TASK-12

What is Win collect?

WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows logs to QRadar. WinCollect can collect events from systems locally or be configured to remotely poll other Windows systems for events.

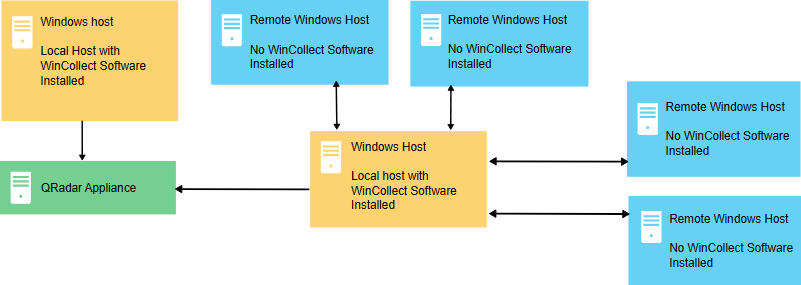
How does WinCollect Work?

WinCollect uses the Windows Event Log API to gather events, and then WinCollect sends the events to QRadar.

WinCollect stand-alone deployment

If you need to collect Windows events from more than 500 agents, use the stand-alone WinCollect deployment. A stand-alone deployment is a Windows host in unmanaged mode with WinCollect software installed. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to QRadar. To save time when you configure more than 500 Windows agents, you can use a solution such as IBM Endpoint Manager. Automation can help you manage stand-alone instances.

Figure 1. WinCollect stand-alone deployment example



WinCollect stand-alone deployment example

You can also deploy stand-alone WinCollect to consolidate event data on one Windows host, where WinCollect collects events to send to QRadar.

Stand-alone WinCollect mode has the following capabilities:

* You can configure each WinCollect agent by using the WinCollect Configuration Console.
* You can update WinCollect software with the software update installer.
* Event storage to ensure that no events are dropped.
* Collects forwarded events from Microsoft Subscriptions.
* Filters events by using XPath queries or exclusion filters.
* Supports virtual machine installations.
* Send events to QRadar using TLS Syslog.
* Automatically create a local log source at the time of agent installation.