Name :- M Om Nivas Reg no :- 21BCE9706

E-mail :- omnivas.21bce9706@vitapstudent.ac.in

Task – 12

Win-Collect and Standalone Win-Collect

Win-Collect Overview :-

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.

WinCollect is one of many solutions for Windows event collection. For more information about alternatives to WinCollect

How does WinCollect Work?

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

Note: Managed deployment is not supported in QRadar on Cloud environments. Customers who use IBM QRadar on Cloud must use stand-alone WinCollect agents.

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.

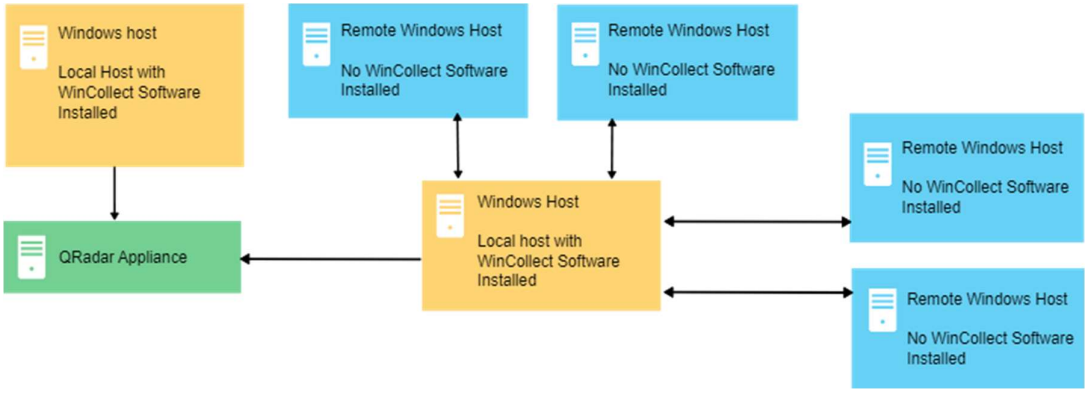

Figure 1. WinCollect stand-alone deployment example

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.

Setting up a stand-alone WinCollect deployment

For a stand-alone deployment, follow these steps:

1. Understand the prerequisites for stand-alone WinCollect, which ports to use, what hardware is required, how to upgrade. For more information, see Installation prerequisites for WinCollect.
2. Install stand-alone WinCollect agents on the Windows hosts. For more information, see Installing the WinCollect agent on a Windows host.
3. If you want to add new log sources to your agent or modify existing log sources, install the WinCollect stand-alone configuration console. For more information, see Installing the configuration console or Silently installing, upgrading, and uninstalling WinCollect software.
4. Configure the destination where the Windows hosts send Windows events. For more information, see Adding a destination to the WinCollect Configuration Console.

5. If you want to use the stand-alone WinCollect agent to collect events from other devices using remote polling, create a credential in the WinCollect stand-alone configuration console, so that WinCollect can log in to the remote devices. For more information, see Creating a WinCollect credential.
6. If you want to add additional log sources to the stand-alone WinCollect agent, do so using the WinCollect stand-alone configuration console. For more information see Adding a device to the WinCollect Configuration Console.

Stand-alone WinCollect Installations

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 IBM® QRadar®.

- **WinCollect Configuration Console overview**
  In stand-alone deployments, use the WinCollect Configuration Console to manage your WinCollect deployment. Use the WinCollect Configuration Console to add devices that you want WinCollect to collect agents from, and add the IBM QRadar destination where you want to send events.
- **Installing the configuration console**
  Download and install the WinCollect configuration console to manage your stand-alone deployment. You can choose an option to install just the WinCollect patch, if you are deploying WinCollect on a large number of Windows hosts that do not require the configuration console.
- **Silently installing, upgrading, and uninstalling WinCollect software**
  Enter a command to complete all installation and upgrading tasks for the WinCollect stand alone patch, and the WinCollect Configuration Console, rather than using the installation wizard. You can also upgrade WinCollect agents by using the agent installer only.
- **Setting an XPath parameter during automated installation**
  In WinCollect V 7.2.8 and later, you can add an XPath parameter to your command line installer for stand-alone WinCollect agent installations.

END