# Windows Event Logs Centralization

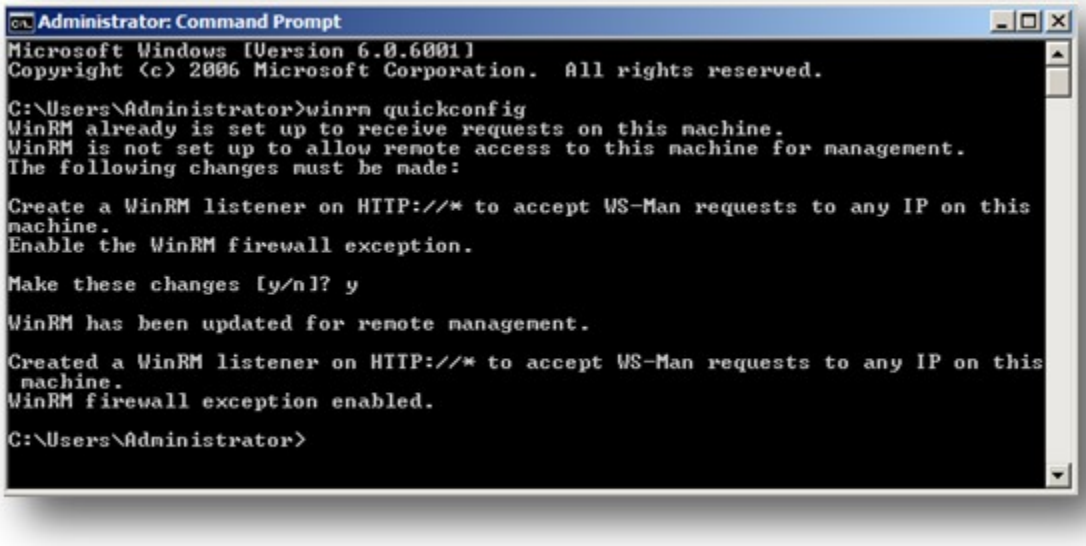
## We always have a requirement to centralized the Event Logs collection so that at one place you can review the logs came from any Windows machine.

**So, here are the configuration steps we can use to centralized Event logs management through Windows Event forwarding**

## Configuring the Event Collector(s)

**Configuring Event Collection Services and Windows Firewall**
In order for Source Computers to communicate with the Event Collector machine, the correct inbound firewall ports need to be open and accepting connections. In addition, the WinRM and Event Collector services need to be running.

**Configuration Steps**
1. On the **Event Collector** machine open a command prompt (Administrator Mode).
2. Type **winrm quickconfig**

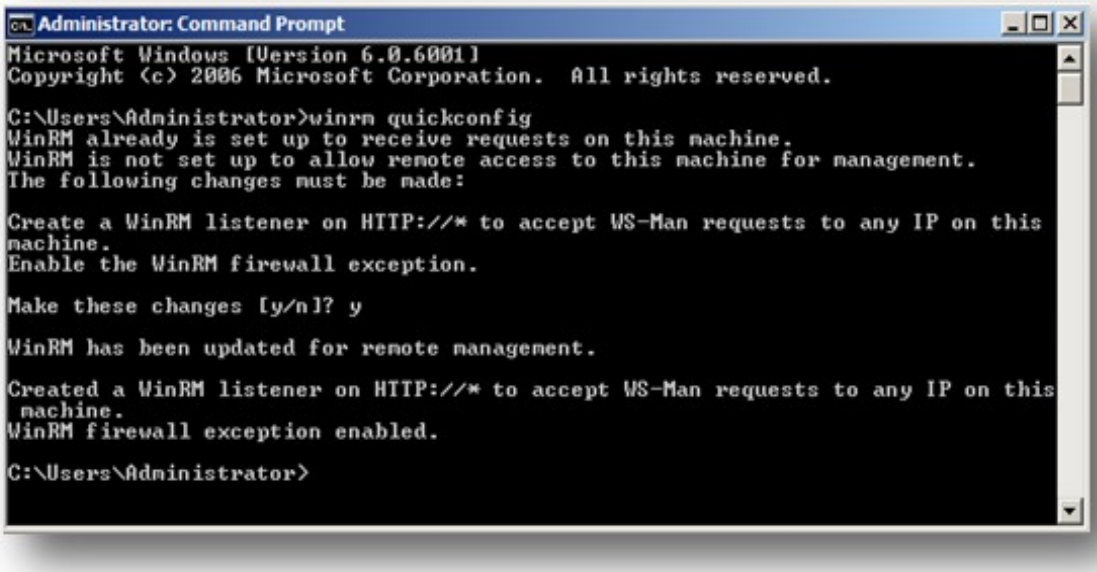



3. When prompted whether to continue with the configuration type **y**

This command will check the current configuration and make the necessary changes. Upon completion the following will have been configured:

