TASK-12 11/09/23 Sameer Chauhan

**Aim**-we have to write about win collect and stand alone win collect



**Win Collect Overview**

Win Collect is a Syslog event forwarder that administrators can use to forward events from Windows logs to JSA. Win Collect can collect events from systems locally or be configured to remotely poll other Windows systems for events .Win Collect is one of many solutions for Windows event collection.

**How Does Win Collect Work?**

Win Collect uses the Windows Event Log API to gather events, and then Win Collect sends the events to JSA.

## Win Collect Managed Deployment

A managed Win Collect deployment has a JSA appliance that shares information with the Win Collect agent installed on the Windows hosts that you want to monitor. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the Win Collect software installed. The Windows host with Win Collect software installed polls the remote hosts, and then sends event information to JSA.

Here is a chart showing win collect deployment example:

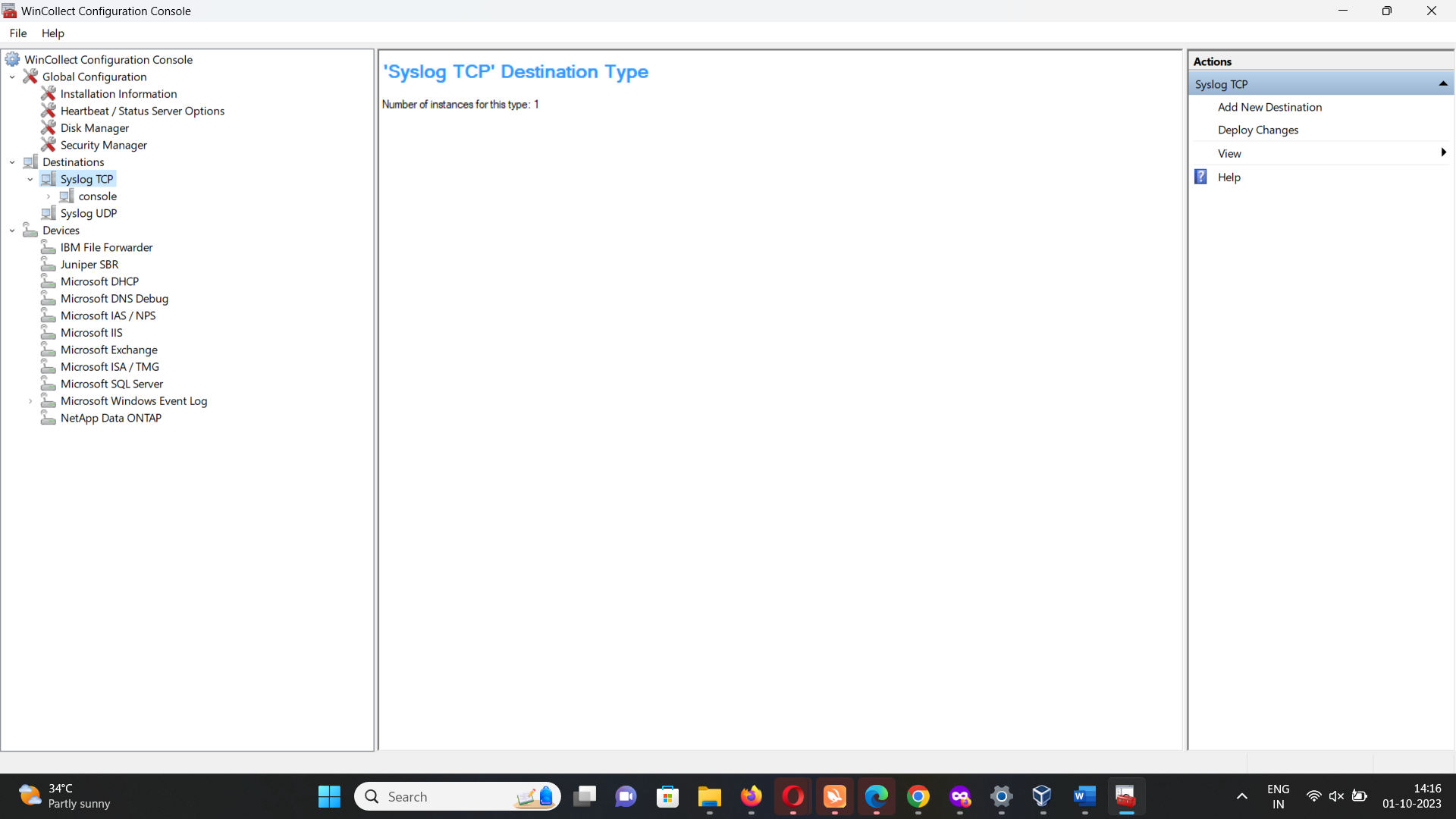
WinCollect
Managed Deployment Example 

In a managed deployment, Win Collect is designed to work with up to 500 Windows agents per Console and managed host. For example, if you have a deployment with a Console, an Event Processor, and an Event Collector, each can support up to 500 Windows agents, for a total of 1,500. If you want to monitor more than 500 Windows agents per Console or managed host, use the stand-alone Win Collect deployment.

