IBM Security QRadar

WinCollect User Guide V7.2

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 61.

ABOUT THIS GUIDE

1 WHAT'S NEW IN WINCOLLECT V7.2

2 WINCOLLECT OVERVIEW

3 INSTALLATION PREREQUISITES FOR WINCOLLECT

4 WINCOLLECT INSTALLATION

5 POST INSTALLATION INSTRUCTIONS FOR WINCOLLECT AGENTS

About This Guide

The *IBM Security QRadar WinCollect User Guide* provides you with information for how to install and configure WinCollect agents, and retrieve events from Windows-based event sources.

The following IBM Security QRadar products support WinCollect:

- IBM Security QRadar SIEM
- IBM Security QRadar Log Manager

Intended audience

This guide is intended for the system administrator who is responsible for Windows event sources or WinCollect agent installation and configuration in your QRadar deployment or in your network. This guide assumes that you have QRadar administrative access and a knowledge of your corporate network and networking technologies.

Technical documentation

For information about how to access more technical documentation in the QRadar products library, see ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the ***IBM Knowledge Center*** (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Contacting customer support

For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

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 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.

1 WHAT'S NEW IN WINCOLLECT V7.2

WinCollect v7.2 includes updates.

Distributed WinCollect deployment

Using a distributed deployment, you can configure WinCollect agents to communicate with an Event Collector. The Event Collector then sends the data to your QRadar Console. You can manage your distributed deployment by using the QRadar user interface. To use this feature, your QRadar system must be updated to v7.2.1 Patch 3 or later.

Learn more

64-bit installation

For new installations, depending on your Windows operating system bit version, you can download 32-bit or 64-bit WinCollect agent installer. If you are upgrading, when you install the WinCollect agent RPM, the installer automatically detects the operating system bit version.

Communication management port change

WinCollect now uses port 8413 for management communication.

Learn more

Automatic log source creation

When you install the WinCollect agent on a WinCollect host you can now configure the agent to automatically create a log source in QRadar. This log source is created when the agent first registers with QRadar. This log source will collect the configured windows event log types from the Windows Server where the agent was installed. This feature eliminates the need to set up a local log source for each agent that is installed. Your QRadar system must be updated to v7.2.1 Patch 1 or later.

Learn more

Updated installation process

When you install the WinCollect RPM, it now includes all of the WinCollect plugins.

You can configure the WinCollect agent installation to automatically create and tune a QRadar log souce.

You can also set the syslog status server, which is useful if you set up a stand-alone installation.

Performance improvements	There are many performance improvements, including significant increases to EPS rates for tuned agents, both for local and remote collection. There are also improvements to the agent logging and statistical information. See **Table 3-2**.
Agent installations on Windows XP systems	Installing the WinCollect agent is supported on Windows XP. See **Table 3-2**.
Heart beats are no longer updated in the QRadar user interface	Heartbeats are supported as a syslog message and the QRadar user interface for WinCollect agents is not updated. You will see new syslog messages for heartbeats that you did not see in previous releases.
Stand-alone installations	WinCollect agents can be installed in stand-alone mode. You can use an endpoint management or software distribution product to manage the installation of your stand-alone WinCollect agents For more information about how to install stand-alone WinCollect agents, consult Professional Services.

2 WinCollect overview

WinCollect is an agent that collects Microsoft Windows-based events from local or remote Windows-based systems and sends them to IBM Security QRadar.

WinCollect is an application that collects events by running as a service on a Windows system. The WinCollect agent can also collect events from other Windows servers where the agent is not installed. WinCollect is centrally managed from the QRadar user interface. Each WinCollect agent deployed in your network can collect and forward events to QRadar Console or Event Collector by using syslog.

Distributed WinCollect agent installation process

You can configure multiple WinCollect agents to communicate with an Event Collector that then sends the data to your QRadar Console. To install a distributed WinCollect agent deployment, you must perform the following procedures:

1. Install the WinCollect agent RPM on your QRadar Console.
2. Create an authorization token for your WinCollect agents.
3. Create destinations for WinCollect events in your deployment.
4. Install the WinCollect agent on your WinCollect hosts and set the Configuration Console as the IP of your Event Collector.
5. Wait for QRadar to automatically discover your WinCollect agents.

3 INSTALLATION PREREQUISITES FOR WINCOLLECT

Before you can install WinCollect agents, you must verify your deployment meets the installation requirements.

Distribution options for WinCollect agents

WinCollect agents can be distributed in a remote collection configuration or installed on the local host. The following WinCollect collection methods are available: local and remote.

Local collection

The WinCollect agent collects events only for the host on which it is installed. You can use this collection method on a Windows host that is busy or has limited resources, for example, domain controllers.

Remote Collection

The WinCollect agent is installed on a single host and collects events from multiple Windows systems. Remote collection allows you to easily scale the number of Windows log sources that you can monitor.

Deployment considerations

Use the following strategies to reduce the impact to system performance:

- To reduce the total number of agents, use remote collection where one agent monitors many endpoints.
- If you update a group of WinCollect agents, do it during off-peak operating hours.
- Deploy and manage the WinCollect agents in groups of 100 and monitor system performance for issues.

Communication between WinCollect agents and QRadar Event Collectors

Open ports are required for data communication between WinCollect agents and the QRadar host, and between WinCollect agents and the hosts that they remotely poll.

WinCollect agent communication to QRadar Console and Event Collectors

All WinCollect agents communicate with the QRadar Console and Event Collectors to forward events to QRadar and request updated information.

You must ensure firewalls that are between the QRadar Event Collectors and your WinCollect agents allow traffic on the following ports:

- **Port 8413 (management communication)** is required for managing the WinCollect agents. Port 8413 is used for features such as the heartbeat and

configuration updates. Traffic is always initiated from the WinCollect agent. This traffic is sent over TCP and communication is encrypted.

