



QRadar Support 101: WinCollect Troubleshooting

A discussion about WinCollect, troubleshooting, when to contact support, tips and other helpful information.

<https://ibm.biz/JoinQRadarOpenMic>



Disclaimer

Please Note:

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Let's talk about WinCollect 7.2.8

- Combined logs for troubleshooting
- Statistics discussion
- Exchange updates
- IIS updates



Combined logs for troubleshooting

Simplified logging in WinCollect 7.2.8 combines several log files in to a single entry for the agent. The best option with support is to always zip both the logs and config directories (See <https://ibm.biz/qradarlogs>)

WinCollect 7.2.7 and earlier agent log structure:

- C:\program files\IBM\WinCollect\logs\WinCollect_Code_Active.log
- C:\program files\IBM\WinCollect\logs\WinCollect_Device_Active.log
- C:\program files\IBM\WinCollect\logs\WinCollect_System_Active.log

WinCollect 7.2.8 agent log structure:

- C:\program files\IBM\WinCollect\logs\WinCollect.log

```
INFO System.ComponentFactory : Service DestinationManager v7.2.8 initialized
INFO Code.PayloadRouter : Using 3 router threads.
INFO Code.PayloadRouter : Using stats sweep period of 30 seconds.
INFO System.ComponentFactory : Service PayloadRouter v7.2.8 initialized
INFO Device.Windows2008EventCollector : Windows2008 Event Collector 7.2.8.91 initialized, enabled
INFO System.ComponentFactory : Service Windows2008EventCollector v7.2.8 initialized
INFO Device.Service.DeviceWindowsLog : Initializing...
INFO Device.Service.DeviceWindowsLog : Overriding thread pool type with type AdaptiveThreadPool.
INFO Device.WindowsLog.WindowsLogDeviceReaderPool : Monitoring Windows Log Application on JPs Laptop every 3000 msecs
```

System (about the WinCollect Agent) – agent version, operating system info, host RAM/CPU, service info.

Code (configuration info) – start up, shutdown, spillover events, file locations unavailable, token issues.

Device (event collection) – logs being opened (application, security, system), error codes returned, permissions, authentication issues, tuning messages (falling behind)

Statistics log file

A new statistics file is provided in the logs for administrators. This is useful not only to understand tuning, but to investigate agents deployments or move log sources around when remotely polling sources as 2,500 is the maximum EPS for remote polling.

- Minutes field is an average event/second value for the log type.
- Hours field is an Average/Maximum event/second value.
- Days field is an Average/Maximum event/second value.
- trg field is the target (outgoing/destination) event/second value.

```
Stat Collection from 09-19 14:50:37 to 09-19 16:05:37 :  
EvtLog.172.18.233.54.Application 60 Minutes: AVG 2220 2100 ...  
==>> 24 Hours: AVG/MAX 2121/2455 1921/2430 1577/2300 1684/2341 ...  
==>> 3 Days: AVG/MAX 2011/2482 1675/1939 ...
```

```
Stat Collection from 05-02 12:30:05 to 05-02 12:40:05 :  
EvtLog.192.168.1.15.Application 10 Minutes: AVG 2174 2085 2129 2129 2130 2089 2129  
EvtLog.192.168.1.15.Security 10 Minutes: AVG 0.10 0.10 0.05 0.02 0.05 0.10 0 0 0.07  
EvtLog.192.168.1.15.System 10 Minutes: AVG 0.02 0.04 0.04 0.02 0 0.02 0.04 0 0.04  
trg.QRadar 10 Minutes: AVG(Outgoing) 1989 1980 2177 2129 2130 2129 2197 2150 1798
```

IIS Updates for WinCollect 7.2.8

- Added support for remote polling. Remote vs local can be defined by the value in the **Root Directory** field.

Local: %SystemDrive%\inetpub\logs\LogFiles

Remote: \\HostnameorIP\inetpub\logs\LogFiles

- Log file rollover improvements
- Event payload now details the path of the IIS file name in the payload and the portion that follows the root directory specified in the log source configuration.
- Removed support of IIS 5 and earlier.

Log Source Type	Microsoft IIS
Protocol Configuration	WinCollect Microsoft IIS ▾
Log Source Identifier	172.1.2.3
Local System	<input type="checkbox"/>
Domain	██████████
User Name	██████████
Password	••••
Confirm Password	••••
Root Directory	W172.11.22.33\C\$\inetpub
Polling Interval	5000
Protocol Logs	
FTP	<input checked="" type="checkbox"/>
NNTP/News	<input type="checkbox"/>
SMTP/Mail	<input type="checkbox"/>
W3C	<input checked="" type="checkbox"/>

Microsoft Exchange plug-in for WinCollect 7.2.8

- Added the Microsoft Exchange protocol to WinCollect.
- Remote vs local can be defined by the value in the directory field for each log type.

Local: C:\inetpub\logs\LogFiles\W3SVC1

Remote: \\<Server>\C\$\inetpub\logs\LogFiles\W3SVC1

- You can select to collect from OWA Access, Message Tracking and SMTP/Mail types of logs.

Log Source Type	Microsoft Exchange Server
Protocol Configuration	WinCollect Microsoft Exchange ▾
Log Source Identifier	172.1.2.3
Local System	<input type="checkbox"/>
Domain	██████████
User Name	██████████
Password	••••
Confirm Password	•••
Polling Interval	5000
Protocol Logs	
OWA Access	<input checked="" type="checkbox"/>
OWA Access Directory	:\pub\logs\LogFiles\W3SVC1
Message Tracking	<input checked="" type="checkbox"/>
Message Tracking Directory	:\oles\Log\MessageTracking
SMTP/Mail	<input checked="" type="checkbox"/>
SMTP/Mail Directory	:\Roles\Log\Hub\ProtocolLog

New tools coming soon - WinCollectDeploymentSummary.sh

A new support utility is coming to the /opt/qradar/support directory that can help collect information about your QRadar deployment for support to speed up cases called WinCollectDeploymentSummary.sh (release date TBD).

