly recommended to implement Bitlocker and use it on servers which have sensitive information. Bitlocker can be implemented on both physical and – with some additional configuration – virtual machines.

7. Security Auditing

Security auditing allows the administrator to monitor various activities on the servers such as user activities, forensic analysis, regulator, compliance, troubleshooting, etc. through audit logs. Audit log helps monitoring any unusual activities or intruder attempts to gain access. Other forensic attempts are also logged, which allows administrators to take action immediately. These auditing logs can be kept for a while, until you need to analyze some abnormal user activity in the past.

8. Smart Cards

With the increased number of internet application and cloud-based systems, Smart cards help implement a two-factor authentication using the personal identification number (PIN). This reduces the chances of unauthorized access to the organizational network. Smart cards provide effective protection with a secured remote system access, data signing and data encryption. Implementing smart cards can be expensive for some organizations; however, this can be solved by using virtual smart cards. A user can be granted more than one virtual smart cards.

9. Encrypting File System (EFS)

Encrypting File System allows users to encrypt the information on the hard disk with NTFS file system so that data stays secure. EFS is enabled by selecting the check box on the file or folder properties and also allows users to control access permissions. Even though you encrypt files and folders, it is recommended to apply this settings on the folder level and inherit the properties to the files and folders inside it.

10. Windows Firewall

Enabling Windows firewall helps protect the server against unauthorized incoming and outgoing network traffic. It reduces the risk of network security threats and protects database from unauthorized access. Windows Server 2012 supports IKEv2 for IP sec Transport mode; with this feature another machine operating system using IKEv2 will be able to provide end-to-end transport security. Windows 2012 firewall also supports Windows Store app network isolation. This allows developers to customize Windows firewall configuration in order to isolate the network access to the new Windows store apps running in the system.

Hopefully, these recommendations will help you keep the environment properly secured and protect the system from any kind of vulnerabilities or threats. I would also recommend you to make sure to keep antivirus software updated; keep limited access to the Internet; and allow only authorized software to be installed on the servers.

Want to read more articles like this?
Subscribe to our blog:
blog.netwrix.com

PCI DSS v3's Number One Implementation Hurdle



by John O'Neill Sr.

20+ years in IT, consultant, architect, executive, speaker, and author

Security for organizations dealing with credit cards often boils down to one thing; successful implementation of The Payment Card Industry Data Security Standard, better known as PCI DSS. From securing transactions to increasing customer confidence, PCI DSS compliance is a must in the modern economy. The PCI DSS standard version 3.0 requirements became effective January 1, 2015. While v3 has many changes, one is more impactful, and more challenging to implement, than all the others.



Given the evolution of security threats, network penetration testing is more important than ever. PCI DSS v3 clearly recognizes this fact with significant revisions to penetration testing requirements. Penetration testing must now comply with recognized industry standard testing methodologies, such as those developed by the National Institute of Standards and Technology. NIST, a branch of the US Department of Commerce, publishes clear rules for penetration testing in their "Technical Guide to Information Security Testing and Assessment."

Penetration testing ensures the cardholder data environment, or CDE, is completely isolated and protected from an organization's other networks. Perfectly sensible, since no good will come from cardholder information being shared openly on the same network as office email, Internet browsing, and a thousand other apps. The problem is, for many organizations at least, complying with PCI DSS v3's new penetration testing requirements will be quite difficult.

The difficulty is in the details. Penetration testing skills are specialized, demanding significant training and experience. Many organizations trying for PCI DSS v3 compliance are small, with small IT teams and smaller IT budgets. These organizations certainly don't have in-house, industry standard penetration testing skills. Contracting the work is straightforward, but expensive, straining those limited IT budgets. In all cases, these organizations have a hurdle to jump in achieving compliance.

While training on staff IT admins to perform penetration testing may sound appealing, it's not viable. As I mentioned, penetration

testing is highly skilled. These skills can't be force-fed like broccoli to a toddler. They are cultivated over time. IT teams in small organizations are almost stereotypically overextended. Resources just aren't available to bring these testing skills in-house. Outsourcing, as expensive as it may be, is really the only viable option.

A few words of caution; don't throw good money after bad chasing PCI DSS v3's penetration testing compliance requirement. Meticulously select the testing provider. Ensure, in writing, that they perform testing to recognized industry standards for penetration testing. Have them document those standards. Manage expectations by clearly defining, again in writing, that penetration testing isn't the goal. The goal is testing resulting in compliance with PCI DSS v3 section 11.3's requirements. Ask if the final report contains a PCI DSS v3 certification compliance statement.

