

Synchronize a Windows 2012 Server with an External Time Source

June 14, 2013

Synchronizing Time

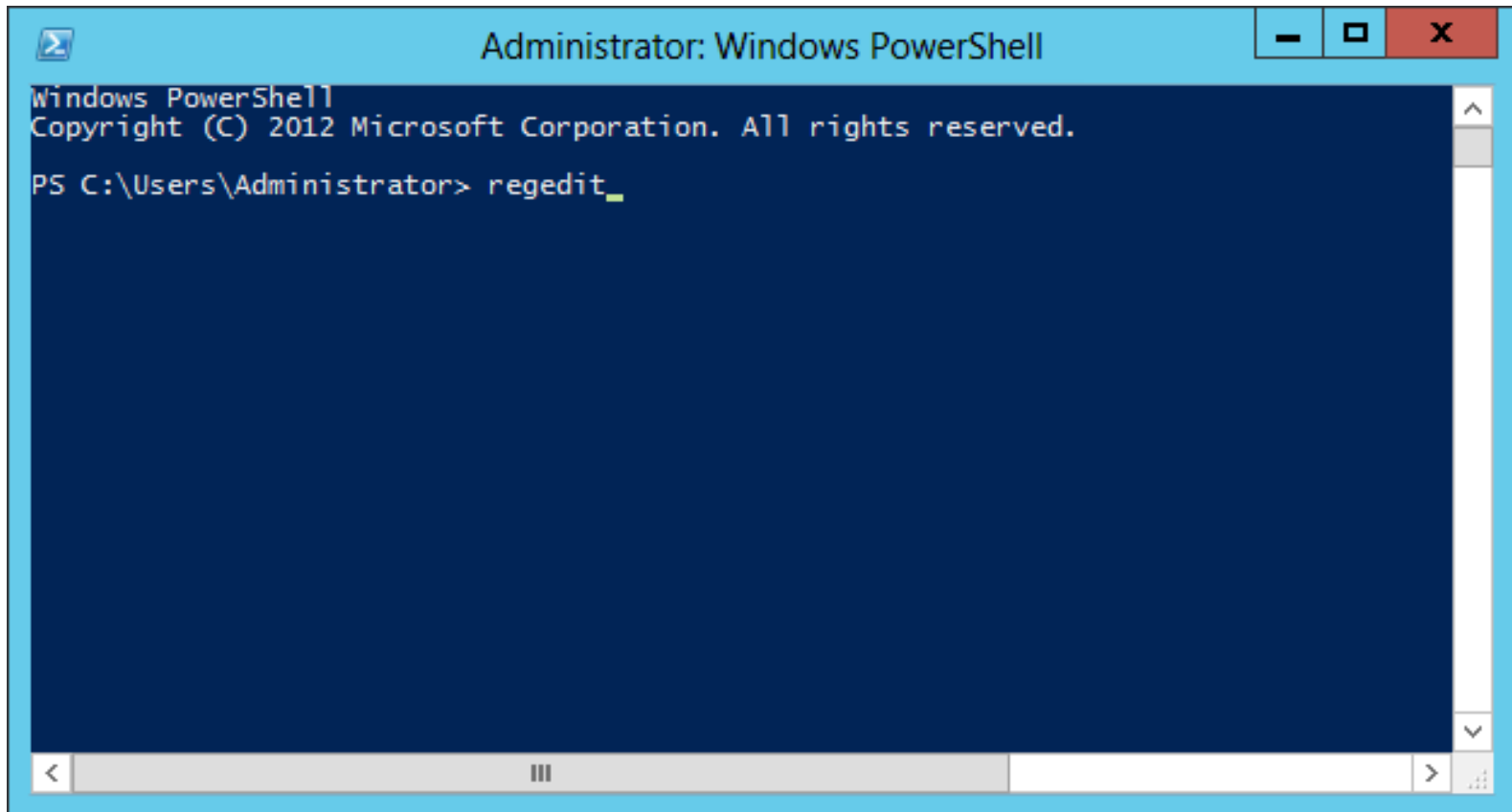
Servers and computers need to synchronize their time with an outside source to maintain the correct time. In this lesson, we will converge our Windows 2012 Server with the US Navy's NTP Server.

We have the opportunity to navigate through the System Registry and safely make changes. The skills we will learn here will help us troubleshoot the Server errors on later dates when the Microsoft Workaround procedures prompt us to check or change a registry setting.



Run Registry Edit (Regedit)

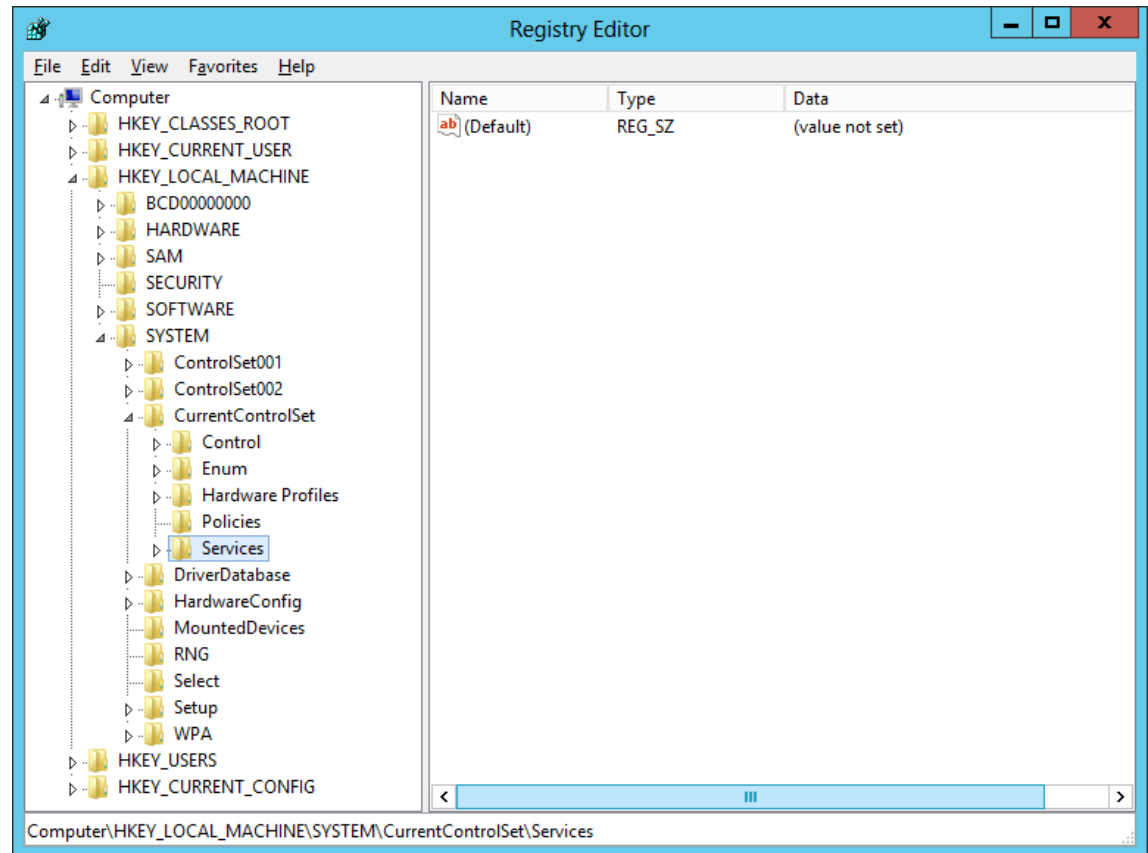
To access the server's system registry, we will choose the PowerShell icon on the Taskbar. Then we type regedit on the PowerShell window.

