QRadar integration has always been a stained-glass window for many of us, be it either an experienced SIEM professional dealing with a new device integration or a SIEM professional in his/her early phase of SIEM journey.

For one such scenario, here are my two cents to avoid such time-consuming researches and hit-and-trials for windows server integrations based on different types of QRadar setups.

Though QRadar is flexible with environmental setups, it is also equally flexible with integration of windows devices, but that flexibility comes at a cost of confusion for many of us. Questions like which integration is best out of

* Syslog (Intended for Snare, BalaBit, and other third-party Windows solutions).
* Forwarded.
* TLS Syslog.
* TCP Multiline Syslog
* Windows Event Log (WMI)
* Windows Event Log Custom (WMI).
* WinCollect.
* WinCollect NetApp Data ONTAP.
* Amazon Web Services protocol from AWS CloudWatch.
* Microsoft Azure Event Hubs.

Now we are only going to discuss the predominant ways of integration, in this post, which are WMI and WinCollect. And how one is better than the other.

**Summary: Table of deployment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nature of WinCollect Deployment** | **Advantages** | **Limitations** | **Ideal for Enterprise** | **Comments** |
| **Managed Wincollect** | * Easy to identify errors using wincollect events. * Easy to integrate multiple log types from same server (Applications/Forwarded events etc.). * Less resource utilization on ECs/EPs since it’s based on push mechanism. * Easy upgrade of wincollect agents. * Filtering of events and using X-path queries are a treat for EPS reduction. | Only 500 WinCollect Agents are recommended per managed host in an environment. | Every distributed QRadar environment. | If the managed hosts (ECs/EPs) are location specific, then while installing wincollect, using closest managed host as configuration server is best. |
| **Standalone WinCollect** | * No limitation on heartbeat management per managed host. * No authentication token is needed | * Centralized upgrade is not possible. * Non logging troubleshooting may become tedious. | Environment where count of windows server is higher than the available QRadar managed hosts can support for heartbeats. | Should only go for this when endpoint management is strong in the environment. (SCCM/bigfix etc for agent upgrades) |
| **Using Intermediate Jump server for MSRPC polling** | Easy to designate and distribute servers per agent server, | * Centralized credentials used for MSRPC can be compromised. * If the agent server gets disconnected logs can fill up the space of the agent server. * Ports needed for MSRPC are vulnerable in general | Enterprise where segment level security is strong, and credentials can be vaulted for better safety. | I do not recommend this method over managed one as it costs a lot of inconvenience for its value delivered. |

For better understanding on Managed Wincollect please check Annexure I.

For better understanding of Standalone WinCollect and Using Intermediate Jump server for MSRPC polling please refer [Click Here](https://www.ibm.com/docs/en/SSKMKU/com.ibm.wincollect.doc/b_wincollect.pdf)