- **VersionChecker.sh** – Checks the QRadar Version and provides a small warning if the QRadar version is not greater than 7.3.1
- **WinCollectActiveAgentList.sh** – Queries the active agents, then gets the list of folders from each managed host to print out the agent name, version, last heartbeat time, and the QRadar appliance managing the agent configuration.
- **WinCollectChannelBreakdown.sh** – Gets the list of active agents, and uses it to identify the WinCollect log sources and their config parameters when it comes to their 6 main log channel settings.
- **WinCollectConfFileFetch.sh** – After receiving the name of the Active Agent from the prompt, this script searches each managed host for the agent's config folder and copies the AgentConfig.xml file to the active directory and changes its name.
- **WinCollectConfFileLocate.sh** – Queries for the active agents, and checks each managed host to identify whether they have the config files.
- **WinCollectLogSourcesAgents.sh** – Gets the list of active agents, and uses it to provide a list of the log sources broken down by each agent.
- **WinCollectLogSourcesMH.sh** – Gets a list of the managed hosts. It uses the list of managed hosts to separate the log sources. It provides an overall count of log sources for each managed host, and then provides a breakdown by device type description.
- **WinCollectTuningReport.sh** – Provides a sum of the channels that are polled by each agent from each WinCollect Log Source. It then divides the sum by the average polling interval. Values between 20-30 channels per second may be overburdened.
- **WinCollectVersions.sh** – Selects all (*) columns of the qradar table 'ale_component_type'

Version of QRadar: 7.3.1.20171206164824	WinCollect Versions	id	component_name	module_name	type_name	classificationid	version	protocolid
16	StatisticsServer		Statistics	Service	3	7.2.8-88		
17	DiagnosticsEngine		WinCollectCommon	Service	3	7.2.8-88		
18	PayloadFactory		WinCollectCommon	Service	3	7.2.8-88		
19	FileMonitorFactory		WinCollectMonitor	Service	3	7.2.8-88		
20	ParserFactory		WinCollectParser	Service	3	7.2.8-88		
21	SecurityManager		Security	Service	3	7.2.8-88		
22	LogFileReaderFactory		WinCollectPlugin	Service	3	7.2.8-88		
23	DiskManager		WinCollectCommon	Service	3	7.2.8-88		
24	PersistenceManager		WinCollectCommon	Service	3	7.2.8-88		
29	DeviceNetApp		DeviceNetApp	DeviceType	3	7.2.8-88		57
39	DeviceMicrosoftExchange		DeviceMicrosoftExchange	DeviceType	3	7.2.8-88		81
33	DeviceFileForwarder		DeviceFileForwarder	DeviceType	3	7.2.8-88		41
25	StoreAndForwardStage		StoreAndForward	StageType	1	7.2.8-88		
35	DeviceMicrosoftIAS		DeviceMicrosoftIAS	DeviceType	3	7.2.8-88		47
28	DeviceMicrosoftDHCP		DeviceMicrosoftDHCP	DeviceType	3	7.2.8-88		45
31	DeviceJuniperSBR		DeviceJuniperSBR	DeviceType	3	7.2.8-88		48
27	DeviceWindowsLog		DeviceWindowsLog	DeviceType	3	7.2.8-88		39
32	DeviceMicrosoftISA		DeviceMicrosoftISA	DeviceType	3	7.2.8-88		46
30	DeviceMicrosoftIIS		DeviceMicrosoftIIS	DeviceType	3	7.2.8-88		44
38	DeviceMicrosoftDNS		DeviceMicrosoftDNS	DeviceType	3	7.2.8-88		66
34	DeviceMicrosoftSQL		DeviceMicrosoftSQL	DeviceType	3	7.2.8-88		49
26	MessageCache		WindowsMessageCache	Service	3	7.2.8-88		
1	AgentCore		AgentCore	Service	4	7.2.8-88		
36	UNCMachineNameFactory		WinCollectCommon	Service	3	7.2.8-88		
2	InfoRepositoryClient		WinCollectCommon	Service	3	7.2.8-88		
37	RegistryCache		WinCollectCommon	Service	3	7.2.8-88		
3	InfoRepositoryServer		WinCollectCommon	Service	2	7.2.8-88		
4	ConnectionFactory		CommunicationAPI	Service	2	7.2.8-88		
5	Windows2008EventCollector		Win2K8EventLogSupport	Service	3	7.2.8-88		
7	SyslogHeaderStage		DestinationSyslog	StageType	1	7.2.8-88		
8	UDPSendStage		DestinationSyslog	StageType	1	7.2.8-88		
9	LoggerStage		DestinationFileLogger	StageType	1	7.2.8-88		
10	TCPSendStage		DestinationSyslog	StageType	1	7.2.8-88		
11	SimpleEventThrottle		Stream	StageType	1	7.2.8-88		
13	DestinationManager		WinCollectPlugin	Service	3	7.2.8-88		
15	PayloadRouter		Routing	Service	3	7.2.8-88		

WinCollect Active Agents and Config File Location

Agent Name	Version	Time of last heartbeat	Location of Config File
172.18.233.51	7.2.8	2018-06-12 14:09:38.528	172.18.233.202
172.18.233.40	7.2.8	2018-06-12 14:06:07.629	172.18.233.202
172.18.233.44	7.2.8	2018-06-12 14:07:43.562	172.18.233.202
172.18.233.46	7.2.8	2018-06-12 14:06:02.454	172.18.233.202