A screenshot of an Administrator: Windows PowerShell window. The window has a blue title bar with the text "Administrator: Windows PowerShell" and standard window control buttons (minimize, maximize, close). The main area is a dark blue terminal with white text. The text reads: "Windows PowerShell", "Copyright (C) 2012 Microsoft Corporation. All rights reserved.", and "PS C:\Users\Administrator> regedit_". A scroll bar is visible on the right side of the terminal area.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> regedit_
```

How to Navigate the Registry Editor

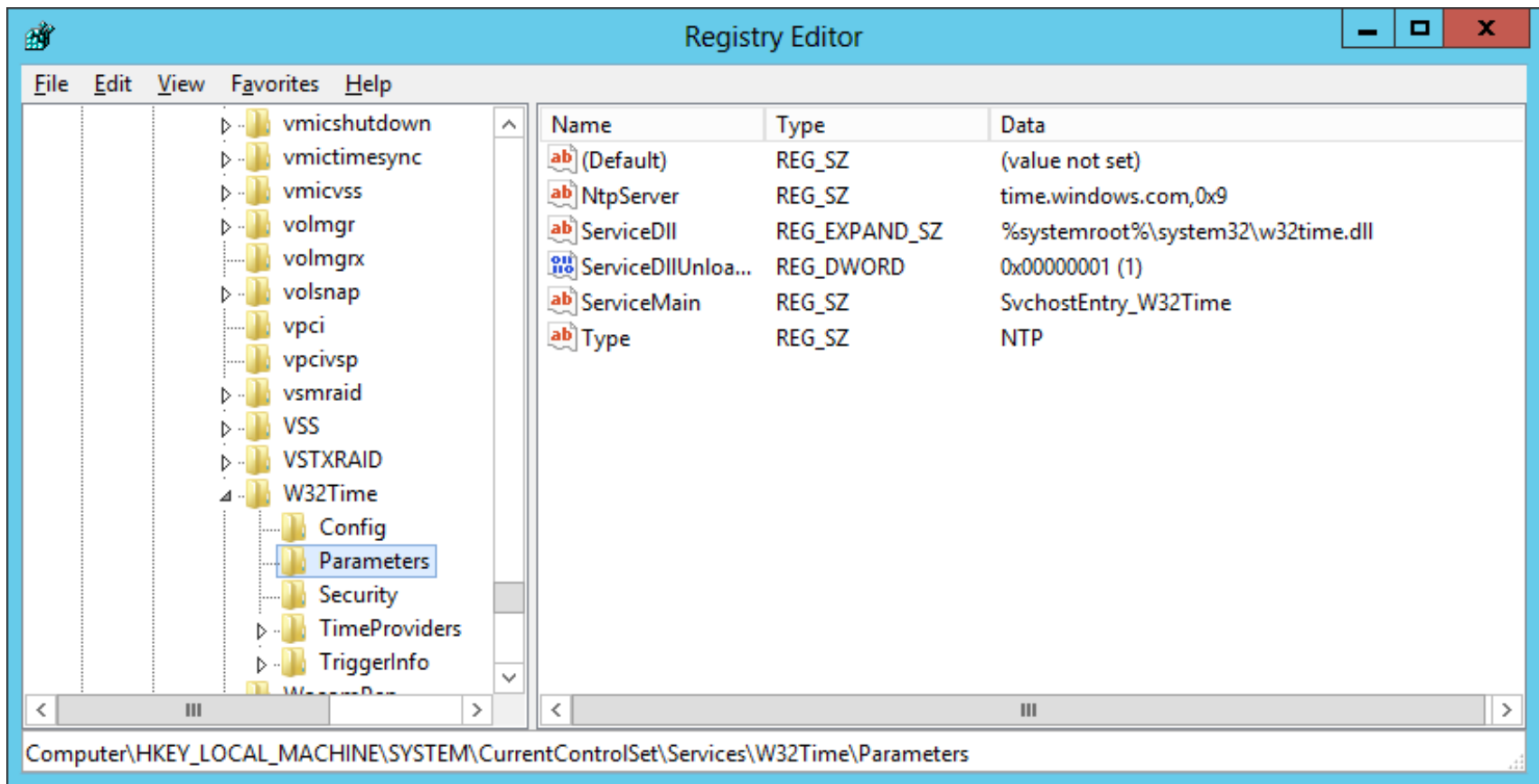
The Registry Edit window will come into view on our desktop and we need to come across HKEY_LOCAL_MACHINE under Computer. We can press the plus symbol on the left and the folder tree will expand. We can inflate the System folder, and the Current Control Set folder. When we are in the System Registry, we need to be careful to be in the correct location when making changes.



Many time network administrators and technicians will see the registry path written is this format to save space: HKLM\SYSTEM\CCS\Services\W32Time\Parameters

System Settings on a Folder

We follow the path to HKLM\SYSTEM\CCS\Services\W32Time\Parameters and we find that there are six system settings inside the Parameters folder.

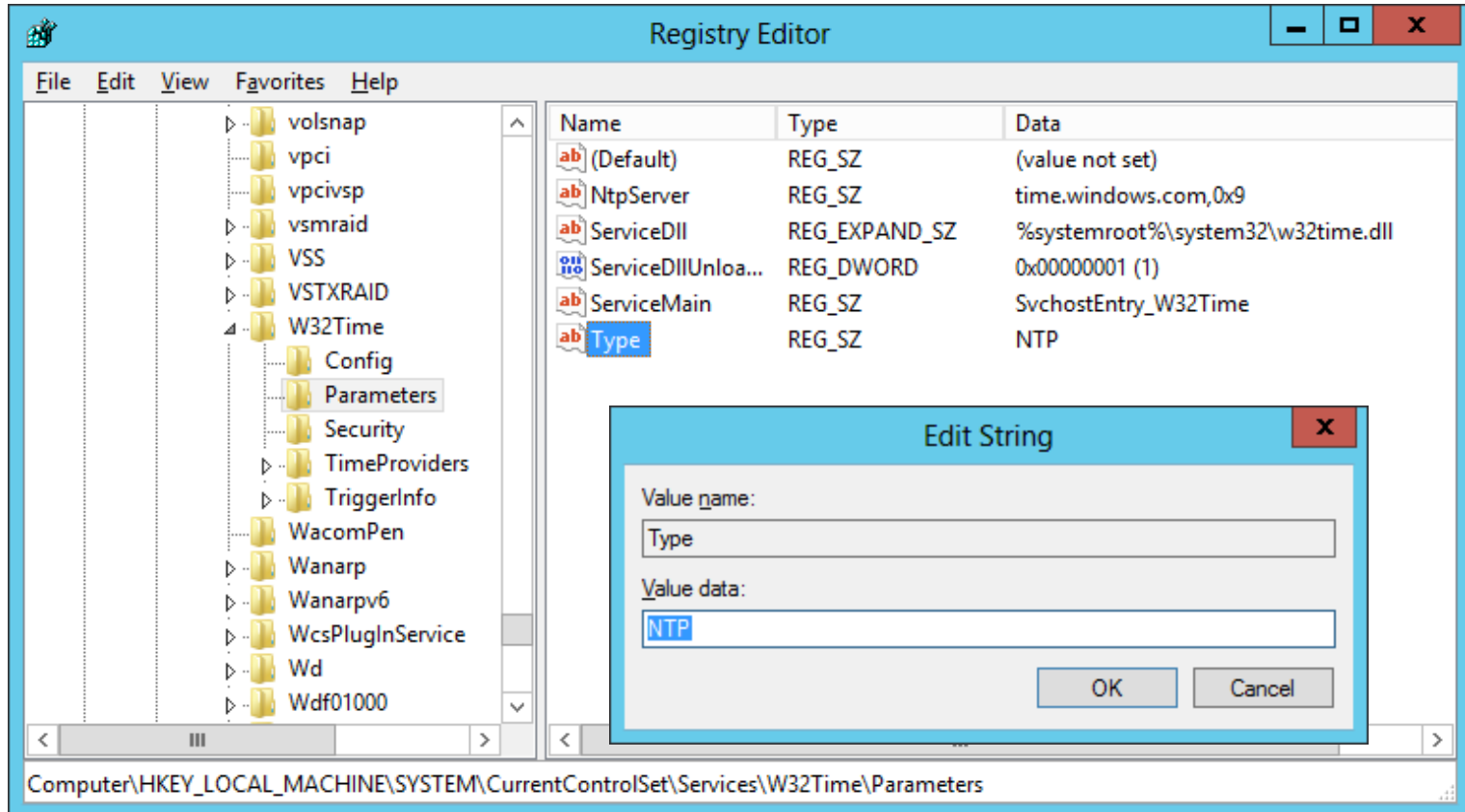


The screenshot shows the Windows Registry Editor window. The left pane displays the tree view with the path `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters` selected. The right pane displays a table of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