Annexure I

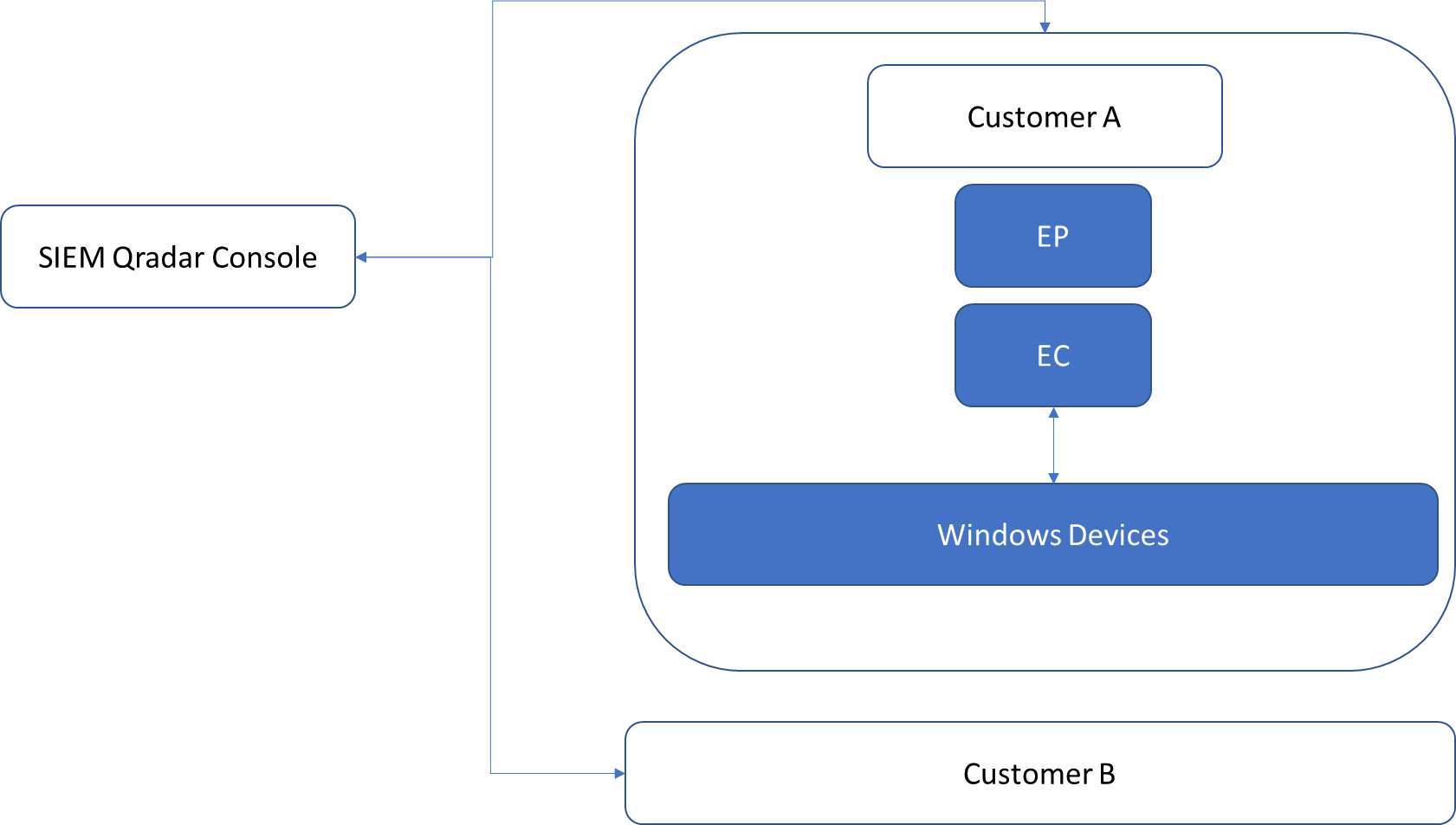
Abbreviations:

|  |  |
| --- | --- |
| EP | Event Processor |
| EC | Event Collector |
| DC | Data Center |
|  |  |

# QRadar Setup 1: Managed Security Service Provider (MSSP)

## Scenario 1: Tenants with EPs/ECs hosted in one data center location

In this example, the tenant has EP/EC in one location which is then connected to MSSP console.

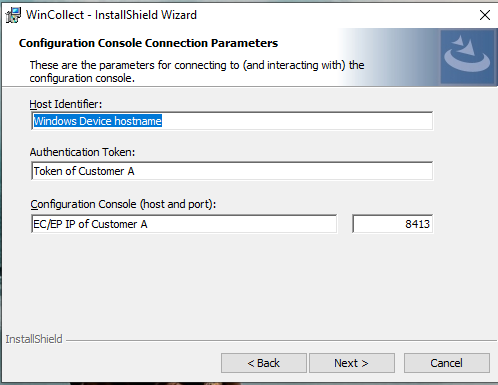


### Which windows Integration method is best suited for such scenario?

### Integration Solution:

Managed WinCollect installation, and the WinCollect management server should be kept local EC/EP IP to avoid multiple connection threats to MSSP console and avoiding security risks as well.