While penetration testing requirements aren't the only revisions in PCI DSS v3, they pose some of the most significant challenges. Because of these challenges, smaller organizations will struggle climbing the mountain that is PCI DSS v3 compliance. They will summit that mountain with determination, management skill, and key partnerships.

Want to read more articles like this?

Subscribe to our blog:
blog.netwrix.com

#completevisibility of Your Windows Server

Introducing Netwrix Auditor for Windows Server



Capture
Every Windows Server Change



Store
Audit Data Efficiently



Report
Who, What, When, Where



Get
Complete Visibility

Learn More: netwrix.com/go/completevisibility

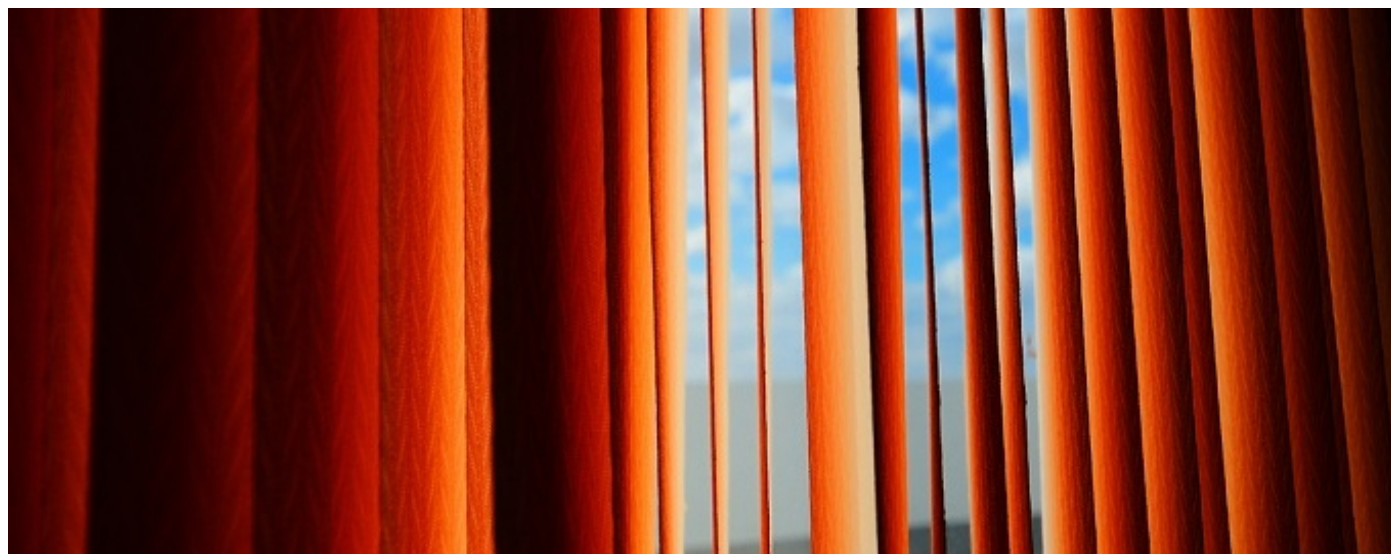
Windows 10 Technical Preview: New Security Features



by Krishna Kumar

10+ years in IT Industry
specializing in designing,
implementation and
administration

Windows 10 is the latest client Operating system released by Microsoft, the technical summary of its latest security features is available for download. High hopes have been pinned on Windows 10, since Windows 8, its previous version, was kind of a let-down in the market. Following in the steps of the previous version, Windows 10 will give you the same experience on both workstation and mobile device. The fact that everything now is cloud ready opens the gates for more security breaches. Microsoft has made sure to provide some great advanced features to overcome some of the modern security threats and to avoid data loss.



1. Multi Factor Authentication

Windows 10 offers a new inbuilt Multi Factor Authentication, which helps administrators protect user systems by integrating user credentials with a pin through mobile devices or biometric readers: with Windows 10, various biometric devices are supported. With a single-step authentication, it is quite easy for hackers to break in and take control of the machine stealing data with a couple of clicks. But due to the dual-factor authentication which is quite complex, hackers are going to have a hard time breaking into a system or getting past biometrical security.

2.

Data Protection

User's client machines can contain business critical information and many organizations deploy or configure Bitlocker for the clients to encrypt the disks on local machines. This helps protect data, but not much can be done once the data leaves client machines. To address this issue, Windows 10 offers data loss prevention (DLP) to protect the files, which is quite transparent to the users, as they don't have to change their working style. In fact, they don't even have to switch apps or modes to protect their corporate data. Windows 10 automatically encrypts corporate apps, data, email, website content and other sensitive information, because it reaches a device from corporate network locations. Users can also choose to differentiate between corporate and personal data in order to encrypt and protect just one kind of data.

