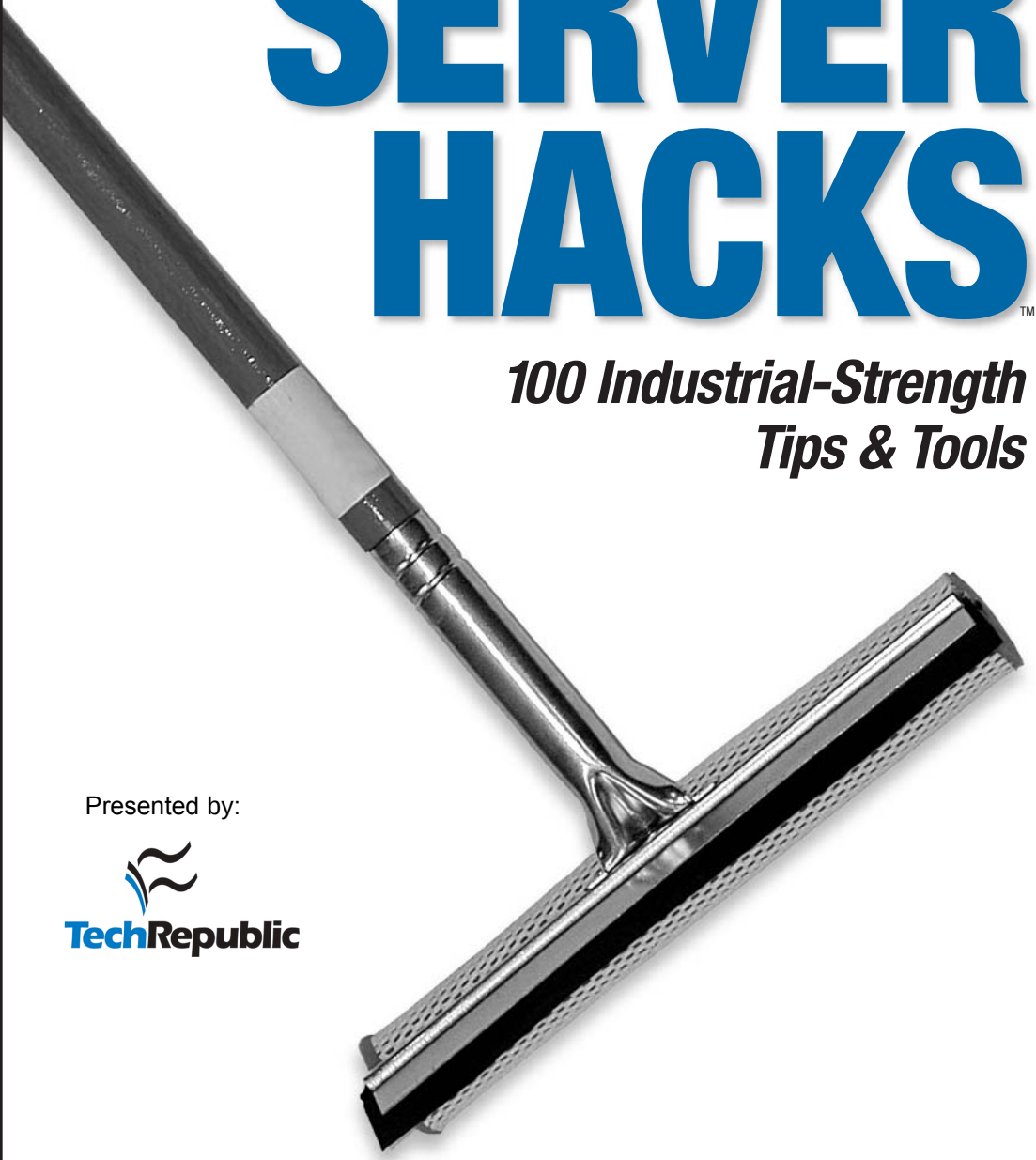
WINDOWS SERVER HACKS™

100 Industrial-Strength Tips & Tools



Presented by:

TechRepublic

O'REILLY®

Mitch Tulloch

HACK #12 Get Event Log Information

Need to check on the size and configuration settings of your event logs? Use this script instead of the GUI; it's faster!