NtpServer	REG_SZ	time.windows.com,0x9
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
ServiceDllUnloa...	REG_DWORD	0x00000001 (1)
ServiceMain	REG_SZ	SvchostEntry_W32Time
Type	REG_SZ	NTP

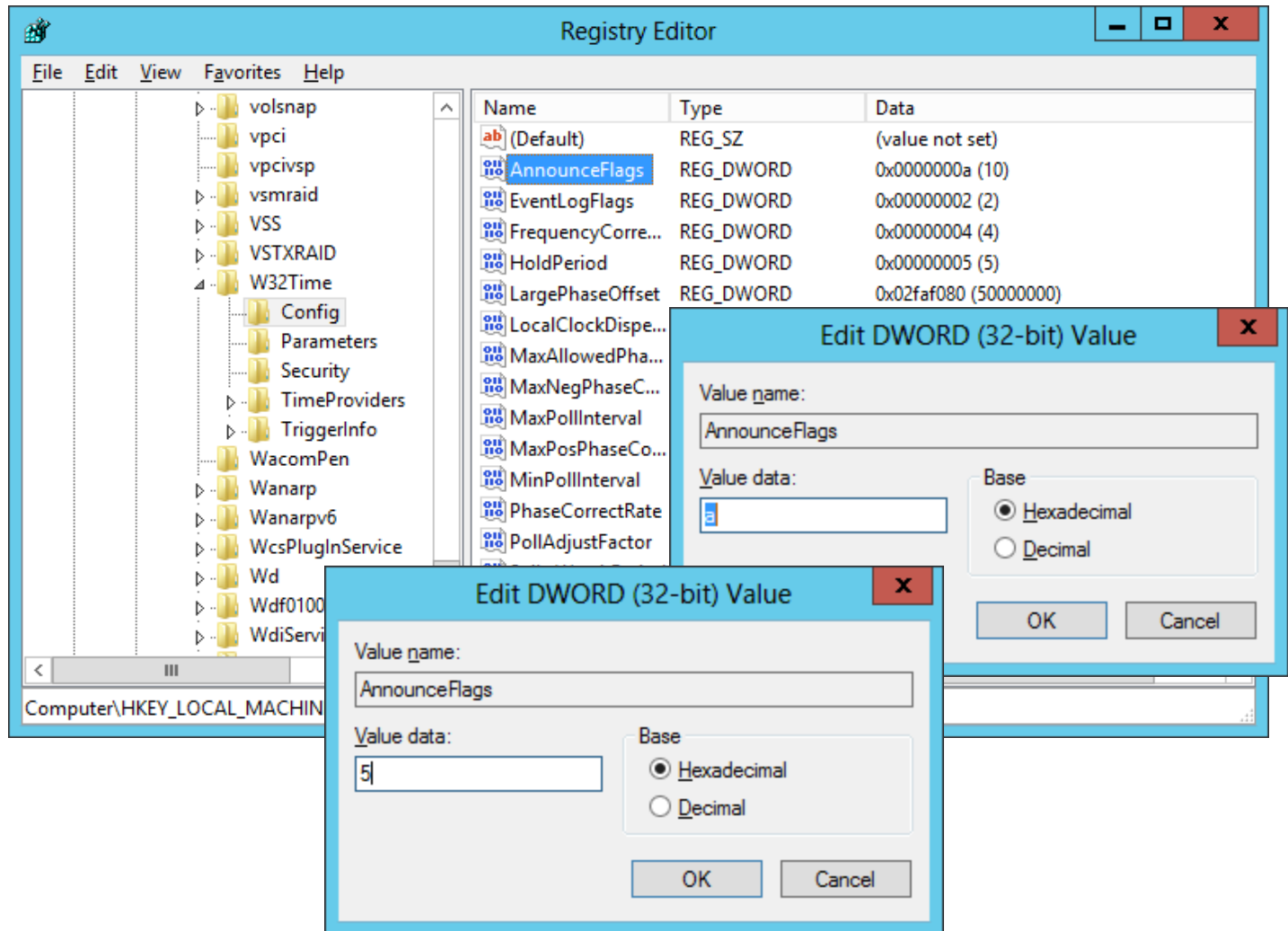
Changing the Type Setting

With the Parameters folder highlighted, we double click on Type and the Edit String window will appear. It should read NTP. If it does not change it and press the OK button.



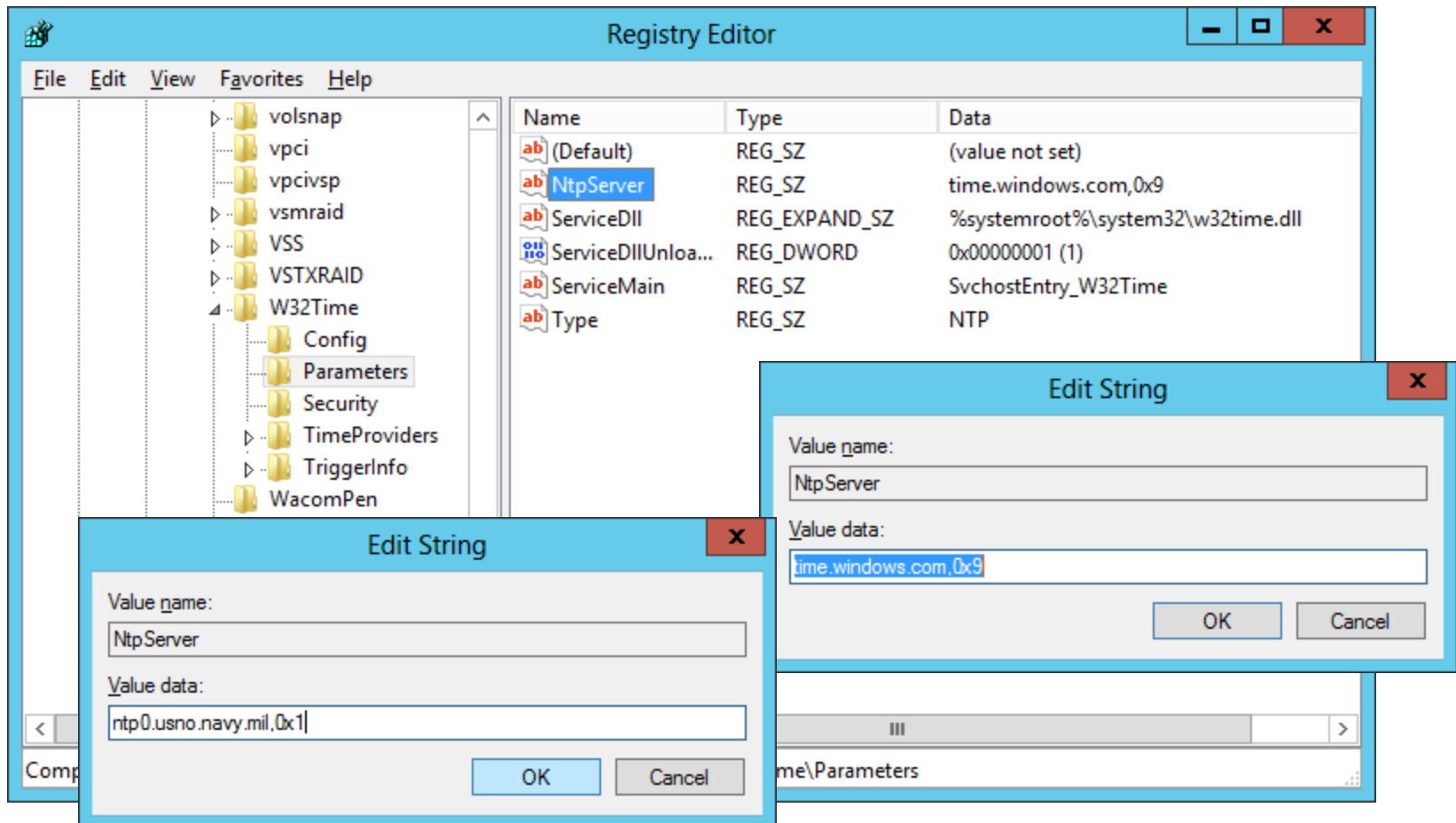
Changing the AnnounceFlags Setting

Next, with the Config folder highlighted, we double click on AnnounceFlags and the Edit DWORD Value window will appear. Change "a" to "5". We should press the OK button to save the change.



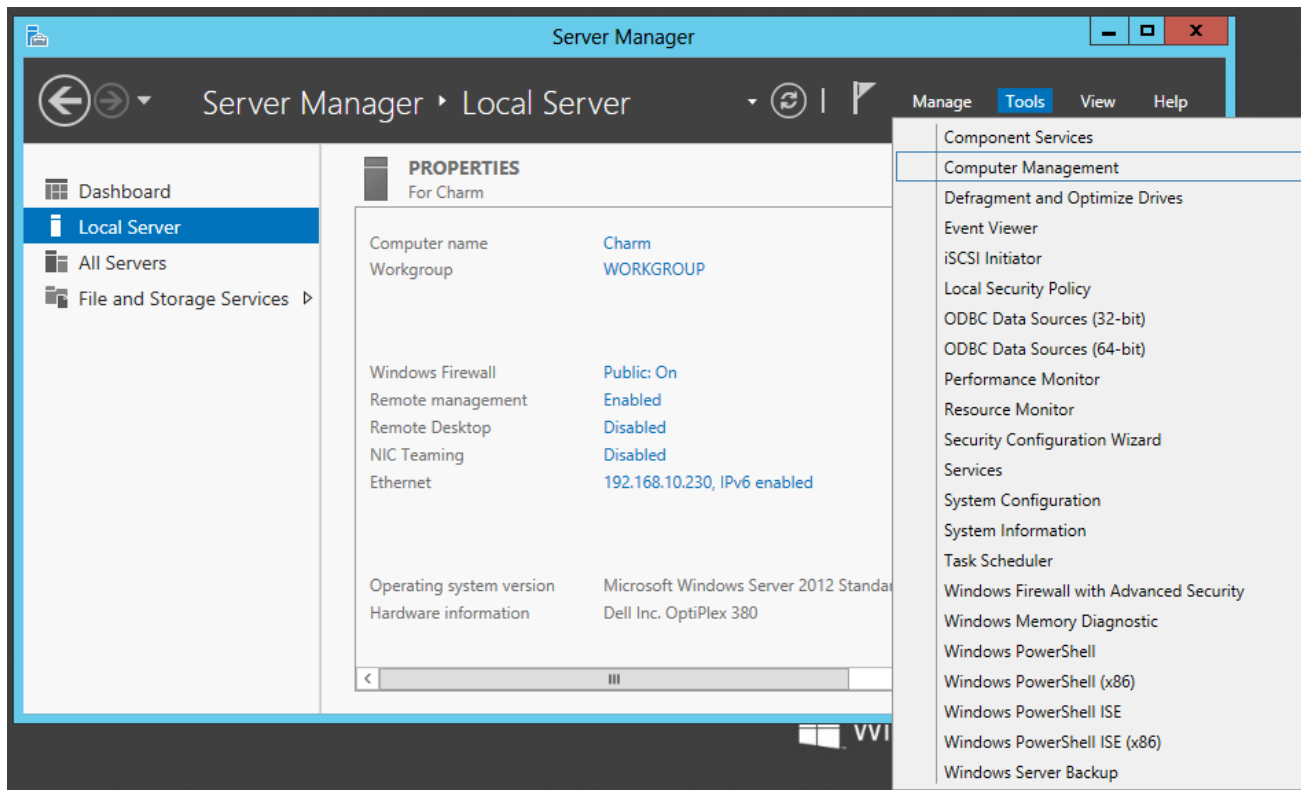
Changing the NtpServer Setting

Return to the Parameters folder and we double click on NtpServer and the Edit String window will appear. Change “time.windows.com,0x1” to “ntp0.usno.navy.mil,0x1”. We should press the OK button to save the change. We now can close the Registry Editor.



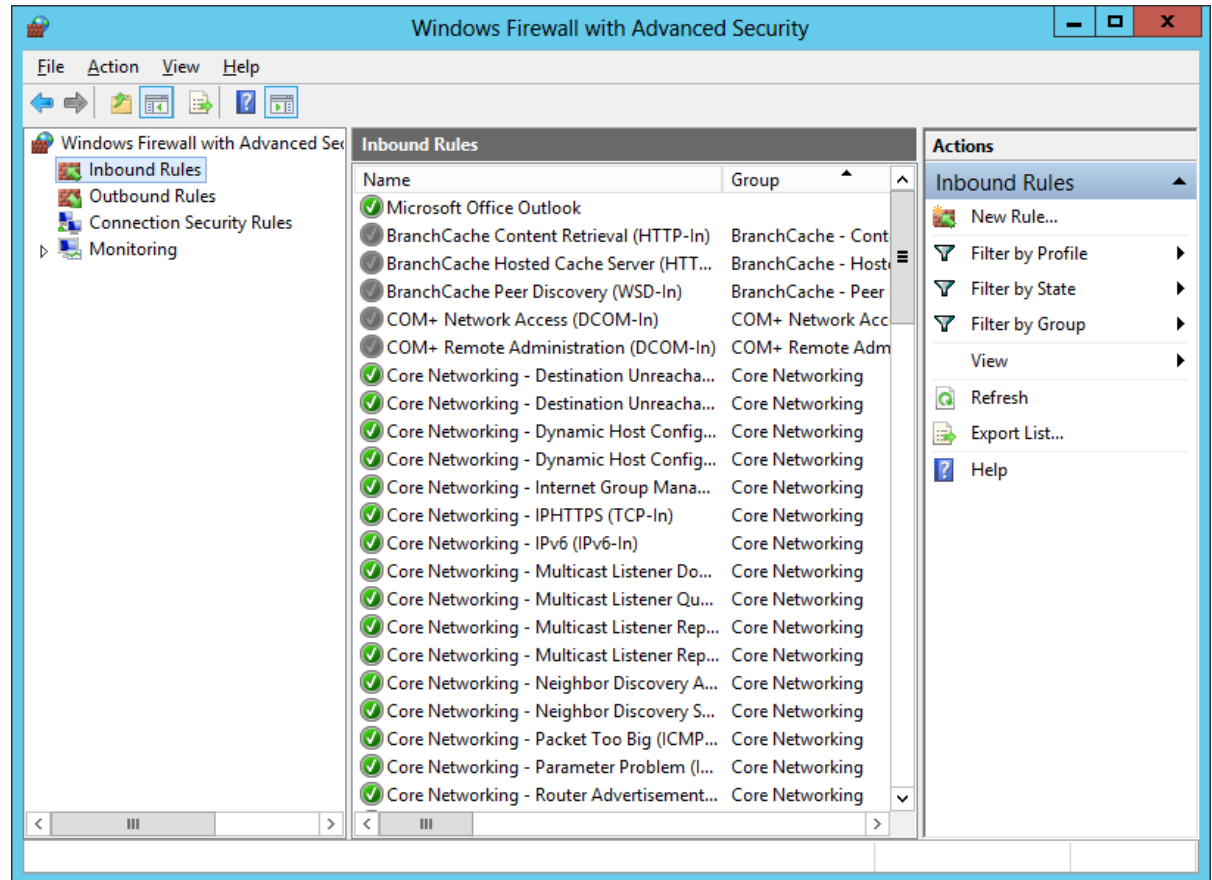
Setup Security Policies

To open an inboard port on the Windows Firewall on the Windows 2012 Standard Server, we select the Server Manager button from the Task Bar and select Tools from the Dashboard. From the list we choose Windows Firewall and Advanced Security.



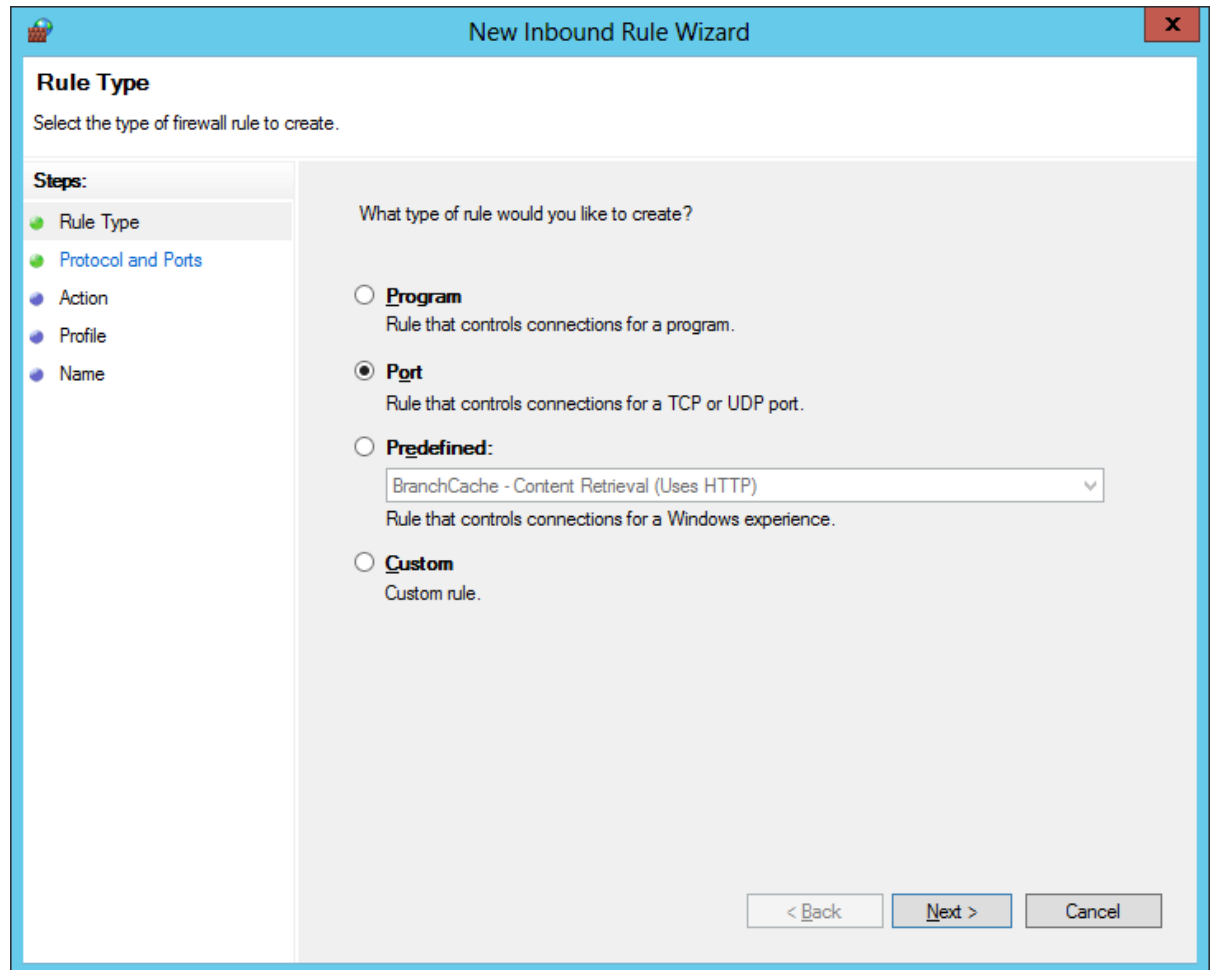
Open Inbound Port UDP123