**Windows Remote Management** service set to **Automatic (Delayed Start)** and **Started**.
Windows Firewall port(s) **Windows Remote Management (HTTP-In) Port 5985** configured for inbound communication OR Windows Firewall port(s) **Windows Remote Management (HTTP-In) – Compatibility Mode – Port 80** configured for inbound communication.

**Configuration steps**
4. Type **wecutil qc**




5. When prompted whether to continue with the configuration type **y**

This command will check the current configuration and make the necessary changes. Upon completion the following will have been configured:

**Windows Event Collector** service set to **Automatic (Delayed Start)** and **Started**

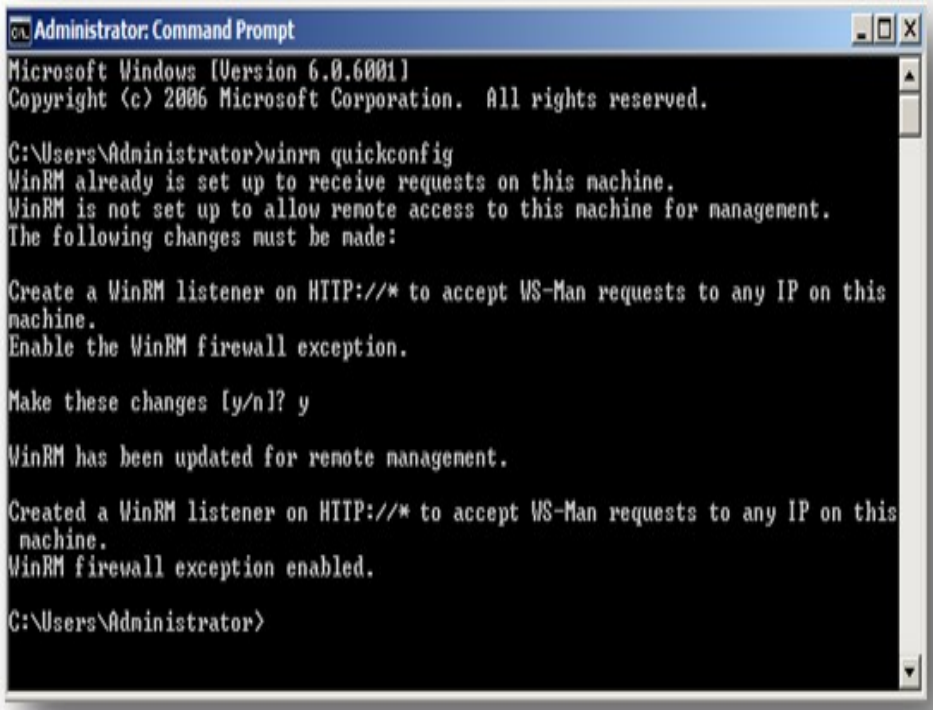
## Configuring Event Subscriptions

The Windows Event Forwarding architecture stores the subscription definition on the Event

Collector, in order to reduce the number of touch-points in case a subscription needs to be created or modified. The following subscription will be configured so that event source computers retrieve subscriptions from the event collector host (Source-Initiated subscriptions).

Subscriptions are defined on the Event Collector through the new Event Viewer user interface by selecting the **Create Subscription** action, when the **Subscriptions** node is highlighted. The Subscription may also be created via the **WECUTIL** command-line utility.