Monitoring event logs is an essential part of an administrator's job. Unfortunately, viewing event log settings and log file sizes from the GUI is cumbersome, and it would be useful to have an easier way to obtain this information.

That's exactly what this hack is all about. You can run the script on Windows NT/2000 and later to obtain the current file size, maximum file size, and number of records, and you can overwrite settings on the Application, System, and Security logs.

The Code

Type the following script into Notepad (make sure Word Wrap is disabled) and save it with a *.vbs* extension as *loginfo.vbs*. Or, if you like, you can download the script from the O'Reilly web site.

```
Option Explicit
On Error Resume Next
Dim strMoniker
Dim refWMI
Dim colEventLogs
Dim refEventLog
Dim strSource

'moniker string stub - security privilege needed to get
'numrecords for Security log
strMoniker = "winMgmts:{(Security)}!"

'append to moniker string if a machine name has been given
If WScript.Arguments.Count = 1 Then _
strMoniker = strMoniker & "\\" & WScript.Arguments(0) & ":"

'attempt to connect to WMI
Set refWMI = GetObject(strMoniker)
If Err <> 0 Then
WScript.Echo "Could not connect to the WMI service."
WScript.Quit
End If

'get a collection of Win32_NTEventLogFile objects
Set colEventLogs = refWMI.InstancesOf("Win32_NTEventLogFile")
If Err <> 0 Then
WScript.Echo "Could not retrieve Event Log objects"
WScript.Quit
End If
```

```
'iterate through each log and output information
For Each refEventLog In colEventLogs
WScript.Echo "Information for the " & _
refEventLog.LogfileName & _
" log:"
WScript.Echo " Current file size: " & refEventLog.FileSize
WScript.Echo " Maximum file size: " & refEventLog.MaxFileSize
WScript.Echo " The Log currently contains " & _
refEventLog.NumberOfRecords & " records"

'output policy info in a friendly format using OverwriteOutDated,
'as OverWritePolicy is utterly pointless.
'note "-1" is the signed interpretation of 4294967295
Select Case refEventLog.OverwriteOutDated
Case 0 WScript.Echo _
" Log entries may be overwritten as required"
Case -1 WScript.Echo _
" Log entries may NEVER be overwritten"
Case Else WScript.Echo _
" Log entries may be overwritten after " & _
refEventLog.OverwriteOutDated & " days"
WScript.Echo
End Select
Next

Set refEventLog = Nothing
Set colEventLogs = Nothing
Set refWMI = Nothing
```

Running the Hack

To run the script, use *Cscript.exe*, the command-line version of the Windows Script Host (WSH). Simply type `cscript loginfo.vbs` at a command prompt from the directory in which the script resides. Here is a sample of typical output when the script runs on a Windows 2000 machine:

```
C:\>cscript loginfo.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Information for the Security log:
 Current file size: 65536
 Maximum file size: 524288
 The Log currently contains 166 records
 Log entries may be overwritten after 7 days

Information for the Application log:
 Current file size: 524288
 Maximum file size: 524288
 The Log currently contains 2648 records
 Log entries may be overwritten as required
```

```
Information for the System log:
 Current file size: 524288
 Maximum file size: 524288
 The Log currently contains 2648 records
 Log entries may be overwritten after 7 days
```

Note that when you run this script on a domain controller it displays information concerning the Directory Service, File Replication Service, and DNS logs as well.

—*Rod Trent*

Additional resources

- Sign up for the Windows 2000 Server newsletter
- Sign up for the Windows Server 2003 newsletter
- See all of TechRepublic's newsletter offerings
- Ten great Windows Server hacks (TechRepublic)
- From its help desk calls, Microsoft reports top 10 security errors (TechRepublic)
- Active Directory: Lock it down in 10 steps (TechRepublic)