3.

Hardening Clients

Windows 10 provides another option to protect users from security breaches. Only trusted apps can run on client machines. Organizations can decide which apps should be installed. With this security feature, users cannot install any third-party application that is not signed and which could cause potential threat to the organizations.

4.

Mobile Device Protection

Remote or sales team hardly come to office and they mostly use VPN to connect from their mobile devices like tablets etc. There is always a potential risk associated with their connection to office via VPN. Windows 10 provides an option of custom specification of allowing or denying access to apps when VPN connection is used. This enhances the security and also protects organizations from various threats, particularly when they use the BYOD model.

5.

Protection from Phishing Attack

In Hyper-V environment, whenever a user is authenticated with Active Directory domain controller, a token is generated and this token is used to access resources. If this token is compromised, hackers can easily access resources without any authentication. Windows 10 helps avoid these kinds of phishing attacks by storing user access tokens inside a secure container. With this solution, hackers will not be able to extract the token, even if the Windows kernel is compromised.

Windows 10 is the next generation client operating system with some cool new features and experience for the users. Looks like, once the final version of Windows 10 is released and adopted, organizations will move towards highly secured environment.

How to Detect Who Created a Scheduled Task on Windows Server

New scheduled tasks created on Windows Server by someone who doesn't belong to your IT department might indicate a virus attack, which could result in a sensitive data leakage. In order to reduce this risk, it's necessary to monitor creations of scheduled tasks in real time.



1. Run `eventvwr.msc` > Windows Logs > Right-click "Security" log > Properties: Make sure the "Enable logging" check box is selected. Increase the log size for at least 1gb.
2. Set retention method to "Overwrite events as needed".
3. Open Event viewer and search the application log for the 4698 event ID with to find latest created scheduled tasks.

4. In order to create instant alert after every scheduled tasks creation you need to edit the following PowerShell script by setting your parameters up and save it as detectst.ps1 for example (follow comments):

```
$Subject = "New Scheduled Task Has Been Created" # Message Subject
$Server = "smtp.server" # SMTP Server
$From = "From@domain.com" # From whom we are sending an e-mail(add anonymous logon permission
if needed)
$To = "To@domain.com" # To whom we are sending
$Pwd = ConvertTo-SecureString "enterpassword" -AsPlainText -Force #Sender account password
#(Warning! Use a very restricted account for the sender, because the password stored in the script will be
not encrypted)
$Cred = New-Object System.Management.Automation.PSCredential("From@domain.com" , $Pwd) #Sender
account credentials
$encoding = [System.Text.Encoding]::UTF8 #Setting encoding to UTF8 for message correct display
#Powershell command for filtering the security log about created scheduled task event
$Body=Get-WinEvent -FilterHashtable @{LogName="Security";ID=4698;} | Select TimeCreated,
machinename, @{{n="Task Creator";e={{[xml]$_}.ToXml().Event.EventData.Data | ? {$_.Name -eq
"SubjectUserName"} | %{$_.'#text'}}},@{{n="Scheduled Task
Name";e={{[xml]$_}.ToXml().Event.EventData.Data | ? {$_.Name -eq "TaskName"} | %{$_.'#text'}}} |
select-object -first 1
#Sending an e-mail.
Send-MailMessage -From $From -To $To -SmtpServer $Server -Body "$Body" -Subject $Subject -Credential
$Cred -Encoding $encoding
```

5. Run "Task Scheduler" > Create new schedule task > Enter its name > Triggers tab > New trigger > Set up the following options:
 - Begin the task on an event
 - Log – Security
 - Source – Blank
 - EventID – 4698.
6. Go to the "Actions" tab > New action with following parameters:
 - Action – Start a program
 - Program script: PowerShell
 - Add arguments (optional): – File "filepath to our script"
 - Click "OK".
7. Now you will be notified about every scheduled task created on your windows server via e-mail that will contain scheduled task creation time, name, computer name on which this task was created and the name of the creator.

See Real-Life Use Cases: netwrix.com/go/scheduled_task_creation

How to Detect Unauthorized Software Installation on Windows Server – Who? What? When?

Suspicious software on your Windows Server may be the result of an unauthorized installation by your own employee or originate from a hackers' attack. Any suspicious software can potentially cause leakage of sensitive data, not to mention server performance slowdown or infringement of compliance policies. That is why it is vital to be aware of any occurrences of software installation and see what was installed, who did it and when – shortly after it happened.