**Configuration Steps**
1. On the **Event Collector** open the **Event Viewer**.
2. Navigate to the **Subscriptions** node.
3. From the menu bar, choose **Action->Create Subscription…**
4. The **Subscriptions Properties** dialog will appear:

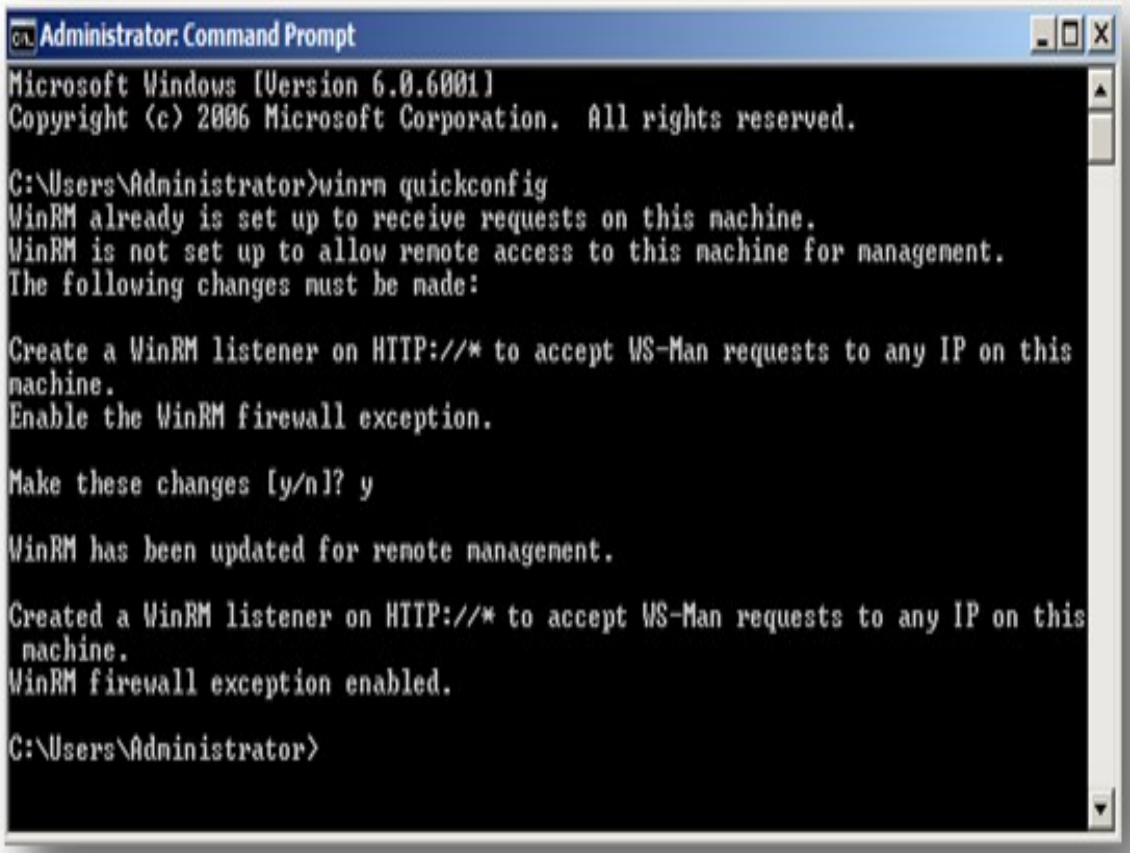



From here, you can specify a name, description, and the destination log (where the events will be collected).

5. Select **Forwarded Events** for the destination log.
6. Choose **Source Computer Initiated** (as Group Policy configures the Source Computer to contact the Event Collector for subscriptions settings).

**NOTE:** The **Subscription Type** can also be configured as **Collector initiated**. In this case Source Computers will need to be manually added to the Subscription either through the Subscription configuration or the WECUTIL command-line utility (which can also be scripted using PowerShell).
It is recommended that **Source computer initiated** is used, as this configuration is the most scalable.