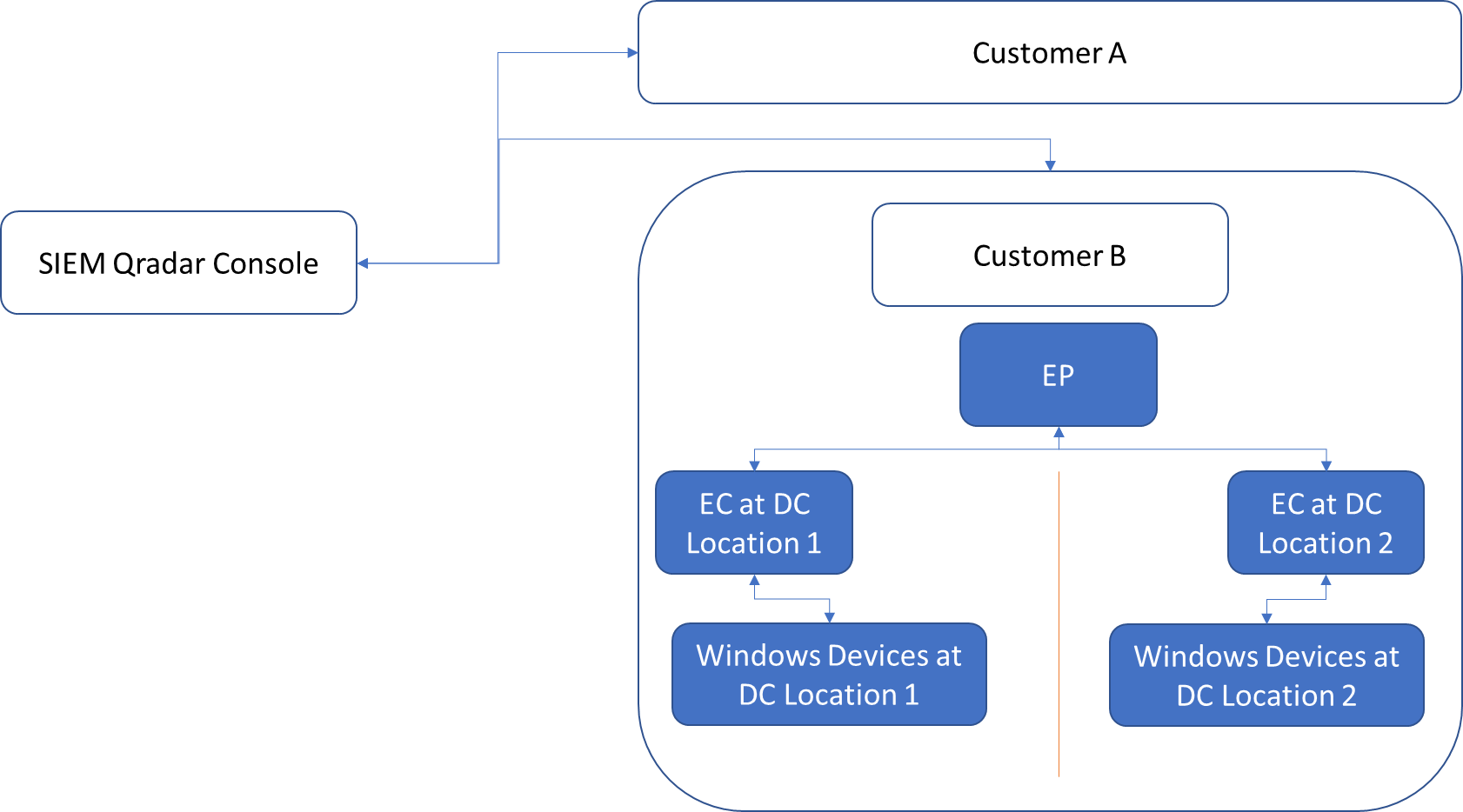
Example: All the WinCollect installed on windows devices at customer A will have management and status server as EC/EP IP of customer A.



Following command can install the wincollect using a batch file provided the installer should be at the directory from where the command is executed.

wincollect-7.3.1-16.x64.exe /s /v"/qn INSTALLDIR=\"C:\Program Files\IBM\WinCollect\" AUTHTOKEN=7545b39c-0fff-490c-9554-2682217ce7a2 FULLCONSOLEADDRESS=192.168.1.17:8413 HOSTNAME=DESKTOP-JB79938 LOG\_SOURCE\_AUTO\_CREATION\_ENABLED=True LOG\_SOURCE\_AUTO\_CREATION\_PARAMETERS=""Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=DESKTOP-JB79938&Component1.LogSourceIdentifier=DESKTOP-JB79938&Component1.Log.Security=true&Component1.Log.System=true&Component1.Log.Application=true&Component1.Log.DNS+Server=false&Component1.Log.File+Replication+Service=false&Component1.Log.Directory+Service=false&Component1.Destination.Name=192.168.1.17&Component1.RemoteMachinePollInterval=3000&Component1.EventRateTuningProfile=High+Event+Rate+Server&Component1.MinLogsToProcessPerPass=1250&Component1.MaxLogsToProcessPerPass=1875"""