WinCollect Log Sources for Each Managed host

count	hostname
116	vm233202
9	vm233203

The following query results are the log sources for managed host: 'vm233202'

count	devicetype	description	hostname
1	Microsoft	DHCP Server	vm233202
1	Microsoft	DNS Debug	vm233202
1	Microsoft	IAS Server	vm233202
1	Microsoft	IIS	vm233202
1	Microsoft	SQL Server	vm233202
109	Microsoft	Windows Security Event Log	vm233202
1	NetApp	Data ONTAP	vm233202
1	Universal	DSM	vm233202

The following query results are the log sources for managed host: 'vm233203'

count	devicetype	description	hostname
1	Juniper	Steel-Belted Radius	vm233203
1	Microsoft	DHCP Server	vm233203
1	Microsoft	IAS Server	vm233203
2	Microsoft	IIS	vm233203
1	Microsoft	SQL Server	vm233203
2	Microsoft	Windows Security Event Log	vm233203
1	Universal	DSM	vm233203

WinCollect Tuning Report

Tuning for Agent: "172.18.233.51"	Log Source	Security Channels	System Channels	Application Channels	DNS Channels	File Channels	Directory Channels	Total Channels	Average Interval(ms)	Tuning(channels/s)
WinCollect @ 172.18.233.51		1	1	1	1	0	0	4	3000	1

New tools coming soon - WinCollectHealthCheck.sh

A new health check utility to assist support with cases is coming to QRadar soon via a weekly auto update (release date TBD)

Where?

```
/opt/qradar/support/WinCollectHealthCheck.sh
```

Example output

Last Heartbeat Test:

```
Passed : There are 199 WinCollect Agents that have a heartbeat within the last 30 minutes
Passed : There are 0 WinCollect Agents whose last heartbeats are beyond 30 minutes
Passed : There are 0 WinCollect Agents that have no heartbeat
Passed : There are 0 WinCollect Agents that have not been deployed
```

HeartBeat Test Passed

Version Test:

```
Passed : There are 0 WinCollect Agents that are version 7.2.5
Passed : There are 0 WinCollect Agents that are version 7.2.6
Passed : There are 0 WinCollect Agents that are version 7.2.7
Passed : There are 199 WinCollect Agents that are version 7.2.8
```

Version Test Passed

New tools coming soon - WinCollectHealthCheck.sh (continued)

Status Test :

```
Passed : There are      0 WinCollect Agents that are not communicating.  
Passed : There are    199 WinCollect agents running.  
Passed : There are      0 WinCollect Agents in "Stopped"  status.  
Passed : There are      0 WinCollect Agents that are Unavailable.  
Passed : There are      0 Dirty WinCollect Agents.
```

Status Test Passed

RPM Test :

```
Passed : WinCollect 7.2.5 RPM files were not found  
Passed : WinCollect 7.2.6 RPM files were not found  
Passed : WinCollect 7.2.7 RPM files were not found  
Passed : WinCollect 7.2.8 RPM files were found
```

RPM Test Passed

LogSource Test :

```
Passed : There are    199 Log Sources whose last event times are less than 720 minutes  
Passed : There are      0  Log Sources whose last event times are beyond 720 minutes
```

