Knowledge Base

Detailed Usage of the Event Viewer /AUXSOURCE Switch Option

PSS ID Number: 312216

Article Last Modified on 10/13/2003

The information in this article applies to:

- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, 64-Bit Enterprise Edition
- Microsoft Windows XP Professional
- Microsoft Windows Small Business Server 2003, Premium Edition
- Microsoft Windows Small Business Server 2003, Standard Edition

---

This article was previously published under Q312216

SUMMARY

This article describes how to use the **/auxsource** switch to translate seemingly useless Event Viewer messages, such as the following one
The description for Event ID (1202) in Source (ClusSvc) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. One may be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details. The following information is part of the event: SAMMCPQCLU2, SAMMCPQCLU1, -4662149.
into useful troubleshooting information, such as the following message:
The time delta between node SAMMCPQCLU2 and node SAMMCPQCLU1 is -4662149(in 100 nanosecs).
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.
The two error messages are identical Event Viewer output. The difference is that the **/auxsource** switch is being used with second message.

This article describes:

- The default function of Event Viewer.
- How **/auxsource** works.
- How to use **/auxsource**.
- The syntax for **/auxsource**.
- Who can use **/auxsource**.
- Caveats for using **/auxsource**.

NOTE: This **/auxsource** information is currently not available in Windows XP Help.

MORE INFORMATION

The Default Function of Event Viewer

When you open a saved event log in Event Viewer, you have to select the type of event log to use: Application, Security, System, and so forth. The list of event log types is read from the computer that is hosting the .evt file and that is on a network share. This list is combined with the list of event log types that are on the computer that is running Event Viewer.

If the saved event log is either on a remote computer for which you are not a member of the Administrator group, or on a remote computer on which Remote Registry Service is not running, Event Viewer cannot retrieve information about the log types that are supported by the remote computer; therefore, you cannot retrieve event descriptions or categories if the actual type of the log is not included in this list, such as File Replication service (FRS), DNS, and Active Directory.

Even if the correct log type is included in this list, some events may have been generated by components that were installed only on the computer that generated the saved event log and not on the local computer or on the computer that is hosting the .evt file. In this case, descriptions and categories may be available for some events in the log but not for others.

How /AUXSOURCE Works

You can only use the **/auxsource** switch if you are running Event Viewer on a Windows XP Professional or Windows XP Server-based computer. You can also use this switch to read Microsoft Windows 2000 event logs, but only from a Microsoft Windows XP-based computer.

With the **/auxsource** switch, you can view saved event logs (.evt files) on a problematic computer. You can work with these logs locally or you can help a customer over the phone; however, refer to the "Caveats" section in this article to see the requirements for helping a customer with these logs.

The key to these messages is that the missing information is imbedded in the components to which the messages are related. For example, if an error message such as the one in the "Summary" section in this article is logged in Event Viewer and it references Microsoft SQL Server or Windows Clustering (or any other component or application), the information is not displayed because the message information is stored in the corresponding component or application. To view the information, you have to look at the event logs on that computer. With **/auxsource**, you can view the missing information even though you are not logged on to the computer that is experiencing the problem.

How to Use /AUXSOURCE

To use **/auxsource**, use the following methods:

- Start Event Viewer with the **/auxsource**, and then point it to the problematic computer over a network connection.

- Start Event Viewer with the **/auxsource**, and then point it to a reference server.

  A reference server is a computer that contains all of the software and the operating system components that the problematic computer contains. It is an image of the customer's computer, or (at least) a computer that is running the components for which you want to view the output. The reference server can also be the computer on which you view the logs, such as the local workstation; however, the local workstation must be running all of the same components as the problematic computer. In the case of a clustered computer with server software, this may not be possible unless you want to create a single-node cluster apart from your workstation.

/AUXSOURCE Syntax (Usage)

Use the following syntax for the **/auxsource** switch

```
mmc /a eventvwr.msc /auxsource=server
```

where you can reference *server* by:

- IP address

- Fully qualified domain name (FQDN)

- NetBIOS name

NOTE: The **/auxsource** switch is not case sensitive and *server* is either the reference server or the server that generates the event logs.

Requirements for /AUXSOURCE Users

To use **/auxsource**, you must be able to access the registry as an administrator on the server that is specified in the **/auxsource=server** syntax. If you are not logged on as an administrator on that server, you can either run Event Viewer by using the **runas** command or you can establish a connection to the IPC$ share of the **/auxsource=computer** syntax by using the following command-line syntax:

```
net use \\servername\ipc$ /u:domainname\username *
```

NOTE: If the remote computer does not allow remote registry access (possibly because Remote Registry Service is not running), you cannot use the **/auxsource=computer** syntax even if you are a member of the Administrator group on the remote computer.

The inability to establish the necessary security rights that are needed on the computer in the **/auxsource=computer** syntax is silent, which means that no errors are displayed; however, this becomes evident when you do not see the advanced log types in the **Open log file** dialog box. In place of the IPC$ connection, you can create matching user names and passwords in the domain of the server in **/auxsource=server**.

Caveats

Self Logging Applications and DNS, FRS, and Active Directory

When you are viewing logs for DNS, FRS, and Active Directory, Event Viewer must be running on a domain controller. You cannot use the **/auxsource** switch from a workstation or from a member server to view the log details.

The same caveat applies to programs such as Microsoft Exchange, which maintain their own logs and (or) write their logs to the System log or Application log; you have to be logged on to a computer with that type of software installed.

Windows 2000

You cannot use this switch to view log details when you are logged on to a Windows 2000-based computer; however, you can use the switch from a Windows XP-based computer to view the information in a log output from a Windows 2000-based computer. If you place the Windows XP file Els.dll, which enables the switch, on a Windows 2000-based computer, you receive the following error message:
"snap-in failed to initialize". Name: event Viewer ClSID:{975797fc-4e2a-11d0-b702-00c0rfd8dbf7
The **/auxsource** switch only works with the message type that is referenced in the "Summary" section in this article, and no other event log message is affected one way or another by the switch.

Keywords: kbenv kbinfo KB312216
Technology: kbSBServ2003Pre kbSBServ2003Search kbSBServ2003St kbSBServSearch kbWinServ2003Ent kbWinServ2003Ent64bit kbWinServ2003Ent64bitSearch kbWinServ2003EntSearch kbWinServ2003Search kbWinServ2003St kbWinXPPro kbWinXPProSearch kbWinXPSearch

---