To connect to a NTP server, we open Inbound Port UDP 123. Go to the Start menu and Administrative Tools and click on Windows Firewall with Advanced Security. Select Inbound Policies from the left pane. Click on New Rule on the right pane.



Create a New Rule

Choose the Port Option and the Next button.



New Inbound Rule Wizard

Rule Type
Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

Program
Rule that controls connections for a program.

Port
Rule that controls connections for a TCP or UDP port.

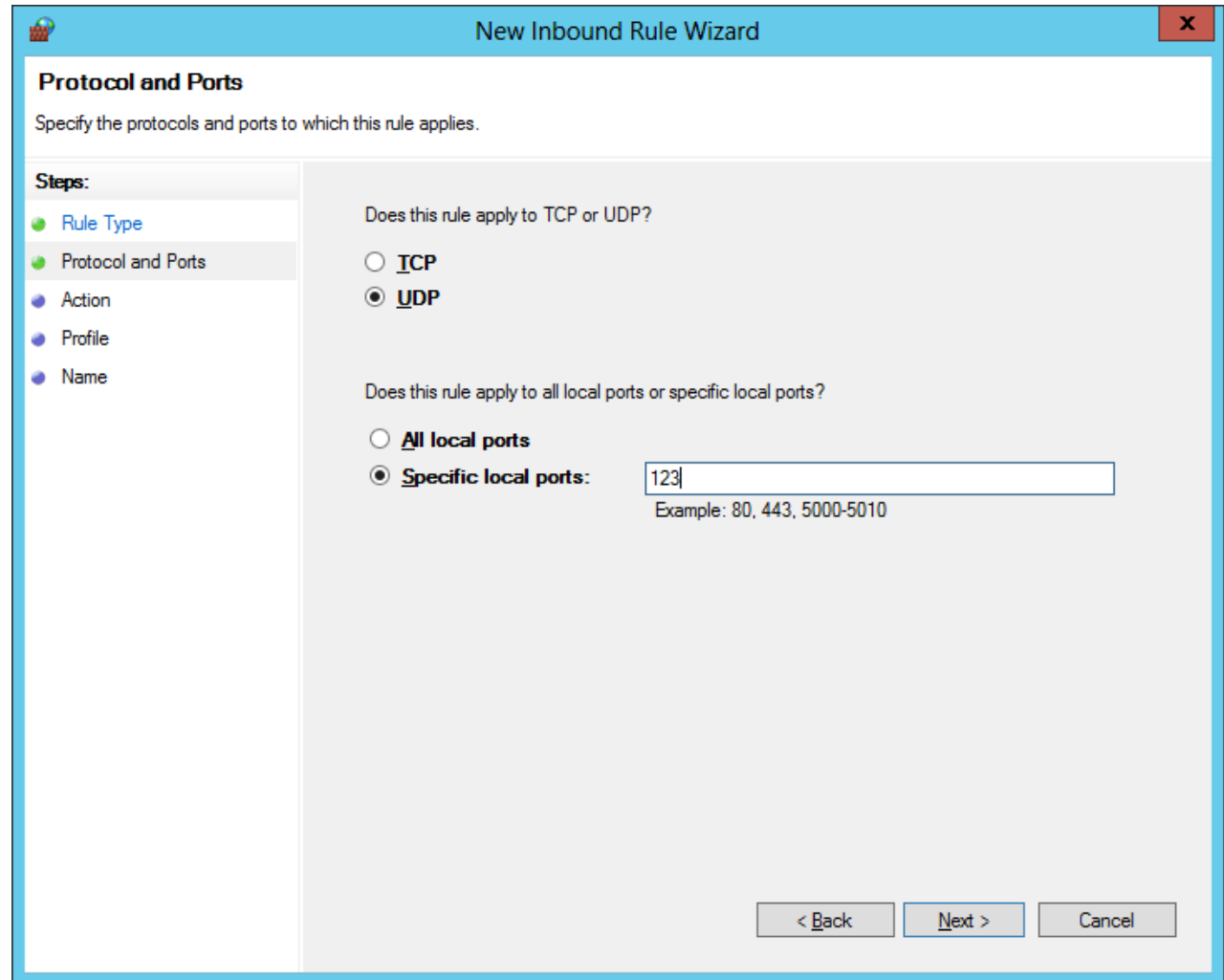
Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

Custom
Custom rule.

< Back Next > Cancel

Open the UDP 123 Port

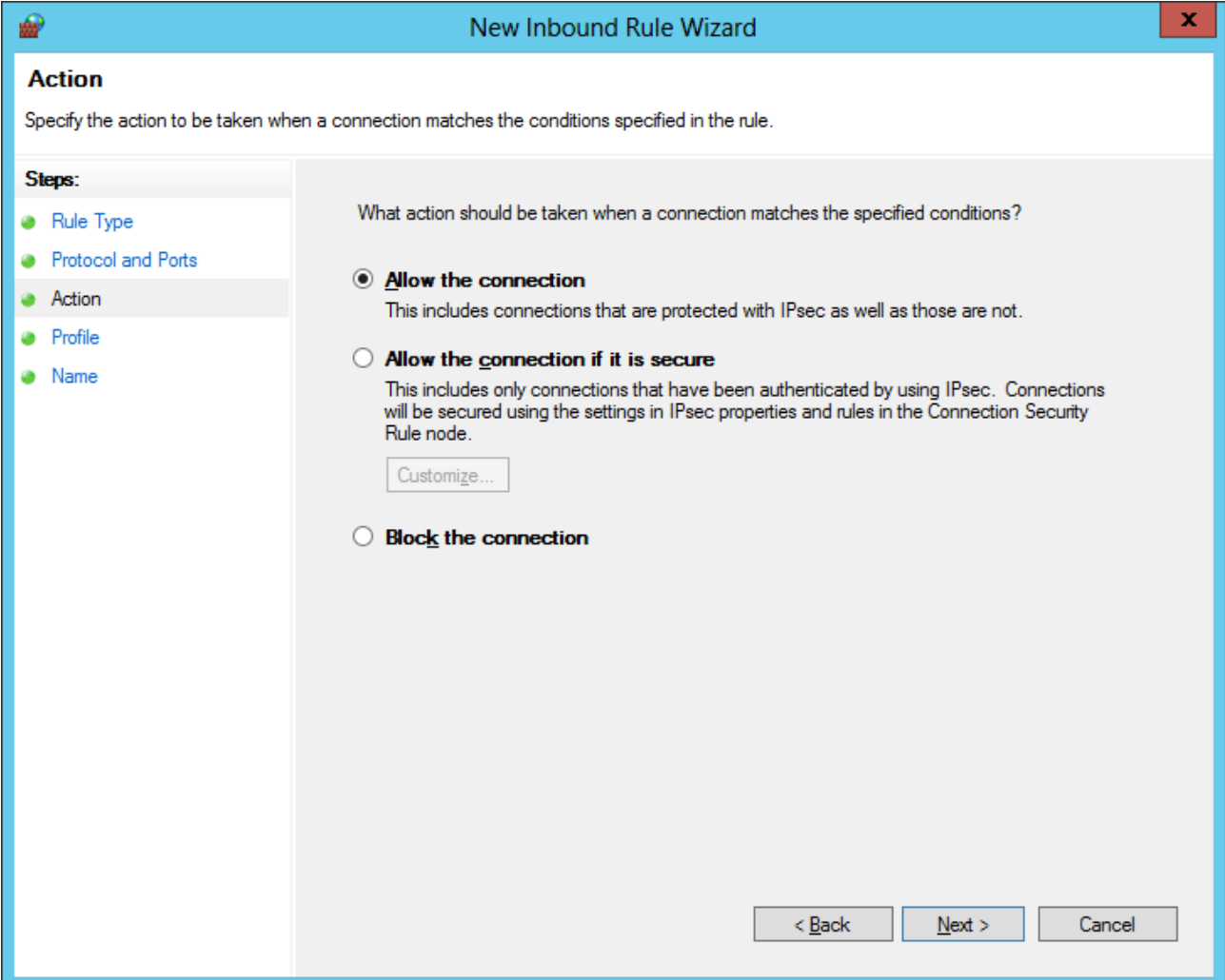
Choose the UDP option and specify the port number as 123 and press the Next button.



The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard' with a close button (X) on the right. Below the title bar, the section is titled 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' sidebar lists: 'Rule Type' (selected with a green dot), 'Protocol and Ports' (selected with a green dot), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot). The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' and 'UDP' (selected); and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports' (selected). Below the 'Specific local ports' option is a text input field containing '123' and an example text 'Example: 80, 443, 5000-5010'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Allow the Connection

We then will opt to allow the connection and push the Next button.



