Windows PowerShell Web Access

Windows PowerShell Web Access, introduced in Windows Server 2012, lets you configure Web Server (IIS) as a gateway, providing a web-based Windows PowerShell console targeted at a remote computer. For more information, see Install and Use Windows PowerShell Web Access (http://go.microsoft.com/fwlink/?LinkID=221050).

Install-PswaWebApplication (requires elevation)
Quick configuration of the PSWA application and application pool. The cmdlet installs the web application, **pswa** (and an application pool for it, **pswa_pool**), in the **Default Web Site** container that is displayed in IIS Manager. For a test environment only, add the **UseTestCertificate** parameter, which applies a self-signed test certificate to the website. Do not use a test certificate in any environment that should be secure.
Add-PswaAuthorizationRule (in WS12 R2, can run on remote computers with -Credential parameter)
Adds a new authorization rule. Authorizes specified users or groups access to specified session configurations on specified computers. Without authorization rules, no users can access anything by using the web-based console.
Remove-PswaAuthorizationRule
Removes a specified authorization rule from Windows PowerShell Web Access.
Get-PswaAuthorizationRule
Returns a set of Windows PowerShell Web Access authorization rules. When it is used without parameters, the cmdlet returns all rules.
Test-PswaAuthorizationRule (in WS12 R2, can run on remote computers with -Credential parameter)
Evaluates authorization rules to determine if a specific user, computer, or session configuration access request is authorized. By default, without parameters, the cmdlet evaluates all authorization rules. By adding parameters, you can specify an authorization rule or a subset of rules to test.

Function keys for Windows PowerShell Web Access

In the web-based console, some function keys are different than those in PowerShell.exe, and some function keys are not supported in the web-based console. For a complete list of shortcuts for PowerShell.exe that aren't supported in Windows PowerShell Web Access, see Use the Web-based Windows PowerShell Console (http://go.microsoft.com/fwlink/?LinkId=254378).

Shortcut in PS.exe	Shortcut in PSWA
Ctrl+C to cancel	**Ctrl+Q** or **Cancel** button
F5	Use the **History** scroll buttons
Alt+Space, **c** or **Exit**	Click **Exit**, or type **Exit**
(none)	Click **Save** to save a session for later

Provide alternate credentials at sign-in

If the credentials to manage a remote computer are different from those you use to authenticate on the Windows PowerShell Web Access gateway, specify alternate credentials in the **Optional Connection Settings** area on the Windows PowerShell Web Access sign-in page. For detailed instructions, see Use the Web-based Windows PowerShell Console (http://go.microsoft.com/fwlink/?LinkId=254378).

Management Infrastructure

Quick and easy event forwarding using WS-Man:

1. Set up 3 types of event forwarding: **Push**, **Pull**, **Source-Initiate**
2. Event gets published in NT event log
3. Passed on to WS-Man (event forwarding functionality)
4. WS-Man forwards event to the event collector
5. Event collector collects events in forwarded channel of event log
   - One collector can scale to multiple sources and events
   - More information about how to enable event forwarding: http://msdn.microsoft.com/en-us/library/bb870973.aspx http://technet.microsoft.com/en-us/query/bb736545

Out-of-band management using WS-Man: examples

Power On
Example winrm invoke RequestStateChange cimv2/CIM_ComputerSystem -r:http://machine:623 -a:digest -u:admin -p:*password* @{RequestedState="2"}
Power Off
Example winrm invoke RequestStateChange cimv2/CIM_ComputerSystem -r:http://machine:623 -a:digest -u:admin -p:*password* @{RequestedState="3"}
Get chassis info
Example winrm enumerate cimv2/CIM_Chassis -r:http://machine:623 –a:digest -u:admin -p:*password*
Get operating system info
Example winrm get wmicimv2/Win32_OperatingSystem

Common remote management tasks

Add servers to existing list of TrustedHosts
Example Set-Item wsman:\localhost\Client\TrustedHosts Server01 -Concatenate -Force
Create a new listener over port 5985 (for older releases of Windows Server)
Example winrm create winrm/config/Listener?Address=*+Transport=HTTP winrm set winrm/config/Listener?Address=*+Transport=HTTP @{Port="5985"}
Configure the number of maximum shells allowed per user
Example winrm s winrm/config/winrs @{MaxShellsPerUser="X"}