The managed Win Collect deployment has the following capabilities:

* Central management from the JSA Console or managed host.
* Automatic local log source creation at the time of installation.
* 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.
* Console can send software updates to remote Win Collect agents without you reinstalling agents in your network.
* Forwards events on a set schedule (Store and Forward)

Here we can see Win Collect Configuration Console installed in our pc:



What is stand alone Win Collect ?

A stand-alone deployment is **a Windows host in unmanaged mode with Win Collect 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 Win Collect software installed.

**Win Collect Stand-alone Deployment**

If you need to collect Windows events from more than 500 hosts, use the stand-alone Win Collect deployment. A stand-alone deployment is a Windows host in unmanaged mode with Win Collect 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 Win Collect software installed. The Windows host with Win Collect software installed polls the remote hosts, and then sends event information to JSA. To save time when you configure more than 500 Windows hosts, you can use a solution such as Juniper Networks Endpoint Manager. Automation can help you manage stand-alone instances.

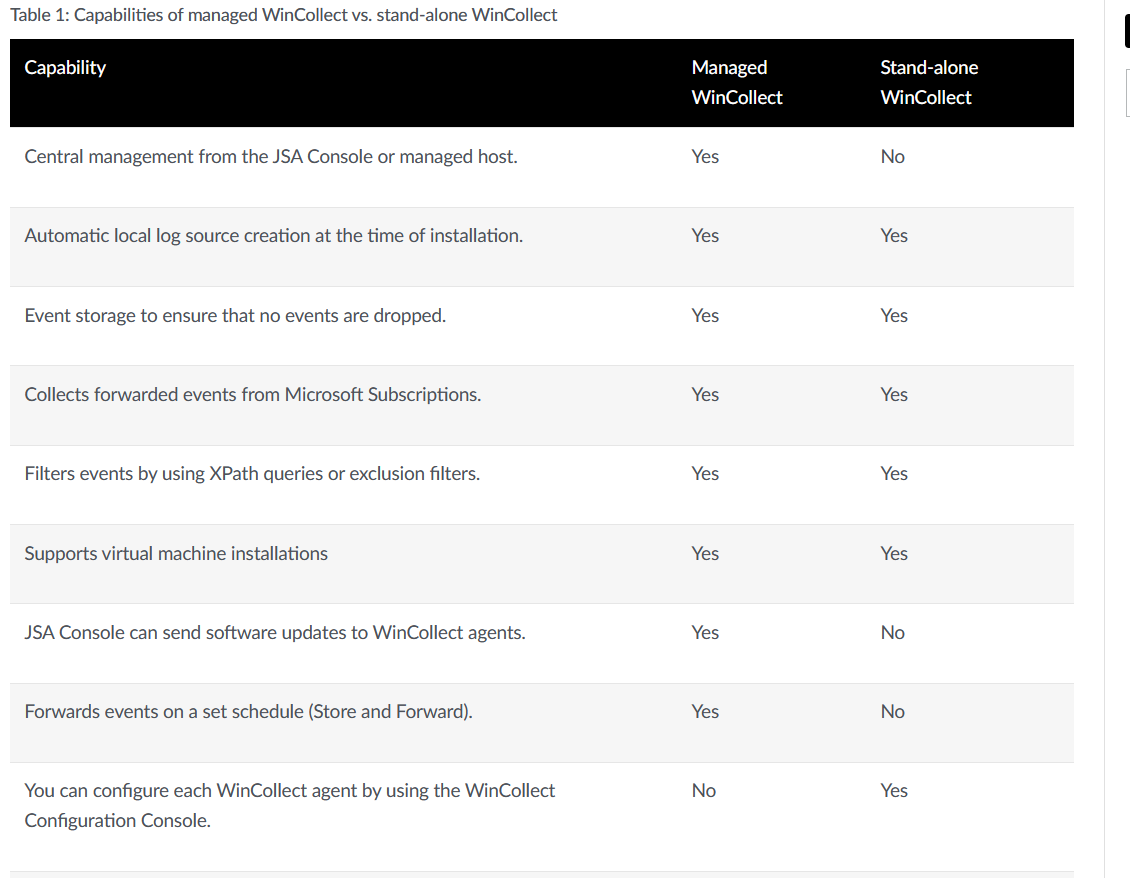
Here we can see stand alone Win Collect deployment example:

WinCollect Stand-alone Deployment
Example

We can also deploy stand-alone Win Collect to consolidate event data on one Windows host, where Win Collect collects events to send to JSA.

Stand-alone Win Collect mode has the following capabilities:

* You can configure each Win Collect agent by using the Win Collect Configuration Console.
* You can update Win Collect 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.
* Sends events to JSA using TLS Syslog.
* Automatically create a local log source at the time of agent installation.



Above image tells us the difference in managed vs stand alone win collect agent

**Log Sources for Win Collect Agents**

A Win Collect agent can collect and forward events from the local system or remotely poll a number of Windows-based log sources and operating systems for their events.

You can add log sources that communicate through a Win Collect agent individually for remote polling. If the log sources contain similar configurations, you can simultaneously add multiple, or bulk add log sources. A change to an individually added log source updates only the individual log source. A change that you make to a group of log sources updates all of the log sources in the log source group. You can add a local log source for local collection. You can create a log source manually, if it wasn't auto created.