Docs / Windows / Apps / Win32 / Desktop Technologies / Diagnostic

Windows Event Collector

Article • 08/19/2020 • 2 minutes to read • 5 contributors

You can subscribe to receive and store events on a local computer (event collector) that are forwarded from a remote computer (event source). The Windows Event Collector functions support subscribing to events by using the WS-Management protocol. For more information about WS-Management, see About Windows Remote Management.

Event Forwarding and Event Collection Architecture

Event collection allows administrators to get events from remote computers and store them in a local event log on the collector computer. The destination log path for the events is a property of the subscription. All data in the forwarded event is saved in the collector computer event log (none of the information is lost). Additional information related to the event forwarding is also added to the event. For more information about how to enable a computer to receive collected events or forward events, see Configure Computers to Forward and Collect Events.

Subscriptions

The following list describes the types of event subscriptions:

- Source-initiated subscriptions: allows you to define an event subscription on an event collector computer without defining the event source computers. Multiple remote event source computers can then be set up (using a group policy setting) to forward events to the event collector computer. For more information, see Setting up a Source Initiated Subscription. This subscription type is useful when you do not know or you do not want to specify all the event sources computers that will forward events.
- Collector-initiated subscriptions: allows you to create an event subscription if you know all the event source computers that will forward events. You specify all the event sources at the time the subscription is created. For more information, see Creating a Collector Initiated Subscription.

Windows Event Collector Functions

For more information and code examples that use the Event Collector functions, see Using Windows Event Collector.

For more information about the functions used to collect and forward events, see Windows Event Collector functions.

Recommended content

Appendix L - Events to Monitor

Learn more about: Appendix L: Events to Monitor

Using Windows Event Collector - Win32 apps

This section lists the topics that explain the tasks that can be accomplished using the Windows Event Collector SDK. Code examples and explanations for all the tasks are included in each of the following topics.

Creating a Collector Initiated Subscription - Win32 apps

You can subscribe to receive events on a local computer (the event collector) that are forwarded from remote computers (the event sources) by using a collector-initiated subscription.

4624(S) An account was successfully logged on. (Windows 10) - Windows security

Describes security event 4624(S) An account was successfully logged on.

Use Windows Event Forwarding to help with intrusion detection (Windows 10) - Windows security

Learn about an approach to collect events from devices in your organization. This article talks about events in both normal operations and when an intrusion is suspected.

Best practice of configuring EventLog forwarding performance - Windows Server

This article introduces the best practice of configuration of EventLog forwarding in a large environment.

4663(S) An attempt was made to access an object. (Windows 10) - Windows security

Describes security event 4663(S) An attempt was made to access an object.

4688(S) A new process has been created. (Windows 10) - Windows security

Describes security event 4688(S) A new process has been created. This event is generated when a new process starts.

Show more ∨