Log Source Test Passed



WinCollect – Managed vs Standalone



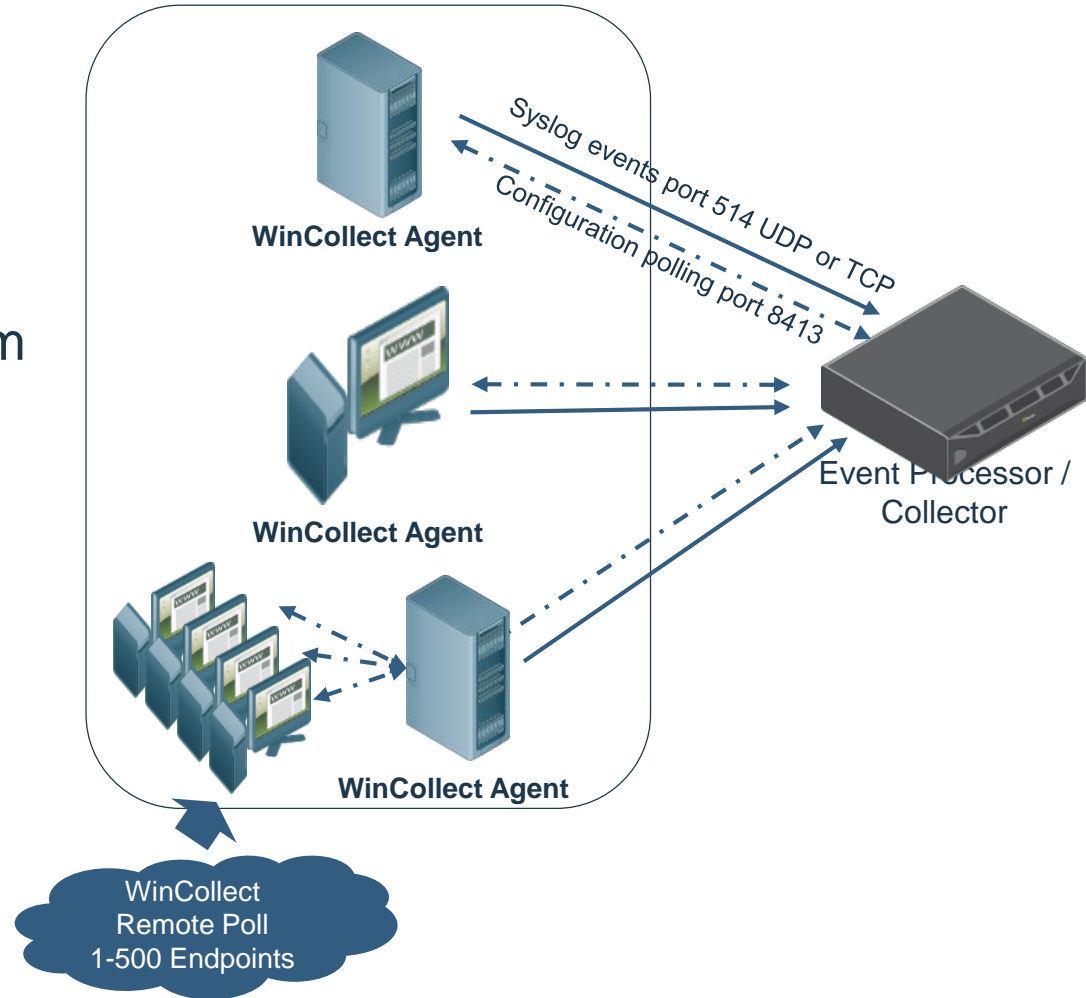
WinCollect managed deployment

Pros

- Manage event collection in QRadar.
- Deployment of Agent code from QRadar appliance via an SFS file.

Cons

- 500 Agents per QRadar appliance (Event Collector / Event Processor) Limit



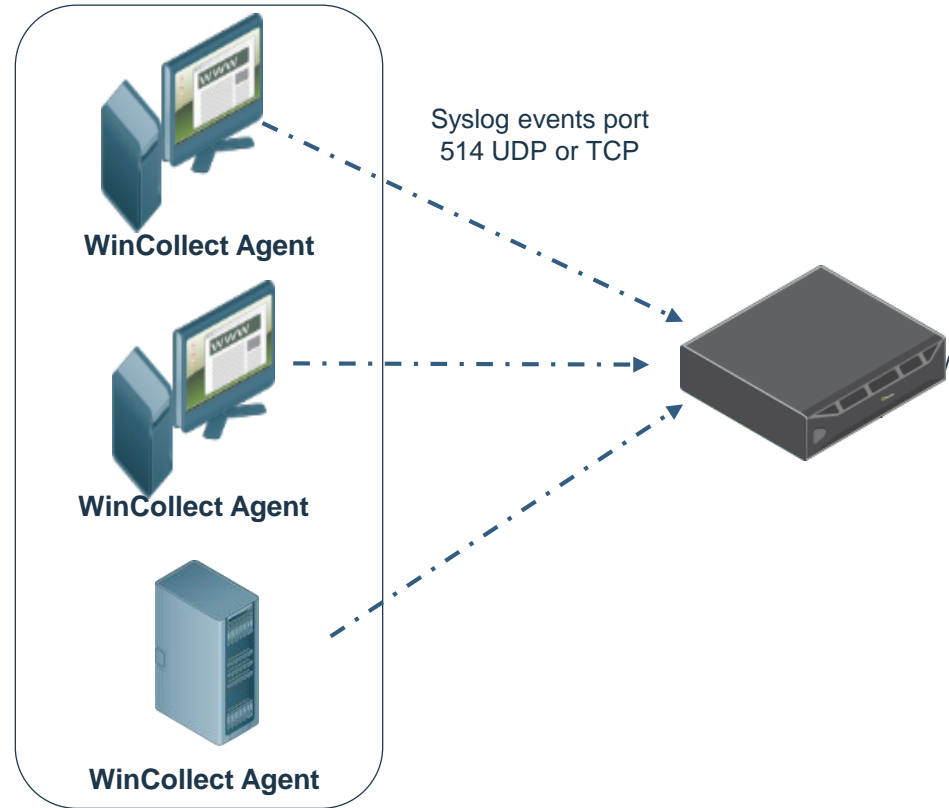
WinCollect stand-alone deployments

Pros

- No Restriction for Large Deployments
 - Bypass 500 managed agent limit
- Can be management by automation (SCCM/BigFix)
- Point of Sale (POS) deployment
 - Golden Master Image w/ WC preconfigured
- Full control of AgentConfig, fine tuning

Cons

- Management by SCCM
 - Configuration out of QRadar control
- Limited Configuration Tools



Are my agents managed or standalone?

1. You can view WinCollect user interface, if there is an agent list you have managed agents WinCollect.
2. The install_config.txt file will tell you if an agent is managed or standalone.

Managed

The WinCollect agent is installed with a Configuration Server specified.

- The Agents management is done on the QRadar Console.
- When WinCollect is upgraded on the QRadar Console, the agent will upgrade itself the next time it polls the Configuration Server.
- For the Agent to collect logs from local or remote servers. The Log Source is created on the QRadar Console and then when the agent polls the Configuration Server it pulls down the Log Source information and then starts to collect the logged events.

Standalone

The WinCollect agent is installed and no Configuration Server is specified.

- The Agent management is done on the Windows server.
- The WinCollect Configuration Console software is also installed (**Requires .NET 3.5**)
- Log Source creation and Destination configuration is done on the Windows server thru the WinCollect Configuration Console.
- Upgrading the agent is done either manually on the Windows server or thru a Third party Software deployment process.

Install_config.txt for a managed agent

```
ApplicationIdentifier=LAPTOP-9Q
ConfigurationServer=192.15.1.12
ConfigurationServerPort=8413
ConfigurationServerMinSSLProtocol=TLSv1
ConfigurationServerMaxSSLProtocol=TLSv1.2
StatusServer=192.15.1.12
ApplicationToken=t4d6PAJQQEX.....
BuildNumber=27
```

Install_config.txt for a standalone agent

```
ApplicationIdentifier=LAPTOP-9Q
ConfigurationServer=
ConfigurationServerPort=8413
ConfigurationServerMinSSLProtocol=TLSv1
ConfigurationServerMaxSSLProtocol=TLSv1.2
StatusServer=172.16.77.32
ApplicationToken=
BuildNumber=27
```



Troubleshooting Tuning Issues



About WinCollect agent tuning - <http://ibm.biz/tunewincollect>

Tuning for EPS rates is done using two fields in the log source configuration **Event Rate Tuning Profile** & **Polling Interval**; however EPS is not necessarily the most important factor to consider outside of the agent capabilities.

