Learn about WinRM & WinRS

How can WinRM & WinRS help you, how to activate them as well as examples of how to use them?

David Davis

Network administration - *New in Windows Vista, Windows Server 2003 R2, Windows Server 2008 (and Server 2008 Core) is WinRM & WinRS. They are new command line management tools, allowing system administrators to make significant improvements in remote management and execution of programs on Windows computers. However, to use these tools, you need to activate and study its command line functions. This article will provide problems for beginners to use these tools .*

What is remote management (WinRM)?

Windows Remote Management (known as WinRM), is a remote management service for Windows Server 2003 R2, Windows Vista and Windows Server 2008. WinRM is the 'server' component of this remote management application, while WinRS (Windows Remote Shell) is 'client' for WinRM, which runs on a remote computer to remotely manage a WinRM server. It should be noted that both computers must be installed and enabled WinRS to work and retrieve information from the remote system.

WinRM is built on Web Services for management standards (WS-Management). It uses the HTTP protocol (port 80) and SOAP requests to do the job. The advantage here is that HTTP requests can be sent and received easily through the firewall. This makes managing computers running someone else's Windows operating system remotely on the Internet easier, but the weakness that is adjacent to it is that malicious attackers can easily perform attacks on computers. run this operating system via the Internet. However, another advantage of WinRM in using HTTP is that there is no need to open some additional ports on the server and client firewall if HTTP send is allowed. According to Microsoft, WinRM is' new tool for the opening of standard APIs for system management purposes'.

You probably already know a bit about the Windows Management Instrumentation (WMI) database. This database includes all types of hardware and software information on the computer. Windows system management application will use this database to perform any necessary management tasks performed on the computer.

WinRM uses the WMI database to perform the same tasks that you or your systems management package can be implemented with other programming interfaces such as VBScript. The advantage of WinRM is that it uses port 80 (HTTP) as mentioned above, and allows WinRM to share the port sent to 80 with IIS.

WinRM supports multi-style authentication to prevent someone from performing administrative tasks on your servers and clients. Remember, activating WinRM also means opening an avenue for attacks to infiltrate your system. However, just like any port when opened, if there is an appropriate authentication and encryption mechanism, you can completely overcome this problem.

There is another way that you can also use WinRM to use the command line tool *winrm.cmd*. With this CLI utility, you can easily retrieve information from the WMI database to perform any desired system management functions.

As you can see below, WinRM has a command line interface with lots of options. This WinRM help information will appear when WinRM is not "activated" or not "listened" to on the system.

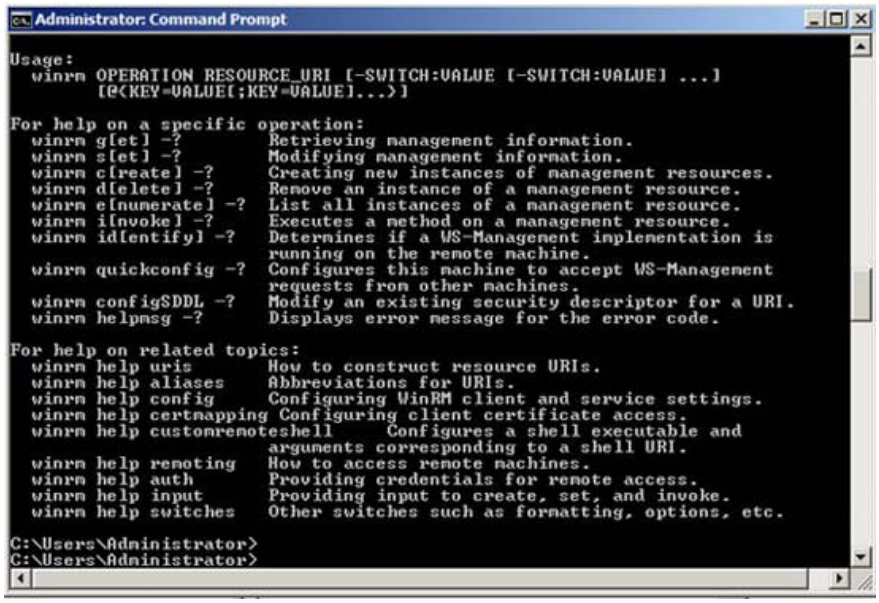

Figure 1: WinRM command line options

How to activate and use WinRM

If you use Windows 2008 Server, WinRM will be installed but not enabled by default. This is an important security precaution. The easiest way to determine if WinRM is enabled and working on your computer is to prompt the CMD command and run:

winrm enumerate winrm / config / listener

If you do not see a response appear, it means WinRM is not running. To configure WinRM to automatically run and allow remote access, use the **winrm quickconfig** command as described below:

C: UsersAdministrator> ***winrm quickconfig***
WinRM không ??t ???c ?? cho phép truy c?p t? xa cho máy này ?? qu?n lý.
The following changes must be made:
*T?o m?t danh sách WinRM trên HTTP: // * ?? nh?n ???c các máy ph?c v? yêu c?u nào nào nào nào nào này.*
Make these changes [y / n]? ***y***
WinRM has been updated for remote management.
*Created a WinRM listener on HTTP: // * to accept WS-Man requests to nào nào IP này.*
C: UsersAdministrator>
N?u b?n c?u hình quickconfig, I reran l?nh enumeration v?i các k?t qu?:
C: UsersAdministrator> ***winrm e winrm / config / listener***
Listener

*Address = **
Transport = HTTP
Port = 80
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 10.253.15.98, 127.0.0.1, :: 1, fe80 :: 5efe: 10.253.15.98% 11, fe80 :: 9583: 2148: e1ef: 6444% 10
C: UsersAdministrator>

From here, we know that WinRM is enabled.

