Configure Computers to Forward and Collect Events

02/25/2015 3 minutes to read

Applies To: Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows Vista

Before you can create a subscription to collect events on a computer, you must configure both the collecting computer (collector) and each computer from which events will be collected (source). Updated information about event subscriptions may be available online at Event Subscriptions.

To configure computers in a domain to forward and collect events

1. Log on to all collector and source computers. It is a best practice to use a domain account with administrative privileges.
2. On each source computer, type the following at an elevated command prompt:

```
winrm quickconfig
```

> **Note**
>
> If you intend to specify an event delivery optimization of **Minimize Bandwidth** or **Minimize Latency** , then you must also run the above command on the collector computer.

3. On the collector computer, type the following at an elevated command prompt:

```
wecutil qc
```

4. Add the computer account of the collector computer to the **Event Log Readers Group** on each of the source computers.

> **Note**

By default, the **Local Users and Groups** MMC snap-in does not enable you to add computer accounts. In the **Select Users, Computers, or Groups** dialog box, click the **Object Types** button and select the **Computers** check box. You will then be able to add computer accounts.

5. The computers are now configured to forward and collect events. Follow the steps in Create a New Subscription to specify the events you want to have forwarded to the collector.

Additional Considerations

- In a workgroup environment, you can follow the same basic procedure described above to configure computers to forward and collect events. However, there are some additional steps and considerations for workgroups:
  - You can only use Normal mode (Pull) subscriptions.
  - You must add a Windows Firewall exception for Remote Event Log Management on each source computer.
  - You must add an account with administrator privileges to the Event Log Readers group on each source computer. You must specify this account in the Configure Advanced Subscription Settings dialog when creating a subscription on the collector computer.
  - Type `winrm set winrm/config/client @{TrustedHosts="<sources>"}` at a command prompt on the collector computer to allow all of the source computers to use NTLM authentication when communicating with WinRM on the collector computer. Run this command only once. Where `<sources>` appears in the command, substitute a list of the names of all of the participating source computers in the workgroup. Separate the names by commas. Alternatively, you can use wildcards to match the names of all the source computers. For example, if you want to configure a set of source computers, each with a name that begins with "msft", you could type this command `winrm set winrm/config/client @{TrustedHosts="msft*"}` on the collector computer. To learn more about this command, type `winrm help config.`
- If you configure a subscription to use the HTTPS protocol by using the **HTTPS** option in **Advanced Subscription Settings** , you must also set corresponding Windows Firewall exceptions for port 443. For a subscription that uses **Normal** (PULL mode) delivery optimization, you must set the exception only on the source computers. For a subscription that uses either **Minimize Bandwidth** or **Minimize Latency** (PUSH mode) delivery optimizations, you must set the exception on both the source and collector computers.

- If you intend to specify a user account by using the **Specific User** option in **Advanced Subscription Settings** when creating the subscription, you must ensure that account is a member of the local Administrators group on each of the source computers in step 4 instead of adding the machine account of the collector computer. Alternatively, you can use the Windows Event Log command-line utility to grant an account access to individual logs. To learn more about this command-line utility, type wevtutil sl -? at a command prompt.