Channels

Each time the WinCollect agent needs to poll a remote Windows host the agent will create a channel to complete the query for every event log type being collected. Too many queries per second can cause remote procedure call (RPC) errors when WinCollect attempts to remotely poll a Windows host.

It is recommended that administrators do not exceed **30 channel queries per second** with a WinCollect agent.


The screenshot shows the 'Add a log source' configuration form. The fields are as follows:

- Log Source Name: [Text Input]
- Log Source Description: [Text Input]
- Log Source Type: Microsoft Windows Security Event Log (Dropdown)
- Protocol Configuration: WinCollect (Dropdown)
- Log Source Identifier: [Text Input]
- Local System:
- Domain: [Text Input]
- User Name: [Text Input]
- Password: [Text Input]
- Confirm Password: [Text Input]
- Event Rate Tuning Profile: Default (Endpoint) (Dropdown) - **Highlighted**
- Polling Interval (ms): 3000 (Text Input) - **Highlighted**
- Application or Service Log Type: None (Dropdown)
- Standard Log Types: Security (Checked)
- Security Log Filter Type: No Filtering (Dropdown)
- System:
- System Log Filter Type: No Filtering (Dropdown)


About WinCollect agent tuning - <http://ibm.biz/tunewincollect>

If you find yourself over the maximum number of queries/second, the best method to reduce the number of queries per second for a WinCollect agent is to edit the log source and **extend the polling interval**.

This issue is especially common in new deployments or when new log sources are added and administrators are suddenly seeing LEEF messages for RPC error messages.

 **Before tuning**
$$\frac{(300 \text{ Endpoints} * 3 \text{ Channels})}{10\text{s polling interval}} = 90 \text{ Queries per second}$$

```
<13>Apr 17 10:54:41 myhostname.com LEEF:1.0|IBM|WinCollect|7.2|7|src=myhostname  
dst=10.10.10.10 sev=5 log=Device.WindowsLog.EventLogMonitor msg=Failed to open event  
log myhostname.com [myhostname.com:Security]; will try again in approx 60 seconds.  
Reason: Error code 0x06BA: The RPC server is unavailable.
```

 **After tuning**
$$\frac{(300 \text{ Endpoints} * 3 \text{ Channels})}{30\text{s polling interval}} = 30 \text{ Queries per second}$$

Tuning & Event per second capabilities - <http://ibm.biz/tunewincollect>

Tuning for EPS rates is done using two fields in the log source configuration **Event Rate Tuning Profile & Polling Interval**.

Agents can support specific EPS rates by their collection type and will issue error messages when they are falling behind to their Status Server that was identified during installation.

- Local collection: **5,000** EPS maximum
- Remote polling: **2,500** EPS maximum

```
<13>Sep 22 09:07:56 IPADDRESS  
LEEF:1.0|IBM|WinCollect|7.2|8|src=MyHost.example.com dst=10.10.10.10 sev=4  
log=Device.WindowsLog.EventLog.MyHost.example.com.System.Read msg=Reopening  
event log due to falling too far behind (approx 165 logs skipped). Incoming  
EPS r.avg/max = 150.50/200.00. Approx EPS possible with current tuning =  
40.00
```

Question: How do I determine how many events my Windows systems are generating?

- Before you deploy WinCollect - [Event Log Report tool on our GitHub page](#).
- After you complete your initial agent installation - `../IBM/WinCollect/logs/Statistics.txt`



Error Messages



Let's talk about WinCollect error codes

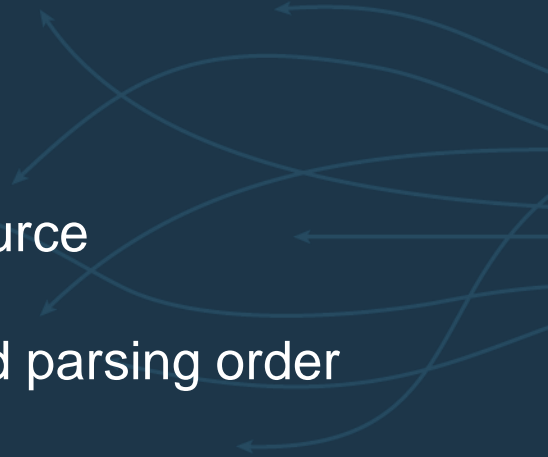
Error code	Can an admin investigate this themselves?
0x06BA - The RPC server is unavailable	Yes, the admin must review channels, log source identifiers, or that the remote system is actually online.
0x0005 - Access denied	Yes, verify credentials or that the user is part of the Event Log Readers group.
0xC000006E - Unknown user name or bad password.	Yes, verify the WinCollect user is not part of the Protected User group.
0x06B5 - The interface is unknown	Yes, is the Event Log service started on the Windows host?
0x80000004 - Agent Upgrades Fails with Timeout Error	<i>Clean up and files in the following directory:</i> <i>../IBM/WinCollect/staging</i> Verify that there is no AgentRC.txt file in the <i>../IBM/WinCollect/config</i> . If there is an AgentRC.txt file, it will prevent the service from starting.
0x80000003 - Configuration server registration failed	Yes, verify you have a valid ConfigurationServer.PEM file and that you are on the latest WinCollect version.