Management Log File Locations

Component	Event Tracing for Windows Channels	Comment
Server Manager console	Applications And Services Logs\Microsoft\Windows\ServerManager-MultiMachine	Client operations events; stored on the computer that is running Server Manager
Server Manager Management Provider	…\ServerManager-ManagementProvider	Events in this log are stored on the managed server
Add Roles and Features Wizard	…\ServerManager-MultiMachine	
Add Roles and Features Wizard Workflow	…\ServerManager-MultiMachine	Event IDs 4000-4099
Server Manager Deployment Provider	…\ServerManager-DeploymentProvider	
Windows PowerShell DSC	…\Microsoft-Windows-DSC	
Windows PowerShell Workflow general	…\PowerShell	Event 45079 shows each activity run
Configure Remote Management task	…\ServerManager-ConfigureSMRemoting	

Related Log File Locations

Component	Event Tracing for Windows Channels
WinRM	Applications and Services Logs\Microsoft\Windows\Windows Remote Management
WMI	…\WMI-Activity
Component-based Servicing (CBS)	%*windir*%\Logs
Deployment Image Servicing and Management (DISM)	%*windir*%\Logs

For detailed help about any cmdlet, including complete descriptions of all parameters, first run Update-Help, and then enter the following in a Windows PowerShell session: Get-Help <*Cmdlet Name*> -Full

Windows PowerShell Core Help topics online: http://go.microsoft.com/fwlink/?LinkID=238561

Windows Server Migration Portal: http://go.microsoft.com/fwlink/?LinkID=247608 Cmdlet Help: http://go.microsoft.com/fwlink/?LinkID=246313
Best Practices Analyzer Help: http://go.microsoft.com/fwlink/?LinkID=223177 Cmdlet Help: http://go.microsoft.com/fwlink/?LinkID=240177
Server Manager Help: http://go.microsoft.com/fwlink/?LinkID=221057 Cmdlet Help: http://technet.microsoft.com/library/jj205465.aspx
Windows PowerShell Script Center: http://technet.microsoft.com/ScriptCenter

Manage Remote Servers

Use Server Manager in Windows Server 2012 R2 (or RSAT for Windows 8.1) to manage remote servers that are running the following operating systems, after those servers are prepared by performing the following steps. See http://go.microsoft.com/fwlink/?LinkID=241358 for more information.

Windows Server 2012 and Windows Server 2012 R2

In Windows Server 2012 and later, Server Manager and Windows PowerShell remote management is enabled by default. If remote management has been disabled, do one of the following:

- On the **Local Server** page of Server Manager, click **Remote Management**. Select **Enable remote management of this server from other computers**.
- Run the following in Windows PowerShell as an administrator: **Configure-SMRemoting.exe -Enable**

Windows Server 2008 R2

In Windows Server 2008 R2, Server Manager and Windows PowerShell remote management is disabled by default. To enable it:, do one of the following:

- In the **Server Summary** area of the Server Manager home page, click **Configure Server Manager Remote Management**. Select **Enable remote management of this server from other computers**.
- Run the following Windows PowerShell script as an Administrator: **Configure-SMRemoting.ps1**

To manage this operating system by using Server Manager in Windows Server 2012 R2, also install the following, in the order shown:

1. .NET Framework 4.5 (http://www.microsoft.com/download/details.aspx?id=30653)
2. Windows Management Framework 4.0 (http://go.microsoft.com/fwlink/?LinkID=293881)
3. KB 2682011 Performance Counter Update (http://go.microsoft.com/fwlink/p/?LinkID=245487)

Windows Server 2008

In Windows Server 2008, Server Manager has no setting to enable remote management. Enable remote management of the server by running **Enable-PSRemoting** in a Windows PowerShell session that has been run as Administrator.

Server Manager in Windows Server 2012 R2 can perform limited management on Windows Server 2008. Install the following, in the order shown. Note that WMF 4.0 cannot be installed on Windows Server 2008.

1. .NET Framework 4.0 (http://go.microsoft.com/fwlink/?LinkID=212547)
2. Windows Management Framework 3.0 (http://www.microsoft.com/download/details.aspx?id=34595)
3. KB 2682011 Performance Counter Update (http://go.microsoft.com/fwlink/p/?LinkID=245487)

Windows Server 2003

Server Manager is not available. To enable remote management, configure WinRM and DCOM remote management as described in Configure Remote Management (http://go.microsoft.com/fwlink/?LinkId=252970).

Server Manager in Windows Server 2012 R2 can get only online or offline and limited data about Windows Server 2003.

Remote Management Settings

In Windows Server 2012 R2, enabling remote management by default does the following:

- Sets Windows Remote Management (WinRM) service startup type to **Automatic** and starts the service
- Enables **Kerberos** and **Negotiate** authentication types
- Enables inbound Windows Firewall rules for WinRM
- Changes subnet scoping rules to allow the following by default
  - Domain or private profile: any IP address
  - Public profile: **LocalSubnet** only
- Sets wsman:\localhost\Service\AllowRemoteAccess to **True**
- Creates a WinRM listener over HTTP port number 5985

The **LocalAccountTokenFilterPolicy** default setting prevents remote management by *local, non-domain* Administrator accounts other than the built-in Administrator account. For more information about remote management in Server Manager, see http://go.microsoft.com/fwlink/?LinkID=252970.