7. Click **Select Computer Groups**.
8. Click **Add Domain Computers** and select the required Source Computers.

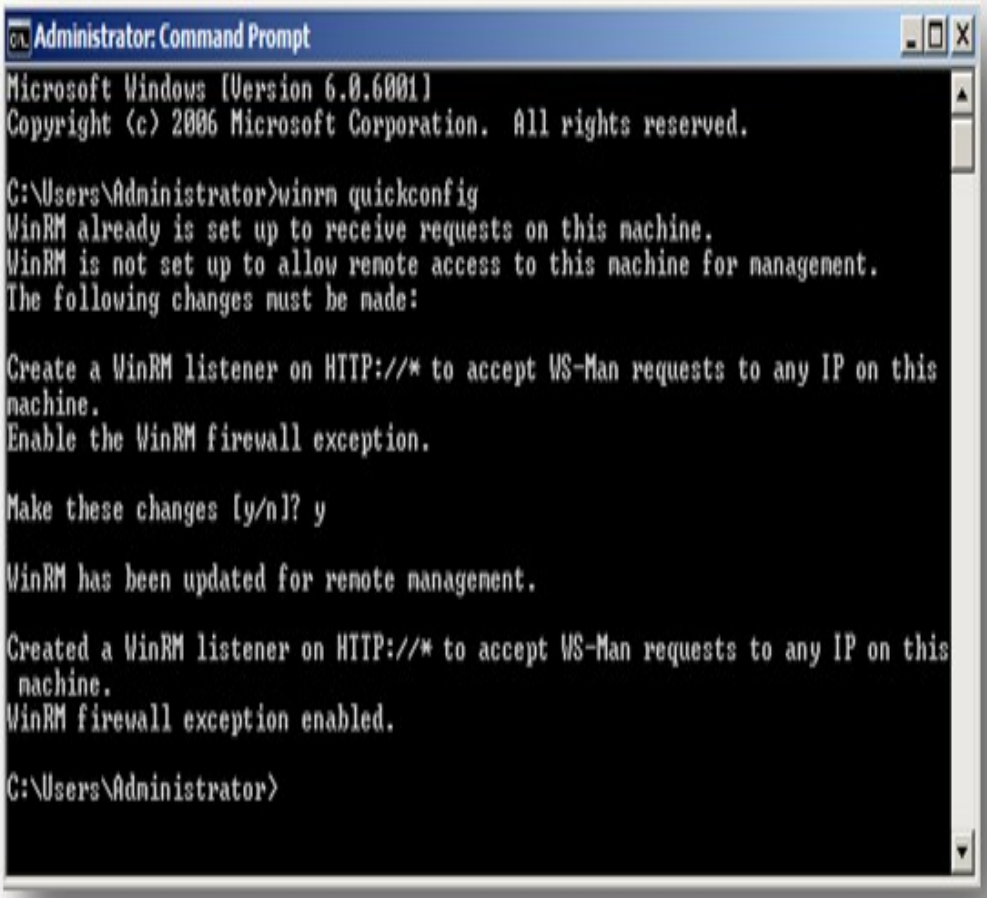



**NOTE:** It is recommended that a computer group which includes the required computer accounts, such as the**Domain Computers** group, is added to the subscription.

9. Click **OK** on the **Computer Groups** dialog.
10. Click **Select Events**.
11. Configure the following **Query Filter**:

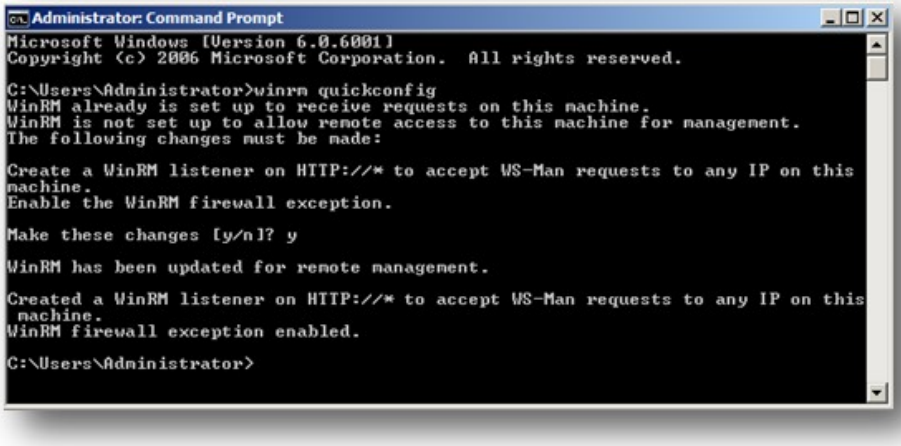
Select the desired **Event Level**

Select **By Log** and check **Windows Logs** to include the all types of windows logs




**NOTE:** In a production environment it may be advantageous to gather all events from the **Application** and**System** logs that have a level of **Critical**, **Error**, or **Warning**. This event scope can be expanded to gather all events from these logs or even add additional logs (like the **Security** log).

14. Select **Minimize Latency**.




**NOTE:**

**Normal**

This option ensures reliable delivery of events and does not attempt to conserve bandwidth. It is the appropriate choice unless you need tighter control over bandwidth usage or need forwarded events delivered as quickly as possible. It uses pull delivery mode, batches 5 items at a time and sets a batch timeout of 15 minutes.