## Scenario 2: Tenants with EPs/ECs hosted in different data center locations

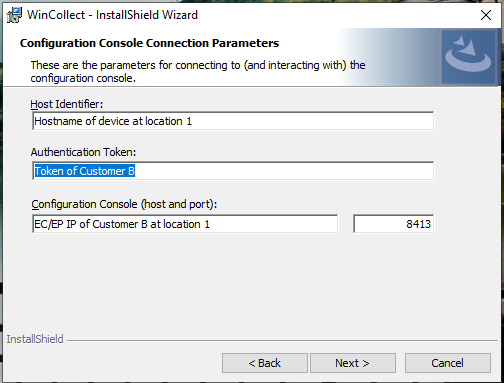


### Which windows Integration method is best suited for such scenario?

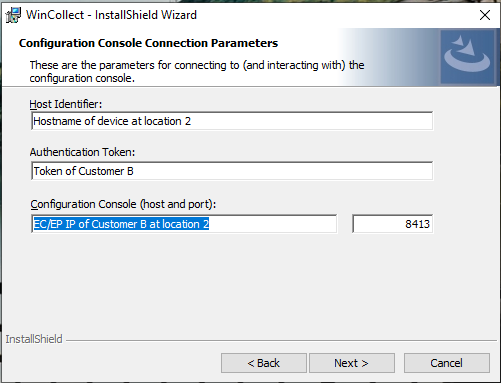
### Integration Solution:

Managed WinCollect installation, and the WinCollect management server should be kept local EC/EP IP to avoid multiple connection threats to MSSP console and avoiding security risks as well.

Example: For customer B, All the WinCollect installed on windows devices at DC location 1 will have management and status server as EC at DC location 1.



Similarly, all the WinCollect installed on windows devices at DC location 2 will have management and status server as EC at DC location 2.



Following command can install the wincollect using a batch file provided the installer should be at the directory from where the command is executed.

wincollect-7.3.1-16.x64.exe /s /v"/qn INSTALLDIR=\"C:\Program Files\IBM\WinCollect\" AUTHTOKEN=7545b39c-0fff-490c-9554-2682217ce7a2 FULLCONSOLEADDRESS=192.168.1.17:8413 HOSTNAME=DESKTOP-JB79938 LOG\_SOURCE\_AUTO\_CREATION\_ENABLED=True LOG\_SOURCE\_AUTO\_CREATION\_PARAMETERS=""Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=DESKTOP-JB79938&Component1.LogSourceIdentifier=DESKTOP-JB79938&Component1.Log.Security=true&Component1.Log.System=true&Component1.Log.Application=true&Component1.Log.DNS+Server=false&Component1.Log.File+Replication+Service=false&Component1.Log.Directory+Service=false&Component1.Destination.Name=192.168.1.17&Component1.RemoteMachinePollInterval=3000&Component1.EventRateTuningProfile=High+Event+Rate+Server&Component1.MinLogsToProcessPerPass=1250&Component1.MaxLogsToProcessPerPass=1875"""

# QRadar Setup 2: In House Security Operation Center (SOC)

## Scenario 1: SOC with limited number of EPs/ECs and huge inventory of windows devices

In such setup it is best to follow the recommended managed wincollect load per managed host, which is 500 wincollect managed by each host (i.e. EP/EC/Console).

Example: If the organization has a console, 1 EP and 1 EC in the environment, as per recommended managed wincollect installation per host, the organization can have 500 wincollect configured for each managed host, a total of 1500 managed wincollects for all the managed hosts of QRadar.

And hence it is advisable to evaluate the inventory and QRadar component mapping, if the load exceeds, it is recommended to use a hybrid model where a wincollect is hosted as an agent server for log polling from devices using WMI protocol.

## Scenario 2: SOC with large inventory of EPs/ECs and windows devices

In an environment which is large enough to host multiple ECs/Eps, evaluation of Inventory available and possible expansion of devices, to managed hosts of existing QRadar setup and possible scalability of it, must be done, before finalizing integration methods of windows devices.