The screenshot shows a window titled "New Inbound Rule Wizard" with a close button (X) in the top right corner. The window is divided into two main sections. On the left, there is a "Steps:" list with five items: "Rule Type", "Protocol and Ports", "Action", "Profile", and "Name". The "Action" step is currently selected and highlighted. The main area on the right contains the text "Specify the action to be taken when a connection matches the conditions specified in the rule." followed by the question "What action should be taken when a connection matches the specified conditions?". There are three radio button options: "Allow the connection" (which is selected), "Allow the connection if it is secure", and "Block the connection". The "Allow the connection" option has a sub-description: "This includes connections that are protected with IPsec as well as those are not." The "Allow the connection if it is secure" option has a sub-description: "This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node." Below this option is a "Customize..." button. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

Action
Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

Allow the connection
This includes connections that are protected with IPsec as well as those are not.

Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

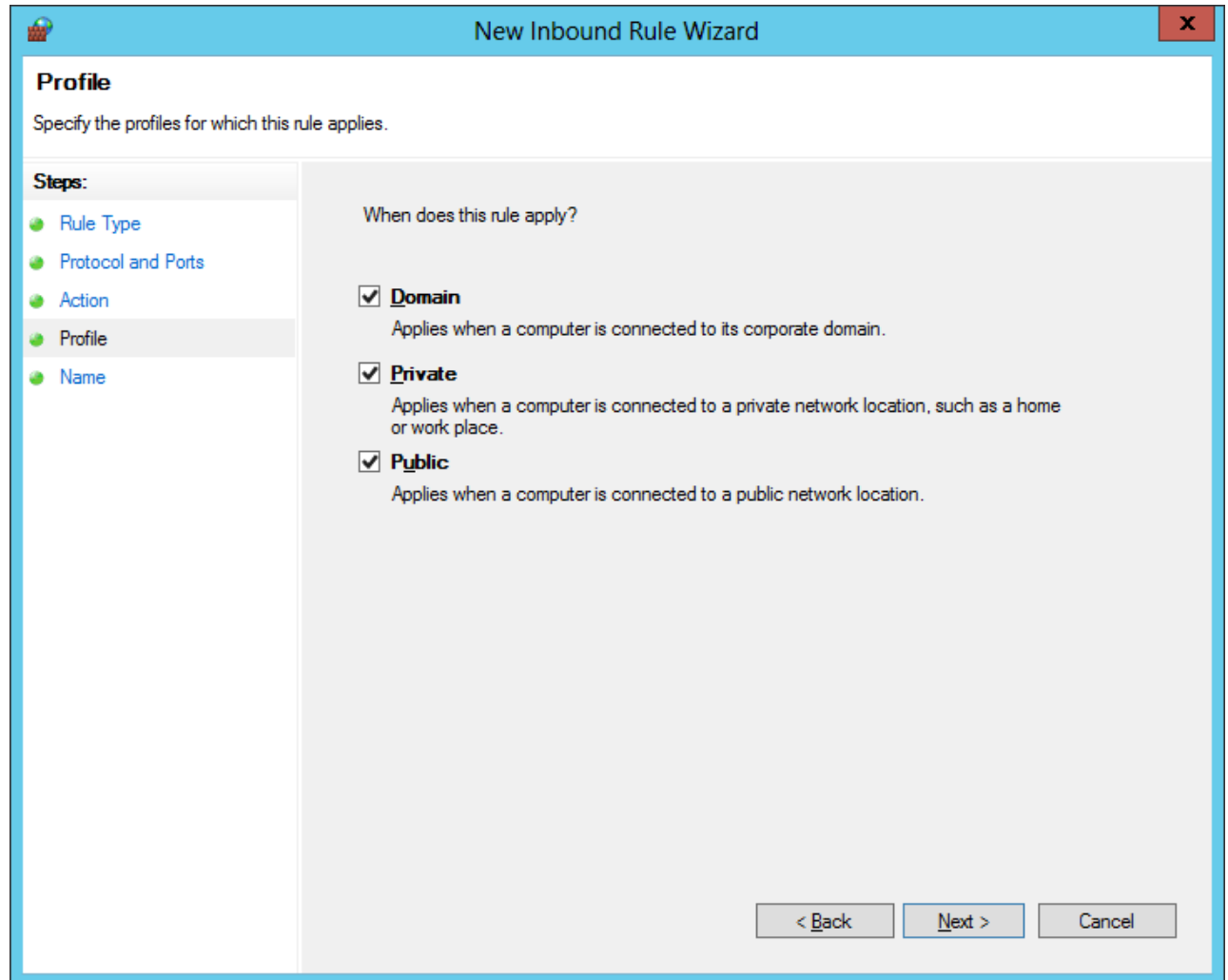
Block the connection

< Back Next > Cancel

Profile the Port

We will annotate the Domain, Private and Public profiles to where the open port applies.

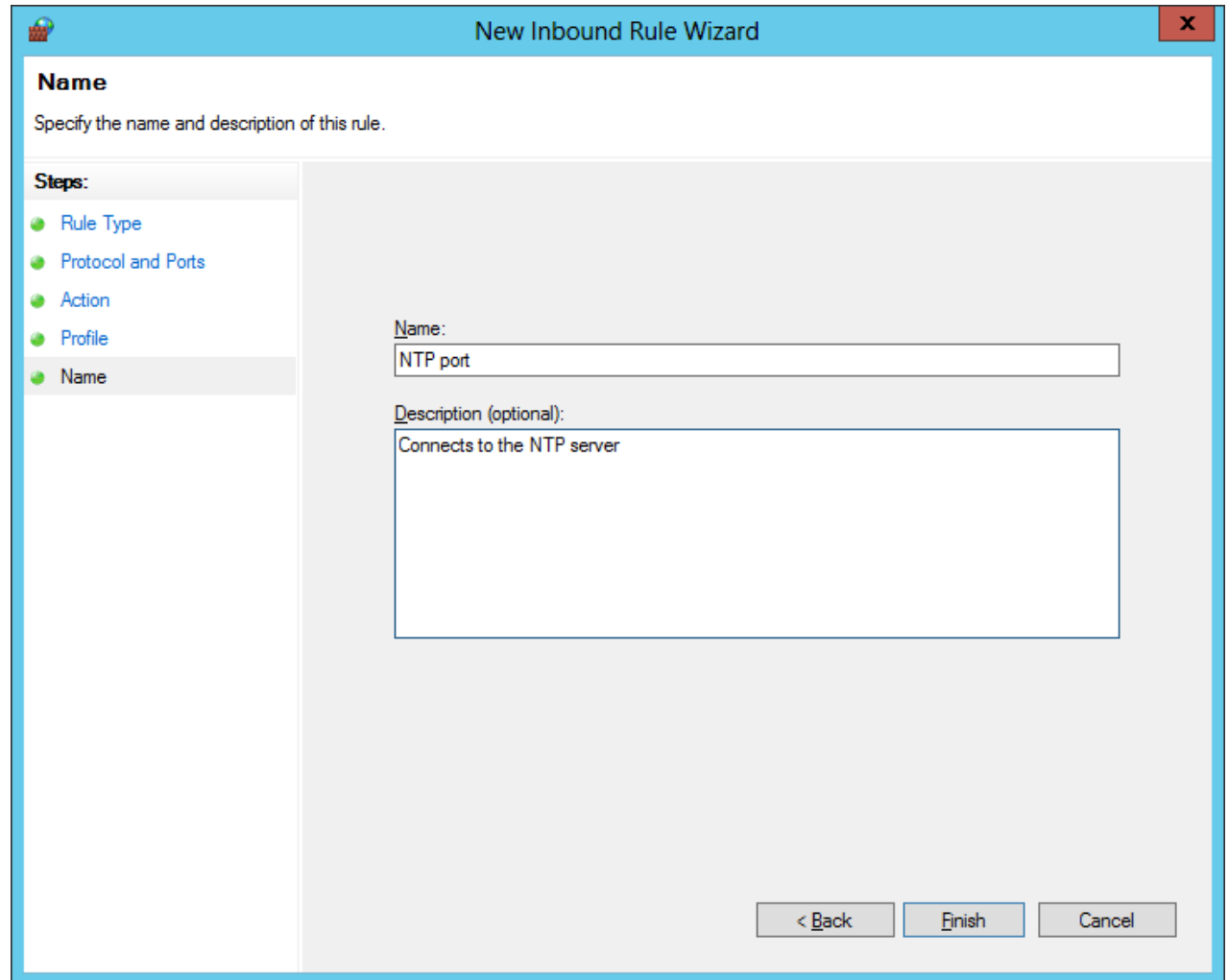