1. Run eventvwr.msc > Windows Logs > Right-click "Application" log > Properties:
 - Make sure the "Enable logging" check box is selected
 - Increase the log size for at least 1 GB
 - Set retention method to "Overwrite events as needed" or "Archive the log when full"
2. Open Event Viewer and search the application log for the 11707 event ID with MsiInstaller Event Source to find the last installed software.

3. To create an instant alert that is triggered upon any software installation, you need to edit the following PowerShell script by setting up your parameters and saving it everywhere as a .ps1 file (e.g., detect_software).

```
$Subject = "New Software Has Been Installed" # Message Subject
$Server = "smtp.server" # SMTP Server $From = "From@domain.com" # From whom we are sending an
e-mail (add anonymous logon permission if needed)
$To = "To@domain.com" # To whom we are sending
$Pwd = ConvertTo-SecureString "enterpassword" -AsPlainText -Force #Sender account password
#(Warning! Use a very restricted account for the sender, because the password stored in the script will
be not encrypted)
$Cred = New-Object System.Management.Automation.PSCredential ("From@domain.com" , $Pwd)
#Sender account credentials
$encoding = [System.Text.Encoding]::UTF8 #Setting encoding to UTF8 for message correct display
#Powershell command for filtering the security log about created user account event
$Body=Get-WinEvent -FilterHashtable
@{LogName="Application";ID=11707;ProviderName='MsiInstaller'} | Select TimeCreated, Message,
UserID | select-object -first 1 #Sending an e-mail. Send-MailMessage -From
$From -To $To -SmtpServer $Server -Body "$Body" -Subject $Subject -Credential $Cred -Encoding
$encoding
```

4. Run "Task Scheduler" > Create new schedule task > Enter its name > Triggers tab > New trigger > Set up the following options:

- Begin the task on an event
- Log – Security
- Source – Blank
- EventID – 4698

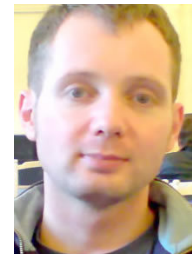
5. Go to the "Actions" tab > New action with following parameters:

- Action – Start a program
- Program script: PowerShell
- Add arguments (optional): – File "filepath to our script"
- Click "OK"

6. Now you will be notified about every scheduled task created on your windows server via e-mail that will contain scheduled task creation time, name, computer name on which this task was created and the name of the creator.

See Real-Life Use Cases: netwrix.com/go/software_installation_ws

Monitoring Event Logs with PowerShell



by Russell Smith

Specializing in the management and security of Microsoft-based IT systems, Russell is the author of a book on Windows security and a contributing author and blogger.

A routine sysadmin task that PowerShell lends itself to is parsing data and text files, and the Windows event logs use XML formatted information that can be easily parsed using the `Get-EventLog` and `Get-WinEvent` PowerShell cmdlets. In this article I'm going to show you how to get started using PowerShell to parse the event logs, and explain the differences between the two cmdlets to make the event log monitoring easier for you.



Get-EventLog vs. Get-WinEvent

`Get-EventLog` was the first PowerShell cmdlet that Microsoft included in Windows to facilitate working with the event logs. As of PowerShell v2.0, the `-ComputerName` parameter was added so that it could also be used to query the logs on remote computers. But `Get-EventLog` has some limitations that led to the introduction of `Get-WinEvent` in PowerShell version 2. `Get-EventLog` only works against the System, Application, and Security logs, and not the new ETL logs (Event Trace Logs) that were introduced with *Event Tracing for Windows* (ETW) in Windows 7, which contain information from a much wider variety of sources than the traditional logs that have been present since the days of Windows NT.

The `Get-EventLog` cmdlet doesn't allow the returned results to be filtered directly, which means that the

dataset must be parsed by piping the results to the `Where-Object` cmdlet for further processing. This might not be too much of a problem if you only want to work with the logs on the local machine, but can become a problem when querying remote computers, as the logs need to be transferred across the network before they can be parsed, which takes extra time and generates unnecessary network traffic if the logs are quite large.