Let's talk about WinCollect error codes (continued)

Error code	Can an admin investigate this themselves?
0x06D9 - There are no more endpoints available from the endpoint mapper	Maybe. Possibly an old OS, such as Windows XP or 2003. MSEVEN protocol might resolve this issue.
0x80000007 - Configuration server registration failed	Maybe. Use WinCollectPing.exe to verify your connection. Verify the syslog-tls.cert file in /opt/qradar/config/trusted_certificates or ensure they are not expired. You might need to regenerate your cert and key pair or move them and regenerate the files or this could be a connection issue.
0x2471 - The requested address is not valid in its context	Yes, if you use a hostname in your log source identifier, try changing the value to an IP address.
0x274D - The target server actively refused the TCP syslog connection	Maybe. Verify connectivity using telnet. This could be caused when the agents are deleted on the QRadar side or this could be a Windows DLL issue. Verify you are not remotely polling too many Windows hosts.
0x2745 - An established connection was aborted by the software in your host machine.	Yes, likely a network issue and will resolve itself on a future socket connection attempt.
0x2746 - Connection reset by peer	Maybe. Socket connection issue and could resolve itself.



General WinCollect Troubleshooting

- Forwarded events (Subscriptions)
 - Agent communication issues
 - Verify communication from Windows
 - I'm not getting any event data
 - Confirming authentication for a WinCollect log source
 - Verify log sources are assigned to your agent
 - WinCollect agent log source – missing events and parsing order
 - Usernames missing in events for Windows
 - Destination configuration issues
- 

Forwarded events (subscriptions) and message=<blank> events

Due to how Microsoft Event Subscriptions work, the locale of the Collector (Server running WinCollect) must be Changed to 'en-US' and the subscription configured to use:

- ContentFormat:RenderedText
- Locale: en-US

The change can be tested by running this commands from an elevated PowerShell prompt on the server where WinCollect is installed:

```
reg query 'HKU\S-1-5-18\Control Panel\International' /v  
LocaleName;reg query 'HKU\S-1-5-19\Control Panel\International'  
/v LocaleName;reg query 'HKU\S-1-5-20\Control  
Panel\International' /v LocaleName
```

```
wecutil gs <subscription name> |select-string 'locale','ContentFormat'
```


Agent communication issues

Test the connection from the WinCollect agent you can run `../WinCollect/IBM/bin/WinCollectping.exe` test command to verify connection to the Configuration Server that runs on the QRadar appliance. This test can verify communication on port 8413, the Authorized Token, and the PEM file issues. If any of these fail it will report issues in the output message.

Common causes:

- Firewall blocking connection on port 8413 or bi-directional traffic issues.
- Authorized Token doesn't match the one set in QRadar.
- Something happen and the PEM file cert is wrong.
- Subnet issues where WinCollect is talking out (SYN) on one subnet and the ACK is returning on a different subnet.

Alternate test

Manually test the ConfigurationServer.PEM file (`../WinCollect/IBM/config/ConfigurationServer.PEM`)

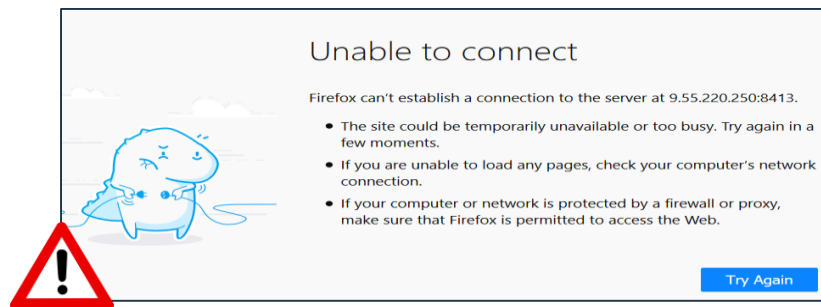
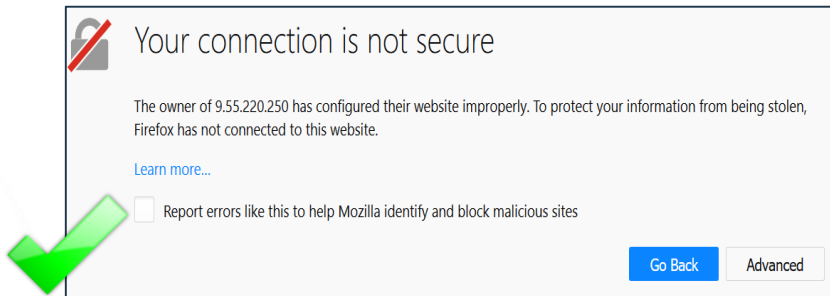
How? Log in to the Windows host. Rename this file or move the PEM file to a temporary folder. The QRadar appliance should issue a new PEM file almost immediately. If the PEM file is not issued when you refresh the folder view in Windows, you have a network communication issue.

Still not sure? Review LEEF status messages or the WinCollect log to see if any specific error messages are generated by the Agent.

Verify communication from Windows

From the Windows server browser you can test a connection to port 8413.

1. Log in to the Windows host with the WinCollect agent installed.
2. To test the connection, type: <https://QRadarIPaddress:8413/>
3. Verify you that you see a Cert message.
4. If you get Unable to connect, you know the connection on TCP 8413 getting blocked or the Listener is unable to connect to the QRadar appliance.



Verify QRadar is listening

Optional: To verify QRadar is listening from the command line, type: `netstat -tulnp | grep 8413`

```
tcp6      0      0  :::8413          :::*              LISTEN      22026/java
```

I'm not getting any event data

What questions is support going to ask me?

