Splunk® Enterprise Troubleshooting Manual 8.0.0

Troubleshoot Windows event log collection

Generated: 12/12/2019 7:58 am
Troubleshoot Windows event log collection

This topic discusses solutions to problems encountered when attempting to get Windows event log data into Splunk.

Problems with collection and indexing of Windows event logs generally fall into two categories:

- **Event logs are not collected from the server.** This is usually due to either a local configuration problem or, in the case of remote event log collection, a network, permissions, or authentication issue.
- **Event logs are collected from the server, but information within the event log is either missing or incorrect.** This is usually due to problems associated with a particular event log channel, or because of the methods used to collect data from those channels.

Troubleshooting issues with event logs collected locally

When you have problems getting data into your local Splunk instance, try these tips to fix the problem:

- Make sure that the desired event log channels are selected in Splunk Web or properly configured in inputs.conf.
- Make sure to select fewer than 64 event log channels per event log input.
- Make sure that you are not attempting to index exported event logs that are incompatible with the indexing system (for example, attempting to index event logs exported from a Windows Server 2008 computer on a Windows XP computer will result in missing log data).
- Make sure that, if you are monitoring non-standard event log channels, that you have the appropriate dynamic linked libraries (DLLs) that are associated with that event log channel. This is particularly important when indexing exported log files from a different computer.

Troubleshooting issues with event logs collected remotely

When you experience issues getting event logs from remote Windows servers, try these solutions to fix the problem:

- Make sure that your Splunk user is configured correctly for WMI.
- Make sure that your Splunk user is valid, and does not have an expired password.
• Make sure that the Event Log service is running on both the source and target machines.
• Make sure that your Active Directory (AD) is functioning correctly.
• Make sure that your computers are configured to allow WMI data between them.
• Make sure that your event logs are properly configured for remote access.

For more information

See the Admin Manual for information on getting started for Windows admins.