Therefore, if you really want to return the entire contents of a log, and don't need to work with it further, using `Get-EventLog` is an option, but `Get-WinEvent` was developed to address the shortcomings of `Get-EventLog`, is equally capable of returning entire logs, and going forwards is likely the cmdlet that Microsoft will support for working with the event logs.

```

PS C:\Users\Russell> Get-WinEvent -LogName 'Microsoft-Windows-BitLocker/BitLocker Management' -MaxEvents 10

ProviderName: Microsoft-Windows-BitLocker-API

TimeCreated              Id LevelDisplayName Message
-----
28/08/2014 20:32:10      782 Information The BitLocker protected volume E: was unlocked...
26/03/2014 22:10:33      782 Information The BitLocker protected volume E: was unlocked...
25/03/2014 16:32:17      782 Information The BitLocker protected volume E: was unlocked...
24/03/2014 11:27:25      782 Information The BitLocker protected volume E: was unlocked...
22/03/2014 15:38:25      782 Information The BitLocker protected volume E: was unlocked...
21/03/2014 09:56:55      782 Information The BitLocker protected volume E: was unlocked...
12/02/2014 20:11:33      778 Warning The BitLocker volume C: was reverted to an unprotected state.
12/02/2014 20:11:32      770 Warning BitLocker decryption was started for volume C:.
12/02/2014 06:00:11      782 Information The BitLocker protected volume E: was unlocked...
26/12/2013 11:29:31      782 Information The BitLocker protected volume D: was unlocked...

PS C:\Users\Russell>

```

PowerShell Event Log Basics

Let's start by returning the entire contents of an event log using *Get-WinEvent*. Open a PowerShell prompt, type the command line below and press ENTER.

```
Get-WinEvent -LogName application
```

This will output the entire contents of the *Application* log to the CLI. In practice, it's likely that you'll only want to see the most recent events, and the easiest way to do that is by adding the *-MaxEvents* parameter:

```
Get-WinEvent -LogName application -MaxEvents 10
```

The above command line displays the last ten events recorded in the *Application* log. *Get-WinEvent* can be used to parse the ETL logs, but you need to find the log name first. To list all the available logs, use:

```
Get-WinEvent -ListLog *
```

And then look for the desired log name, for example, the *BitLocker Management* log can be returned using the command below. Note that apostrophes are required at the top and tail of the log name because it includes a space:

```
Get-WinEvent -LogName
'Microsoft-Windows-BitLocker/BitLocker
Management' -MaxEvents 10
```

You can also get detailed information about a specific log as shown here by adding the *Format-Listcmdlet*:

```
Get-WinEvent -ListLog
'Microsoft-Windows-BitLocker/BitLocker
Management' | Format-List -Property *
```

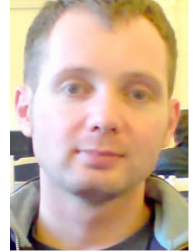
If you want to perform any of the above tasks on a remote computer, just add the *-ComputerName* parameter, followed by the computer name:

```
Get-WinEvent -ListLog
'Microsoft-Windows-BitLocker/BitLocker
Management' -ComputerName contososrv1 |
Format-List -Property *
```

Don't forget that you must hold the necessary permissions to read the desired log, whether it's on the local computer, or a remote device.

Want to read more articles like this?
 Subscribe to our blog:
blog.netwrix.com

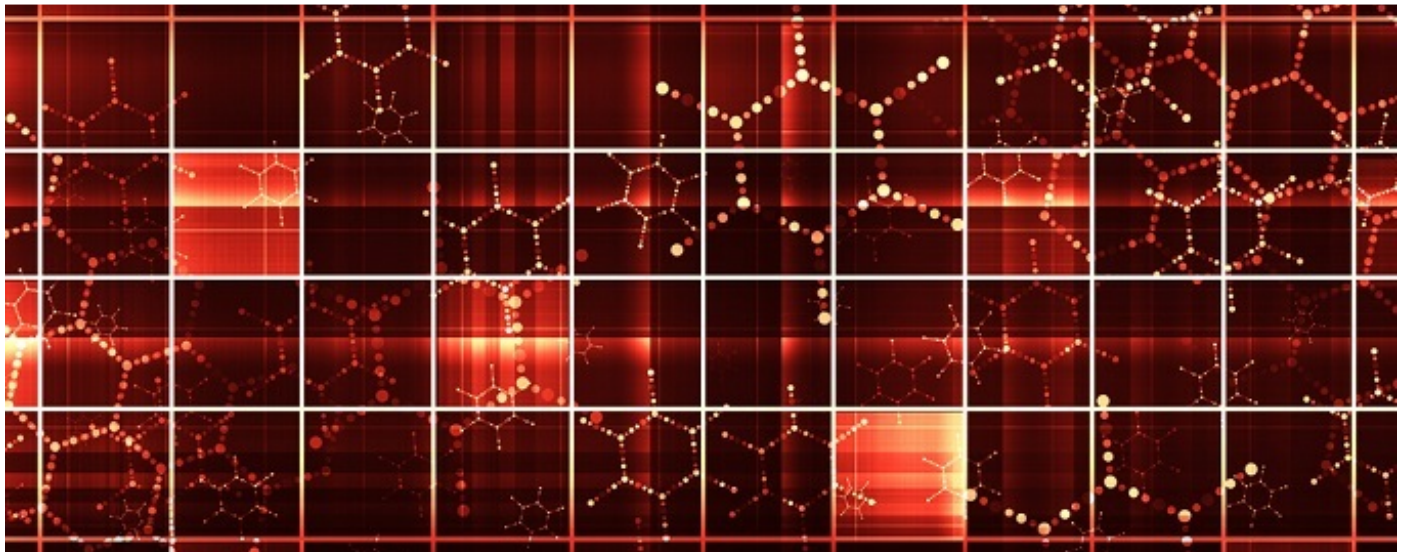
Secure PowerShell Remoting Using Constrained Endpoints