Export Server Manager Settings

To other domain-joined computers

In Active Directory Users and Computers, make the profile of a Server Manager user roaming. Open the **Properties** for a Server Manager user. On the **Profile** tab, add a path to a network share to store the user's profile. On U.S. English builds, changes to the **ServerList.xml** file are automatically saved to the profile. On other builds, copy these two files from the computer that is running Server Manager to the network share that is part of the user's roaming profile:

- %appdata%\Roaming\Microsoft\Windows\ServerManager\ServerList.xml
- %appdata%\Local\Microsoft_Corporation\ServerManager.exe_StrongName_*GUID*\6.3.0.0\user.config

To a workgroup computer

On a computer from which you want to manage remote servers, overwrite these two files with the same files from another computer that's running Server Manager, and that has the settings you want.

- %appdata%\Roaming\Microsoft\Windows\ServerManager\ServerList.xml
- %appdata%\Local\Microsoft_Corporation\ServerManager.exe_StrongName_*GUID*\6.3.0.0\user.config

Run Minimal GUI Options

In Windows Server 2012 and later, you can switch between a server with a GUI, and Server Core or a minimal server interface option as needed. Server Manager runs without Server Graphical Shell, but does not run on Server Core. You can use Server Manager to manage remote servers running Server Core.

For more about Server Core and minimal GUI options, see Windows Server Installation Options (http://go.microsoft.com/fwlink/p/?LinkId=241573).

Install on Offline VHDs or VHDxs

To install features on offline VHDs or VHDxs, the VHDs must:

- Be running Windows Server 2012 R2
- Not have more than one system volume or partition
- Network share containing VHD file must grant these access rights to the computer account of server selected to mount the VHD
  - **Read/Write** access on **File Sharing** dialog box.
  - **Full Control** access on **Security** tab , file or folder **Properties**

Install Roles and Features

In the Server Manager console

On the **Manage** menu, click **Add Roles and Features**. To deploy Remote Desktop Services in either a Virtual Desktop Infrastructure (VDI) or a Session Virtualization configuration, on the **Select installation type** page of the Add Roles and Features Wizard, select **Remote Desktop installation**.

In the Add Roles and Features Wizard, you can install roles and features on the local server, or on a single remote server that is running Windows Server 2012 R2. See details here: http://technet.microsoft.com/library/hh831809.aspx .

Install by using deployment cmdlets (require elevation)

Get-WindowsFeature

Gets information about roles, role services, and features that are available and installed on a server. Add the **ComputerName** parameter to specify a server other than the local server.

Examples

Get-WindowsFeature AD*,Web*

Get-WindowsFeature

Install-WindowsFeature (alias: Add-WindowsFeature)

Installs roles, role services, and features on a server that is running Windows Server 2012 R2. Add the **ComputerName** parameter to specify a server other than the local server. Add the **Source** parameter to specify an alternate location for feature files, in a Features on Demand configuration.

Examples

Install-WindowsFeature -Name Web-Server

Get-WindowsFeature Web* | Install-WindowsFeature

Uninstall-WindowsFeature (alias: Remove-WindowsFeature)

Uninstalls roles, role services, and features from a computer that is running Windows Server 2012 R2. Add the **Remove** parameter to delete unused feature files in a Features on Demand configuration.

Example

Uninstall-WindowsFeature -Name "Telnet-Client","Telnet-Server“ -Remove

Get-WindowsFeature Web* | Uninstall-WindowsFeature

Features on Demand

Run **Uninstall-WindowsFeature -Remove** to delete feature files from Windows Server 2012 R2 servers to save disk space. Later, you can install features by specifying a path to a remote source where feature files are stored.

- When you delete features, features that depend upon the files you remove are also deleted.
- When you delete feature files for a subfeature, and no other subfeatures for the parent feature are installed, then files for the entire parent role or feature are deleted.

For more information, see Configure Features on Demand (http://go.microsoft.com/fwlink/?LinkID=253756).

Install .NET Framework 3.5 and other Features on Demand

To install .NET Framework 3.5 or other features that have been deleted from a target server, do one of the following:

- Specify an alternate feature file repair source path
- Configure Group Policy to provide the source path automatically
- Let the installation get feature files from Windows Update.

See details here: http://go.microsoft.com/fwlink/?LinkId=253762.