Event Subscriptions

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

Event Viewer enables you to view events on a single remote computer. However, troubleshooting an issue might require you to examine a set of events stored in multiple logs on multiple computers.

Windows Vista includes the ability to collect copies of events from multiple remote computers and store them locally. To specify which events to collect, you create an event subscription. Among other details, the subscription specifies exactly which events will be collected and in which log they will be stored locally. Once a subscription is active and events are being collected, you can view and manipulate these forwarded events as you would any other locally stored events.

Using the event collecting feature requires that you configure both the forwarding and the collecting computers. The functionality depends on the Windows Remote Management (WinRM) service and the Windows Event Collector (Wecsvc) service. Both of these services must be running on computers participating in the forwarding and collecting process.

Configure Computers to Forward and Collect Events

37 out of 53 rated this helpful - Rate this topic

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:
3. `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.

4. On the collector computer, type the following at an elevated command prompt:
5. `wecutil qc`
6. Add the computer account of the collector computer to the local Administrators 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.

7. 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.

Create a New Subscription

18 out of 21 rated this helpful - Rate this topic

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

To receive forwarded events on a computer, you must set up one or more event subscriptions. Before setting up a subscription, you must configure both the computer that will receive the forwarded events, and the computer or computers that will forward the events. To learn how to configure the computers, see Configure Computers to Forward and Collect Events.

Once you have configured the computers, you create a subscription to specify which events to collect.

To create a new subscription

1. On the collector computer, run Event Viewer as an administrator.
2. Click **Subscriptions** in the console tree.

   Note

   If the Windows Event Collector service is not started, you will be prompted to confirm that you want to start it. This service must be started to create subscriptions and collect events. You must be a member of the Administrators group to start this service.

3. On the **Actions** menu, click **Create Subscription** .
4. In the **Subscription Name box** , type a name for the subscription.
5. In the **Description box** , enter an optional description.
6. In the **Destination Log box** , select the log file where collected events are to be stored. By default, collected events are stored in the ForwardedEvents log.
7. Click **Add** and select the computers from which events are to be collected.

   Note

After adding a computer, you can test connectivity between it and the local computer by selecting the computer and clicking **Test** .

8. Click **Select Events** to display the **Query Filter** dialog box. Use the controls in the **Query Filter** dialog box to specify the criteria that events must meet to be collected.
9. Click **OK** on the **Subscription Properties** dialog box. The subscription will be added to the **Subscriptions** pane and, if the operation was successful, the Status of the subscription will be Active.

Events raised on the forwarder computers that meet the criteria of the subscription will be copied to the collector computer log specified in step 6.

Additional Considerations

- You cannot use Event Viewer to create a subscription while it is connected to a remote computer.
- You can use the filter from a previously defined Custom View by choosing **Copy from existing Custom View** . Additionally, you can paste an XPATH query into the text box on the XML tab of the **Query Filter** dialog box.
- If a newly created subscription does not activate, you can open the **Subscription Properties** dialog box and select individual source computers to view the status for each of them.

Additional Resources

Configure Advanced Subscription Settings

12 out of 14 rated this helpful - Rate this topic

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

You can configure how collected events are delivered and specify the account used to manage the process of collecting events. Event Viewer provides three event delivery optimization options: **Normal** , **Minimize Bandwidth** and **Minimize Latency** . The following table lists each option along with a description of when it is an appropriate choice.

Event Delivery Optimization Options	Description
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.

The **Custom** event delivery option is never used when managing subscriptions created by using the Event Viewer snap-in. The Event Viewer can only create subscriptions with event delivery settings that correspond to the **Normal** , **Minimize Bandwidth** or **Minimize Latency** options. However, you can use Event Viewer to manage a subscription that was created or updated by using a different method, like the wecutil command-line tool. In that case, the **Custom** option is selected to indicate that the set of delivery settings of the subscription do not correspond to any of those supported by Event Viewer.

To configure advanced subscription settings

1. Perform steps 1—6 of the Create a New Subscription procedure.
2. Click **Advanced** .
3. On the **Advanced Subscription Settings** dialog box, you can either specify an event delivery optimization or specify the account used to manage the process of collecting events.
    - To specify an event delivery optimization: Select the **Event Delivery Optimization** option you want and click **OK** .
    - To specify the account used to manage the process of collecting events, select the **Specific User** option, then click **User and Password** and enter the user name and password of the account and click **OK** . Click **OK** on the **Advanced Subscription Settings** dialog box.

Additional Considerations

The **Minimize Bandwidth** and **Minimize Latency** options both batch a default number of items at a time. You can determine the value of this default by typing the following command at a command prompt:

winrm get winrm/config .

You can change the default number of items in a batch by typing the following command at a command prompt:

winrm set winrm/config @{MaxBatchItems=<NumberOfItems>}

The following example shows how to change the default number of batched items to five:

winrm set winrm/config @{MaxBatchItems="5"}

-