by Russell Smith

Specializing in the management and security of Microsoft-based IT systems, Russell is the author of a book on Windows security and a contributing author and blogger.

PowerShell Remoting is enabled in Windows Server 2012 (and later) out-of-the-box, and while many IT shops see this as a potential security risk, PowerShell is in fact one of the most secure ways to administer servers if best practices are followed. In this article, I'm going to show you how to configure Windows Server 2012 R2 to accept remote PowerShell connections from a specific group of users, and how to restrict the cmdlets that can be run.



What are Constrained Endpoints?

Remote endpoints determine the users that can connect to a device with PowerShell Remoting, as well as what they can do once authenticated. The default PowerShell endpoint allows users that are members of the built-in *Administrators* and *Remote Management Users* group to connect

remotely and exposes all available cmdlets and functions on the device.

The good news is that you can create your own *constrained* endpoints and restrict what users can do, allowing you to minimize the risks of allowing PowerShell Remoting for administration purposes.

Create Constrained Endpoints in Windows Server 2012 R2

Let's create our own constrained endpoint in Windows Server 2012 R2. Log in with local administrator privileges, and click the blue PowerShell icon on the desktop taskbar.

To see the existing endpoints on the server, type *Get-PSSessionConfiguration* in the PowerShell prompt and press *ENTER*. In the PowerShell console, you should see the four default endpoints.

To restrict the cmdlets and functions that a user can execute when they connect to the constrained endpoint, we need to create a configuration file. In the PowerShell console, type the cmdlet shown below and press *ENTER*. *New-PSSessionConfigurationFile* creates a new configuration file called *PrintAdmin.pssc* and sets restrictions including limiting remote users to functions that are part of the *PrintManagement* PowerShell module.

```
New-PSSessionConfigurationFile - Path  
PrintAdmin.pssc - SessionType  
RestrictedRemoteServer -LanguageMode  
NoLanguage - ExecutionPolicy Restricted -  
ModulesToImport PrintManagement  
-VisibleFunctions Get-Printer
```

NoLanguage restricts users to running just cmdlets and functions, i.e. no script blocks, variables, or operators can be used. The *-SessionType* value *RestrictedRemoteServer* limits users to the following proxy functions: *Exit-PSSession*, *Get-Command*, *Get-FormatData*, *Get-Help*, *Measure-Object*, *Out-Default*, and *Select-Object*. The *Restricted* value for *-ExecutionPolicy* parameter also prevents scripts running. Note that there is also a *-VisibleCmdlets* parameter that can be used if the modules you want to import contain cmdlets.

Now that we have a configuration file, we can register a new endpoint called *Helpdesk*:

```
Register-PSSessionConfiguration -Name Helpdesk  
-Path PrintAdmin.pssc -ShowSecurityDescriptorUI
```

You'll be prompted to confirm that you want to configure the new endpoint, restart the WinRM service, and configure access permissions to the endpoint. In this example, I'm going to give a group called *Helpdesk* 'Execute (Invoke)' permission on the new endpoint. Don't forget to give the *Helpdesk* group permission to manage printers on the remote device, otherwise *get-printer* will fail.

If you run *Get-PSSessionConfiguration* again, you will be able to see the new endpoint listed.