**Minimize Bandwidth**

This option ensures that the use of network bandwidth for event delivery is strictly controlled. It is an appropriate choice if you want to limit the frequency of network connections made to deliver events. It uses push delivery mode and sets a batch timeout of 6 hours. In addition, it uses a heartbeat interval of 6 hours.

**Minimize Latency**

This option ensures that events are delivered with minimal delay. It is an appropriate choice if you are collecting alerts or critical events. It uses push delivery mode and sets a batch timeout of 30 seconds.

**Protocol**

HTTPS can be used to secure the communication channel. However, this requires additional configuration steps and requires the Event Collector to use a certificate, see the appendences for more information.

15. Click **OK** on the **Advanced Subscription** dialog.

16. Click **OK** on the **Subscription Properties** dialog.

17. You may get some issue while reading the logs. While the source machines forward their logs to the collection server it may show the Error ID 1234 cannot be found:

Description

"The description for Event ID xzy from source xyz cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer."

To fix this issue, use below command in Administrative Command Prompt:

**wecutil ss "Subscription Name" /cf:Events**

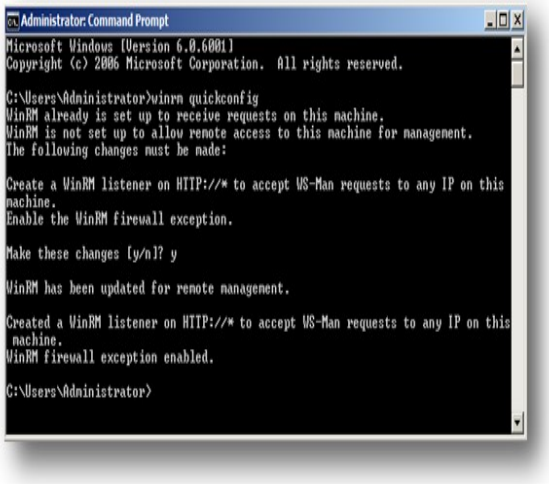
## Configuring the Source Computer(s)

Configuring the WinRM Service
In order for Source Computers to communicate with the Event Collector machine the Windows Remote Management (WinRM) service needs to be running on the Source Computers. WinRM service auto start is necessary for the host to retrieve subscription information from event collectors and send/push event data to the event collector.

The following Group Policy Settings are used to configure WinRM to support Event Forwarding:

Computer Configuration\Policies\Windows Settings\Security Settings**System Services**
**Configuration Steps**
1. Navigate to the **Windows Remote Management (WS-Management)** service.
2. Double click the service.

3. Check **Define this policy setting**.
4. Select the **Automatic** radio button.




5. Click **OK**.

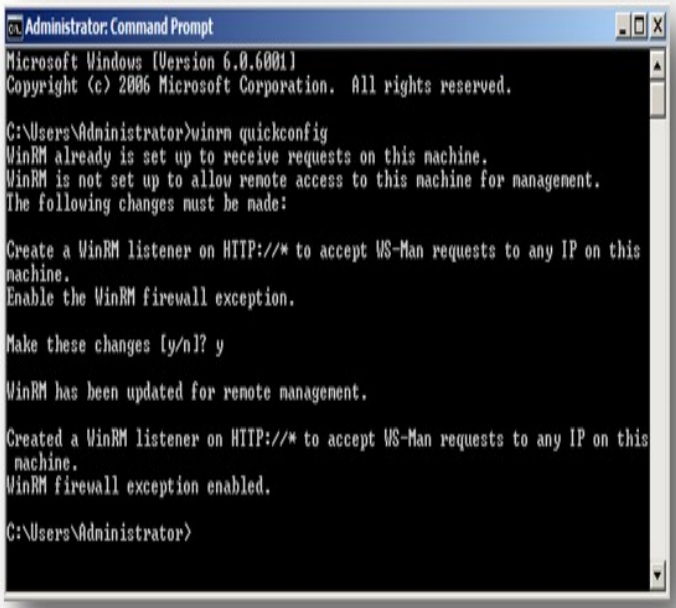
## Configuring the Event Collector(s) Server Address

Group Policy may be used to configure Source Computers (Clients) to forward events to a

collector (or set of collectors). The policy is very simple. It merely tells the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics. All of the other subscription details are held on the Event Collector.