Then we choose the Next button.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The window title is 'New Inbound Rule Wizard' and it has a close button (X) in the top right corner. The main heading is 'Profile' and the instruction is 'Specify the profiles for which this rule applies.' On the left side, there is a 'Steps:' list with five items: 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Profile' step is currently selected and highlighted. The main content area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Name the Rule

We will name the open port rule “NTP port” and give it a short and accurate description.

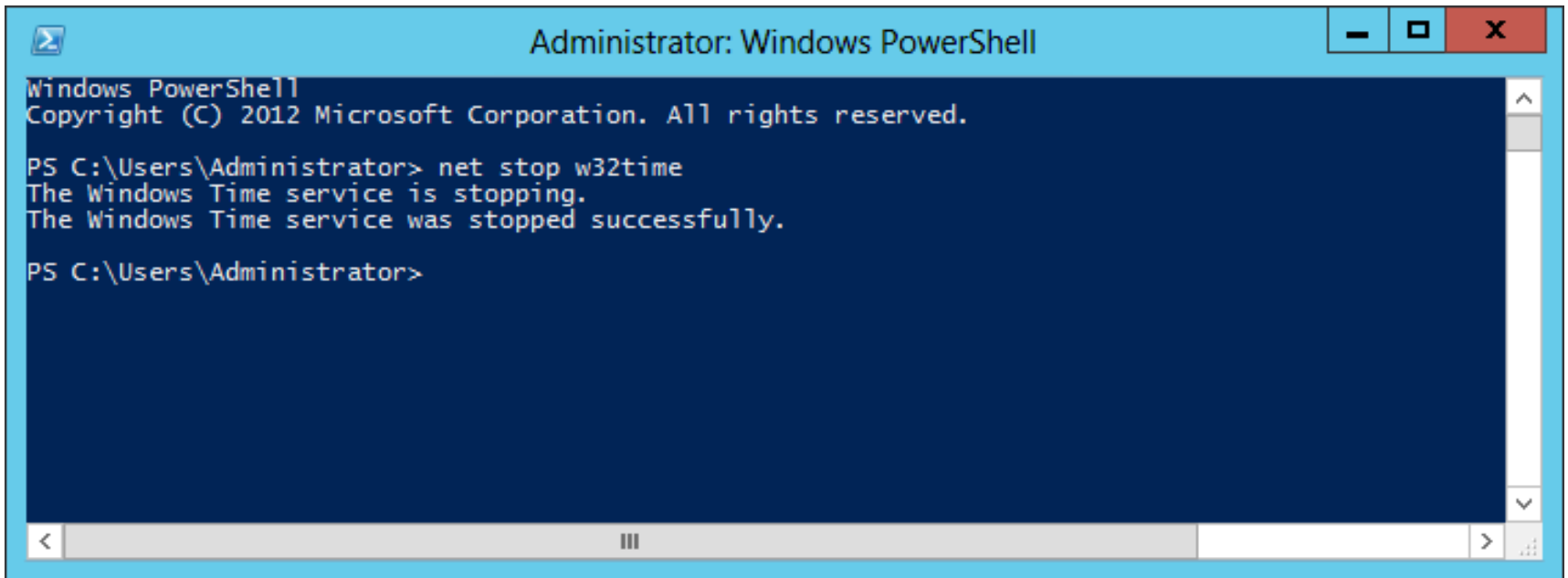


The screenshot shows a window titled "New Inbound Rule Wizard" with a close button (X) in the top right corner. The window is divided into two main sections. On the left is a "Steps:" sidebar with five items: "Rule Type", "Protocol and Ports", "Action", "Profile", and "Name". The "Name" step is currently selected and highlighted. The main area of the wizard is titled "Name" and contains the instruction "Specify the name and description of this rule." Below this instruction are two input fields. The first is labeled "Name:" and contains the text "NTP port". The second is labeled "Description (optional):" and contains the text "Connects to the NTP server". At the bottom right of the wizard are three buttons: "< Back", "Finish", and "Cancel".

Stop Windows Time Service

Now, we open the command prompt window and to stop the Windows Time Service we type:

```
Net stop w32time
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a blue title bar and standard Windows window controls (minimize, maximize, close) on the right. The main area is dark blue with white text. The text shows the command prompt prompt "PS C:\Users\Administrator>" followed by the command "net stop w32time". The output is "The Windows Time service is stopping." followed by "The Windows Time service was stopped successfully." The prompt "PS C:\Users\Administrator>" is shown again at the bottom. A scrollbar is visible on the right side of the text area.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

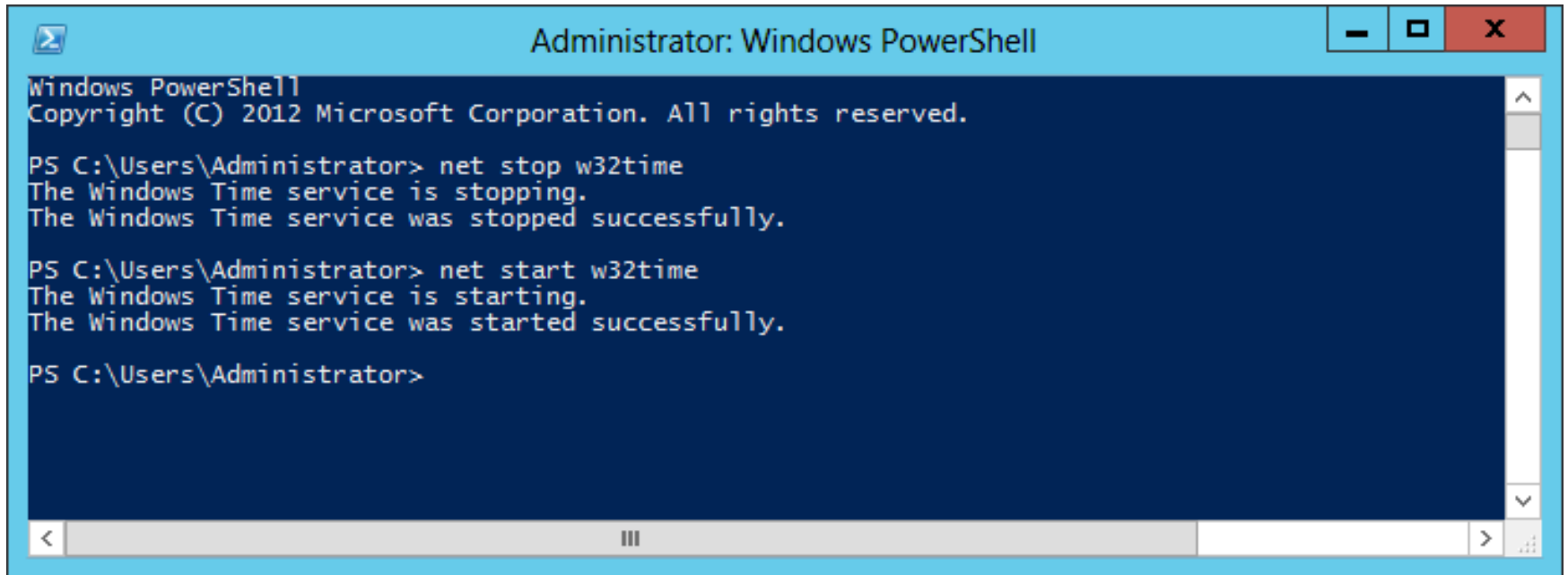
PS C:\Users\Administrator> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