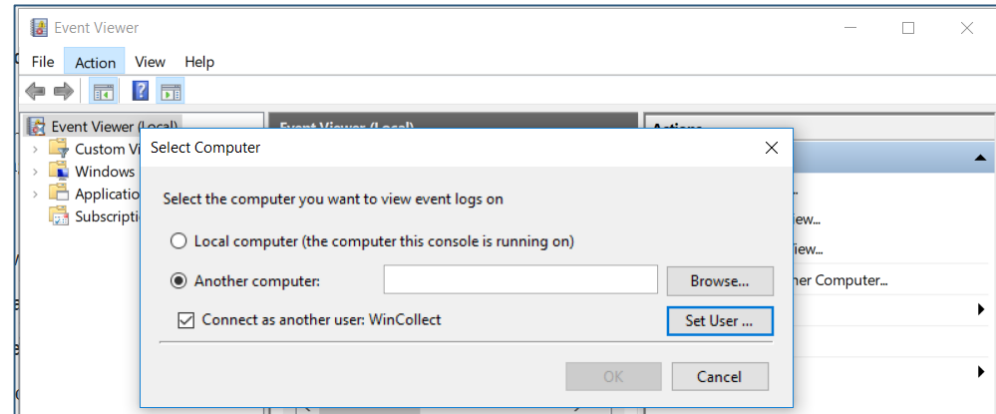
1. Is this on a single agent or for all WinCollect agents?
2. Are you getting any LEEF messages in QRadar and are any of them msg=Error <hex code>?
3. Is the hostname resolving in the network?
4. Has your password expired in the log source?
5. Did you check your ConfigurationServer.PEM file (../WinCollect/IBM/config/ConfigurationServer.PEM)
6. Have you recently restored a configuration backup?
7. Is your authorized service token valid that was generated in QRadar? You can verify that there is a value in ../WinCollect/IBM/config/install_config.txt to review if there is value in ApplicationToken =. You can always use your existing Authorized Service token to generate an ApplicationToken with the following command:
InstallerHelper.exe -T <Authentication Token>

Confirming authentication for a WinCollect log source

A good method to confirm authentication issues for their log sources is to open the Event Viewer from another computer using the credentials from the WinCollect log source. As this doubles as a connection test (is the host reachable) and can help validate the permissions for the log source.

Why? Typically, if you can view the Security event log on a remote Windows host, you should be able to poll for the data with WinCollect.

1. Log on to the Windows host that has the WinCollect agent locally installed.
2. Select **Start > Programs > Administrative Tools**, and then click **Event Viewer**.
3. Click **Action > Connect to another computer**.
4. Select the Another computer option and type the IP address or host name of the server you want to remotely poll for events.
5. Click the **Connect as another user** check box.
6. Click **Set Use**.
7. In the **User name** field, type the domain\username for the user you specified in your log source configuration. For example, test.qradar.com\JonathanP.
8. Type the password for the user and click **OK**.



Verify log sources are assigned to your agent

Click on a WinCollect agents to receive detailed information about the agent, including the number of log sources the agent is currently managing.

Name: WinCollect @ [REDACTED]
Host Name: [REDACTED]
Description: WinCollect agent installed on [REDACTED]

WinCollect Configuration

Enabled:
Automatic Updates Enabled:
Heart Beat Interval: 5 Minutes
Configuration Poll Interval: 5 Minutes
Disk Cache Capacity (MB): 6144
Disk Cache Root Directory: %ALLUSERSPROFILE%\WinCollect\Data

WinCollect Details

Auto discovered: true
WinCollect Version: 7.2.8
OS Version: Windows Server 2008 R2 (Build 3790 SP1)
Last Heart Beat:
Status: Running
Last Configuration: Tue Jan 20 10:48:10 AM 2015
This WinCollect Agent is collecting events from 0 Log Sources

Enabled WinCollect Agent Enabled or Disabled

Automatic Updates If disabled then the Agent's polling requests will be ignored by the Configuration Server.

HeartBeat Interval How often will the Agent send a heartbeat

Configuration Poll Interval Defines how often the WinCollect agent polls the Configuration Server for updated Log Source configuration information or agent software updates. The interval ranges from 0 minutes (Off) to 20 minutes.

No QRadar Log Sources have been assigned to this WinCollect agent yet.

WinCollect agent log source – missing events and parsing order

For every managed WinCollect agent registered to QRadar a Log Source is created, which receives and parses status messages from remote agents. This Log Source is hidden from the Log Source list in the UI as it is considered an internal DSM. This log source can be viewed in the Log Activity tab, Parsing Order view, or when creating a Report on Log Sources.

Or...	Name	Log Source Type	Enabled	Configuration	Credibility	Autodiscover...
1	DESKTOP	WindowsAuthServer	true	WinCollect :: eventcollector0 ::...	5	false
2	WinCollect DSM - DESKTOP	WinCollect	true	Syslog :: eventcollector0 :: qra...	10	false

NOTE: If you are not seeing events in the WinCollect agent Log Source. It could be a Parsing Order issue. This can happen if another Log Source that can receive these type of events is configured either accidentally or from log source autodiscovery. Check the Parsing Order of to insure these events are not getting directed to the wrong Log Source. The correct parsing order is to have the WindowsAuthServer (actual Windows events) above the WinCollect DSM as shows in the screen capture.

Save Cancel

Reviewing WinCollect agent status server events

Filtering for agent status messages

When investigating a WinCollect issue and have no access to the Windows server, you can get some information by viewing the WinCollect agent log source in the Log Activity tab.