Connect to a Constrained Endpoint

Now connect to the endpoint from a remote machine. Log in to Windows 8 with a user that's a member of the *Helpdesk* group or the group to which you assigned permissions on the endpoint. Open a PowerShell prompt and run the command below, replacing *contososrv1* with the name of the remote server:

```
Enter-PSSession -ComputerName contososrv1  
-ConfigurationName Helpdesk
```

Once connected to the remote server, the prompt will change accordingly to indicate you are working with a remote device. Type *get-command* and press *ENTER*, and you'll see the list of available functions and cmdlets are restricted by the endpoint. In this example, you're left with the 7 proxy functions allowed by the *RestrictedRemoteServer* session type and the *get-printer* function specified in the endpoint configuration file.

Want to read more articles like this?

Subscribe to our blog:
blog.netwrix.com

Top 10 Free Tools for Change Auditing and Password Management

Track changes to Active Directory, Exchange, file servers, manage passwords and troubleshoot account lockouts at absolutely no cost.

The following freeware tools can save you a lot of time and make your network more efficient – at absolutely no cost. Some of these tools have advanced commercial versions with additional features, but none of them will expire and stop working when you urgently need them.

1. Change Notifier for Active Directory
Tracks changes to Active Directory (AD) users, group memberships, OUs, permissions, and provides visibility into what's happening inside your AD.
[Free Download](#)

2. Change Notifier for Group Policy
Tracks every change made to your group policy objects (GPOs), including GPO links, audit policy, password policy, and software deployment changes, and fills major gaps found in native auditing tools.
[Free Download](#)

3. Account Lockout Examiner
Alerts on account lockouts, helps troubleshoot these events, and analyzes their potential causes. The accounts can be unlocked via Netwrix Account Lockout Examiner console or mobile device.
[Free Download](#)

4. Change Notifier for Exchange
Reports on what's happening inside your Exchange servers, and tracks both configuration and permission changes with “before” and “after” values.
[Free Download](#)

5. Password Expiration Notifier
Automatically reminds your users to change their passwords before they expire so you can avoid password reset calls. It works nicely for users who don't log on interactively and never receive standard password change reminders at logon time (e.g., VPN users).
[Free Download](#)

6. Change Notifier for File Servers
Tracks changes to files and shares permissions, detects deleted and newly-created files, and reports on file-access attempts. This freeware tool strengthens security of your Windows-based file servers.
[Free Download](#)

7. Password Manager
Allows users to reset forgotten passwords and unlock their accounts through a convenient, web-based, self-service portal and integration with the standard Windows logon procedure. The tool supports up to 100 users.
[Free Download](#)

8. Change Notifier for SQL Server
Detects changes made to your SQL Server configurations, including database creation and deletion, changes to database users, roles, and schemas. It also reports “before” and “after” values for every change, and sends daily reports showing all changes made.
[Free Download](#)

9. Change Notifier for VMware
Allows you to control changes in your virtual environments. It notifies you about changes to VMware virtual machine settings, creation and deletion of virtual machines. It also sends daily reports of all changes made in the past 24 hours with “before” and “after” values.
[Free Download](#)

10. Change Notifier for Windows Server
Alerts you about changes made to your Windows Server configurations, including installed software and hardware, services and scheduled tasks. It sends summary reports listing changes of the last 24 hours with “before” and “after” values.
[Free Download](#)



JOHN BAGLEY

Award-winning professional writer and independent consultant

Windows Server Auditing

How to enable logging of important Windows Server events in Windows event logs

Local Policy Audit Settings

Run gpedit.msc > Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy:

- *Audit account management* > Define > Success
- *Audit object access* > Define > Success

Registry-level Auditing Settings

- Run regedit.exe > HKEY_LOCAL_MACHINE > Right-click "SOFTWARE" > Permissions > Advanced > Auditing (Tab) > Click "Add" > Principal "Everyone" > Type "Success" > Applies to "This key and subkeys" > Advanced Permissions > Check "Set Value", "Create Subkey", "Delete", "Write DAC", "Write Owner" > Click "OK"
- Repeat steps above for the "HKEY_LOCAL_MACHINE\SYSTEM" and "HKEY_USERS\DEFAULT" nodes

Event Log Settings

Run eventvwr.msc > Windows Logs > Right-click "Application" log > Properties:

- Make sure the "Enable logging" check box is selected
- Set retention method to "Overwrite events as needed" or "Archive the log when full"

Repeat this operation for the "Security" and "System" event logs

Open Event viewer and search the corresponding log for the id's listed in the Event ID Reference box

For Detailed Windows Server Auditing, Try Netwrix Auditor — netwrix.com/go/ws-trial

- **Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

Event ID Reference (2003/2008 - 12)