PS C:\Users\Administrator>
```


Start Windows Time Service

To start the Windows Time Service we type:

```
Net start w32time
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

PS C:\Users\Administrator> net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

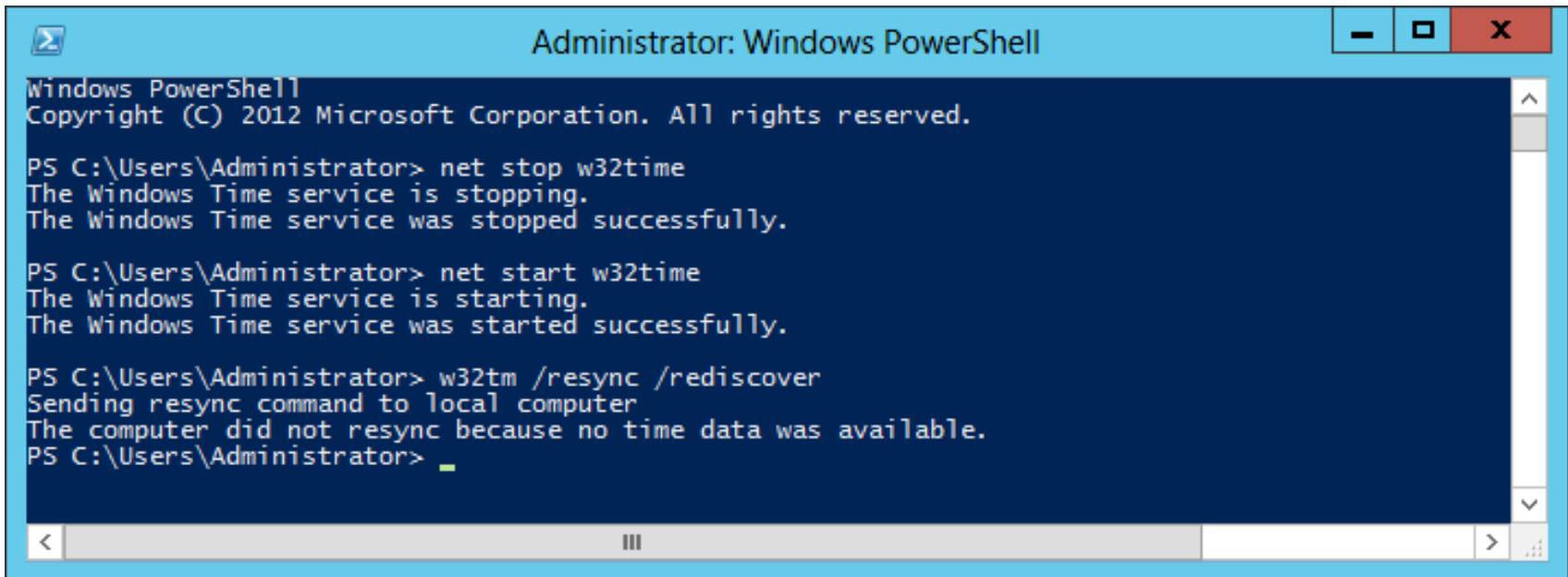
PS C:\Users\Administrator>
```

Resynchronize with the Time Source

To Resynchronize with the time source, we type:

```
W32tm /resync /rediscover
```

The time will synchronize with the source and the devices on the domain will now harmonize. We have completed the lesson and successfully edited the System Registry.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

PS C:\Users\Administrator> net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

PS C:\Users\Administrator> w32tm /resync /rediscover
Sending resync command to local computer
The computer did not resync because no time data was available.
PS C:\Users\Administrator> _
```