Example of a WinCollect agent log source: WinCollect DSM - <Host Identifier>

Original Filters:
Log Source is WinCollect DSM - WIN2008 [\(Clear Filter\)](#) ← **Example of how you filter on WinCollect agent Log Source events**
▶ Current Statistics

	Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Source IP	Source Port	Destination IP
	WinCollect Info	WinCollect DSM - WIN2008	1	20/01/2015 11:09:20	Information	172.16.155.154	0	172.16.193.62
	WinCollect Alert	WinCollect DSM - WIN2008	1	20/01/2015 11:09:19	Alert	172.16.155.154	0	172.16.193.62
	WinCollect Alert	WinCollect DSM - WIN2008	1	20/01/2015 11:09:14	Alert	172.16.155.154	0	172.16.193.62

Information events – Typically Heartbeat messages

```
<13>Jan 20 14:46:16 WIN2008CONFIG  
LEEF:1.0|IBM|WinCollect|7.2|8|src=WIN2008CONFIG dst=172.16.193.62 sev=3 log=Code.SSLConfigServer  
Connection msg=ApplicationHeartbeat
```

Alert events – WinCollect Agent restarting (config change)

```
<13>Jan 20 14:46:15 WIN2008CONFIG  
LEEF:1.0|IBM|WinCollect|7.2|8|src=WIN2008CONFIG dst=172.16.193.62 sev=7 log=System.WinCollectS  
vc.Service msg=SERVICE STATE: APPLICATION RUNNING
```

Error events – Needs investigation, something is not configured correctly

```
<13>Jan 20 14:54:57 WIN2008CONFIG  
LEEF:1.0|IBM|WinCollect|7.2|8|src=WIN2008CONFIG dst=172.16.193.62 sev=5 log=Code.TCPSocket_0  
000000003B.8.8.8.12.514 msg=Error sending data: 10053
```

Username missing in events for Windows

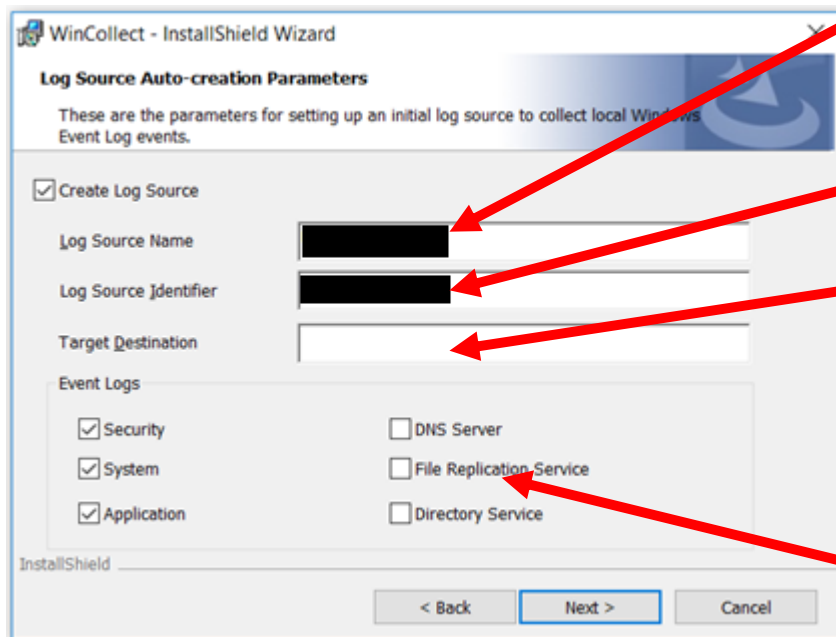
QRadar does not populate usernames for Windows events that are system generated as human beings are not generating the events. This is done by design to help administrators filter events generated by human beings from computer/system accounts. This also provides the added benefit of not updating or populating assets with the last logged in user being a system account.

The following values are considered by QRadar to be system generated usernames. When the Windows Security Event Log DSM encounters these values within a Windows event, the value is populated as N/A in the Username column.

- System
- Username\$
- Management
- Unknown
- Dash (-)
- NETWORK
- NETWORK SERVICE
- Name

Destination configuration issues

If you create a destination for your events in QRadar user interface, the name you provide must be identical to the destination you created. If you use an incorrect value, the value will need to be updated.



Log Source Name Required
A unique name that identifies this Log Source.
Usually it is the server hostname .

Log Source Identifier Required
An id that identifies this server.
Usually it is the server hostname or IP .


Target Destination Required
Customer has two options:
Use the Target name created by QRadar
or create one and use it.

QRadar Target destination name:
Eventcollector0::qradar73t02::UDP
Customer created destination name:
Console

Event Logs Required
Select the logs you want to collect



Troubleshooting with Support

- What can help QRadar Support with cases
 - Location of important logs, configuration files, certs, and more
- 

Location of important logs, configuration files, certs, and more

On the QRadar side (managed WinCollect)

Important logs:

- /var/log/qradar.log
- /var/log/qradar.error
- /var/log/qradar.java.debug

Configuration files for WinCollect agents

- /store/configservices/WinCollect/configserver/<AgentName>

Certificates

TLS certificate is used for communication on port 8413 and for event transfer to Event Collection on port 6514

- /opt/qradar/conf/syslog-tls.keystore
- /opt/qradar/conf/trusted_certificates/syslog-tls.cert
- /opt/qradar/conf/trusted_certificates/syslog-tls.key

On the WinCollect agent

Important logs:

- C:\Program Files\IBM\WinCollect\logs\Statistics.txt
- C:\Program Files\IBM\WinCollect\logs\upgrade_log.txt
- C:\Program Files\IBM\WinCollect\logs\WinCollect.txt

Configuration and Cert files:

- C:\program files\IBM\WinCollect\install_config.txt
- C:\program files\IBM\WinCollect\AgentConfig.xml
- C:\program files\IBM\WinCollect\ConfigurationServer.PEM
- C:\program files\IBM\WinCollect\logconfig.xml

What can help QRadar Support with cases

This list might seem simple, but understanding your issue before we even look at the logs helps us prioritize your problems.

1. **A good description of your issue and include the business impact to your organization.
2. **A phone number where you can be reached and your available hours.
3. Are you on the latest version of WinCollect?
4. Are all WinCollect agents impacted or is this a single agent issue?
5. Did you zip your ../WinCollect/logs and your ../WinCollect/config folders for your case and attach them?
6. If you do not have access to the Windows host with the agent, we might request the Windows admin be present on the call.






Questions?





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.