Security Log

- 636/4732 – Local group member added
- 637/4733 – Local group member removed
- 635/4731 – Local group created
- 638/4734 – Local group deleted
- 624/4720 – User account created
- 630/4726 – User account deleted
- 639/4735 – Local group changed
- 642/4738 – User account changed
- 627/4723 – Change password attempt
- 628/4724 – User account password set
- 685/4781 – User name changed
- 567/4657,4663 – Object access attempt
- 560/4656 – Object open
- 562/4658 – Handle closed
- 602/4698, 4699, 4700, 4701, 4702 – Scheduled task created, deleted, enabled, disabled, updated

Application Log

Event Source: MsInstaller

- 11707 – Software was installed
- 11724 – Software was uninstalled

System Log

Event Source: Service Control Manager

- 7036 – Service state changed
- 7040 – Service start type changed

How to Monitor Deletion of DNS Records

IT service unavailability can be caused by many reasons, and one of them is accidental or malicious deletion of DNS records. For instance, after the deletion of Domain Controller DNS record users will be not able to log in. Deletion of SharePoint server DNS record will make internal corporate resources unavailable. Regular monitoring of DNS record deletions will help IT administrators readily respond to such incidents.

1. Run GPMC.msc > edit "Default Domain Policy" > Computer Configuration → Policies > Windows Settings > Security Settings > Local Policies > Audit Policy → go to "Properties" of Audit directory service access > Define > Success.

2. Computer Configuration > Policies > Windows Settings > Security Settings > Event Log > in "Properties" of below mentioned policies define:

Maximum security log size to 1gb
Retention method for security log to Overwrite events as needed.



3. Open ADSI Edit > Connect to Default naming context > Expand DomainDNS object with the name of your domain > System > Right click MicrosoftDNS > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and all descendant objects" > Permissions > Select the following check boxes: Write all properties, Delete, Delete subtree > Click "OK".
4. Open DNS Manager > Expand your servername > Forward Lookup Zone > Right click the zone you want to audit > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and all descendant objects" > Permissions > Select the following check boxes: Write all properties, Delete, Delete Subtree > Click "OK".
5. Look for Event ID 4662 with Object Type: dnsNode in your Security Event log in order to track DNS records deletion.

See Real-Life Use Cases: netwrix.com/go/dns_deletion



DNS Server Auditing

How to audit DNS records changes on Windows Server 2008/2012

Audit Policy Settings

- Run **GPMC.msc** (url2open.com/gpmc) > edit "Default Domain Policy" > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy > Audit directory service access > Define > Success.
- Computer Configuration > Policies > Windows Settings > Security Settings > Event Log > Define:
 - Maximum security log size to 1gb.
 - Retention method to Overwrite events as needed.

DNS Zone Auditing Settings

Run ADSI edit (url2open.com/adsi) on Domain Controller with DNS role > Connect to Default naming context > Expand DomainDNS object with the name of your domain > System > Right click MicrosoftDNS > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and all descendant objects" > Permissions > Select the following check boxes: Write all properties, Delete, Delete subtree > Click "OK".

DNS Manager Auditing Settings

Open DNS Manager > Expand your servername > Forward Lookup Zone > Right click the zone you want to audit > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and all descendant objects" > Permissions > Select the following check boxes: Write all properties, Delete, Delete Subtree > Click "OK".

Review Auditing Settings

Look for Event ID 4662 with Object Type: dnsNode in the Security Event log on DC whenever DNS record is created, modified or deleted.

For Detailed Windows Server Auditing, Try Netwrix Auditor — netwrix.com/go/ws-trial

- **Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

DNS Record Deletion Methods

- Scavenging
- Manual deletion
- When it gets a valid TTL update with TTL=0
- An LDAP delete command using interfaces such as ADSI edit or LDP

Event ID 4662 Log Content:

- Security ID
- Account Name (Who)
- Account Domain
- Object Name (What)
- Date and Time (When)
- Accesses (Action Taken)

Enable Directory Service Access Auditing in CMD

- `Auditpol /set /category:"DS Access" / Success:Enable`
- `Auditpol /set /category:"DS Access" / Failure:Enable`

Next Steps

Try #1 Change and Configuration Auditing Platform:

Free Trial: setup in your own test environment

netwrix.com/go/completevisibility

Test Drive: virtual POC, try in a Netwrix-hosted test lab

netwrix.com/go/test_drive

Live Demo: product tour with Netwrix expert

netwrix.com/go/live_demo

Contact Sales to obtain more information

netwrix.com/go/contact_sales

netwrix.com | netwrix.com/social



Corporate Headquarters: 8001 Irvine
Center Drive, Suite 820 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749
EMEA: +44 (0) 203-318-02

netwrix
#1 for change auditing