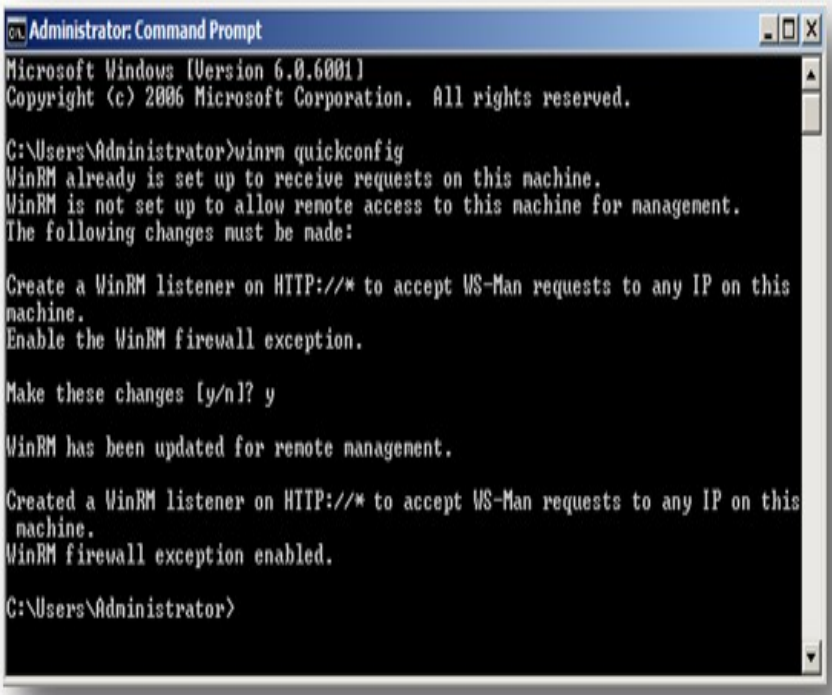
The following Group Policy Settings are used to configure event forwarding:

Computer Configuration\Policies\Administrative Templates\Windows Components**Event Forwarding**\




**Configuration Steps**

1. Edit the Group Policy Object (GPO) being used.
2. Configure the **Configure the server address…** option.
3. Set this to **Enabled**.
4. Click **Show**, the Subscription Managers dialog will be displayed.



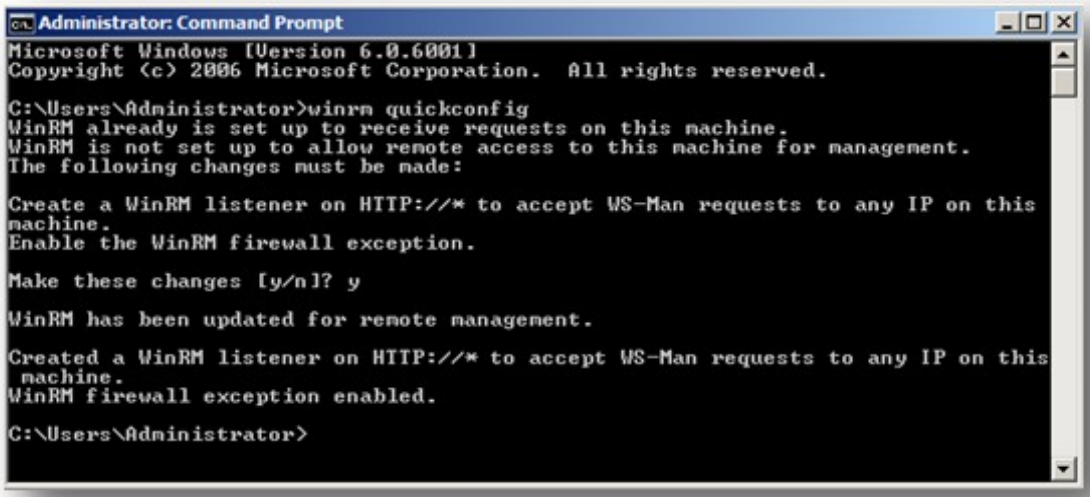

5. Click **Add** and enter the address of the **Event Collector**.

Ex:- **Server=computer.local**

6. Click **OK**.

**NOTE:** When editing Group Policy settings ensure that the Event Collector(s) and Source Computer(s) are under the management scope of the Group Policy Object being edited

**That's it. Know you can see that all the selected Event logs from Source computer(s) being forwarded to Event Collector Computer.**


Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>winrm quickconfig
WinRM already is set up to receive requests on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:
Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.
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 any IP on this machine.
WinRM firewall exception enabled.
C:\Users\Administrator>