This way, if you want to disable WinRM at any point, use the command:

*winrm delete winrm / config / listener? IPAdress = * + Transport = HTTP*

In order to use WinRM, communication hosts need to be members of the same domain as the WinRM host.

What is WinRS and how to use it

WinRS is a Windows remote management utility. With WinRS, you can query remote Windows machines running WinRM. However, it should be noted that your computer must run WinRM to use WinRS.

As you can see in the figure below, **winrs** is a full-featured command-line tool along with effective help information display.

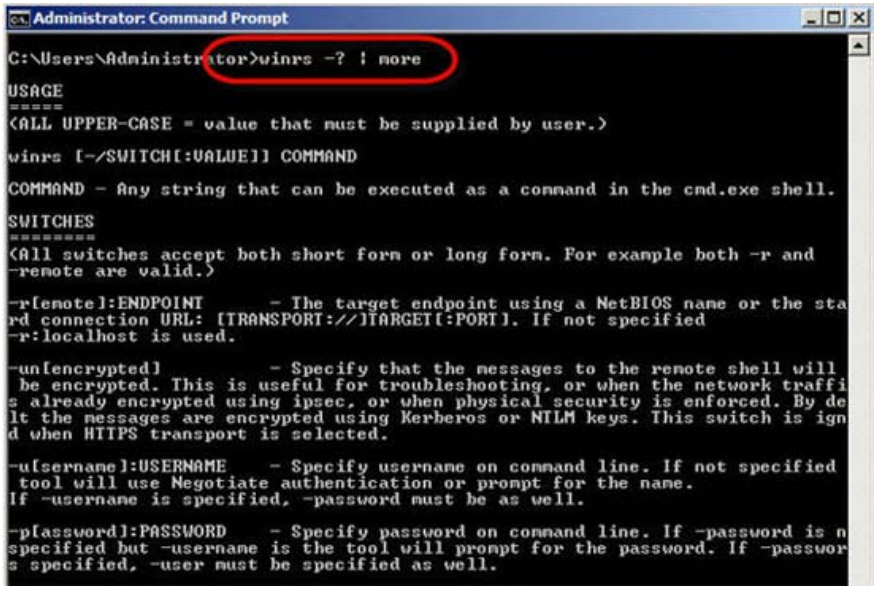

Figure 2: WinRS command line options

One of the most common uses for WinRS is to execute commands on the remote system. This command is communicated using the HTTP protocol / port 80 (default).

Below is an example of where we executed WinRS on localhost running WinRM. We have run two commands - ' **ver** ' and ' **dir C:** '. Each command returns with the appropriate information.

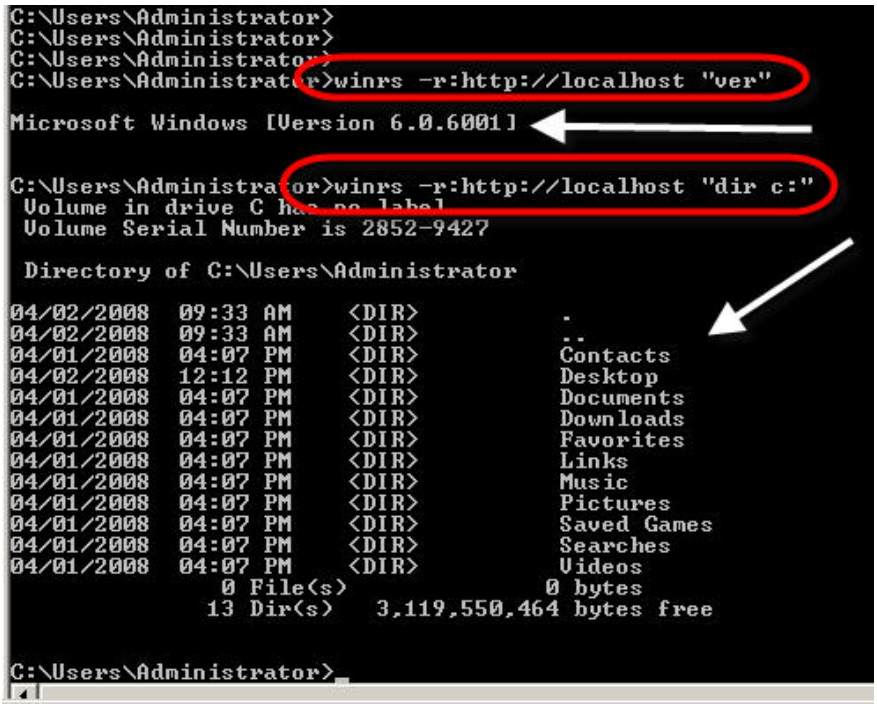

Figure 3: WinRS command illustration

Conclude

WinRM & WinRS are powerful new tools that Windows system administrators should research and use. From afar, you can install the program settings, change the settings or perform troubleshooting (as long as the network works). You can also perform more important tasks and combine WinRS with a click to perform other tasks on a list of computers.

You finished reading the article "**Learn about WinRM & WinRS**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.