- **Port 514 (syslog events)** is used by the WinCollect agent to forward syslog events to QRadar. You can configure WinCollect log sources to provide events by using TCP or UDP. You can decide which transmission protocol is required for each WinCollect log source. Port 514 traffic is always initiated from the WinCollect agent.

WinCollect agents remotely polling Windows event sources

WinCollect agents that remotely poll other Windows operating systems for events include have extra port requirements.

The following ports are used when WinCollect agents remotely poll for Windows-based events:

Table 3-1 Port usage for WinCollect remote polling

Protocol and port	Usage
TCP port 135	Microsoft Endpoint Mapper
UDP port 137	NetBIOS name service
UDP port 138	NetBIOS datagram service
TCP port 139	NetBIOS session service
TCP port 445	Microsoft Directory Services for file transfers that use Windows share

Collecting events by polling remote Windows systems uses dynamic RPC. To use dynamic RPC, you must allow inbound traffic to the Windows system that WinCollect attempts to poll for events on port 135. Port 135 is used for Endpoint Mapping by Windows.

If you remotely poll any Windows operating system other than the Windows Vista operating system, you might need to allow ports in the range between 1024 and port 5000. You can configure Windows to restrict the communication to specific ports for the older versions of Windows Firewall, for example Windows XP. For more information, see your Windows documentation.

Hardware and software requirements for the WinCollect host

The Windows system that hosts the WinCollect agent must meet the following minimum requirements:

Table 3-2 WinCollect host hardware and software requirements

Requirement	Description
Memory	8GB (2GB reserved for the WinCollect agent)
Processing	Intel Core 2 Duo processor 2.0 GHz

Table 3-2 WinCollect host hardware and software requirements

Requirement	Description
Disk space	3 GB of available disk space for software and log files 6 GB might be required if events are stored on a schedule
Available processor resources	20%
Supported operating systems	• Windows Server 2003 • Windows Server 2008 • Windows Server 2008R2 • Windows Server 2012 • Windows 7 • Windows Vista • Windows XP
Required user role permissions	Administrator
Distribution	One WinCollect agent for each host.

To tune your installation to improve the performance of a single WinCollect agent, contact IBM Professional Services.

Event per second rates

Before you install your WinCollect agents, it is important to understand the number of events that can be collected by a WinCollect agent.

The event per second (EPS) rates in Table 3-3 represent a test network. This information can help you determine the number of WinCollect agents that you need to install on your network. WinCollect supports default EPS rates and also supports tuning, which allows you to improve the performance of a single WinCollect agent. You can tune local collection as part of the agent installation. Improving the performance of existing installations and remote collection must be done with the help of IBM Professional Services or IBM Customer Support.

Exceeding these EPS rates without tuning can cause you to experience performance issues or event loss, especially on busy systems.

The following table describes the default EPS rate in our test environment:

Table 3-3 WinCollect test environment

Installation Type	Tuning	EPS	Log Sources	Total EPS
Local Collection	Default	250	1	250
Remote Collection	Default	5 - 10	500	2500

Table 3-3 WinCollect test environment

Installation Type	Tuning	EPS	Log Sources	Total EPS
Local Collection	Tuned	5000	1	5000
Remote Collect	Tuned	varies	varies	2500+

Tuning an agent to increase the EPS rates for remote event collection is highly dependent on your network, the number of log sources you assign to the agent, and the number of events generated by each log source.

Prerequisites for upgrading WinCollect agents

Before you upgrade WinCollect agents, ensure that the following conditions are met:

1. If you are running QRadar V7.1 (MR2), ensure that WinCollect agent 7.1.0-QRADAR-AGENT-WINCOLLECT-7.1-613263 is installed.
2. If you are running QRadar V7.2.0 or later, ensure that WinCollect agent 7.2.0-QRADAR-AGENT-WINCOLLECT-7.2-613265 is installed.

You can confirm the version of the installed WinCollect agent by using one of the following methods:

- In QRadar, select Help > About, then select the link “Additional Release Information”.
- Use ssh to log in to the QRadar console, and run the following command:

rpm -qa | grep -i AGENT-WINCOLLECT

Note: Before you install the new WinCollect agent, open the WinCollect panel in the Admin tab, and ensure that all WinCollect agents are listed as version 7.1.2. If you installed AGENT-WINCOLLECT-7.1-613263 or AGENT-WINCOLLECT-7.2-613265, but one or more agents are still listed as version 7.1.1, ensure that you wait for the V7.1.2 update to be replicated to the agents.
Before you installed the WinCollect agent, the replication time setting was specified by the Configuration Poll Interval in the WinCollect Agent Configuration panel.

4 WINCOLLECT INSTALLATION

To install WinCollect on a Windows-based host, you must download and install a WinCollect agent RPM on QRadar, create an authentication token, and then install a WinCollect agent on a Windows-based host. Install the WinCollect agent on each Windows-based host from which you want to collect events or on the host that you want to use for remote collection.

First time installations require that you install both the WinCollect agent RPM and the WinCollect agent executable (.exe)

Upgrades require that you install only the WinCollect agent RPM. If automatic updates are enabled, the WinCollect agent RPM sends updates to all of the WinCollect agents.

Installing the WinCollect agent RPM on QRadar

To use the QRadar user interface to manage a distributed deployment of WinCollect agents, you must install the WinCollect agent RPM on your QRadar Console. This agent includes the required protocol to enable communication between QRadar system and the managed WinCollect hosts.

Procedure

Step 1 Download the WinCollect agent RPM file from the following website:

http://www.ibm.com/support

Step 2 Copy the RPM to your QRadar system.

Log in to QRadar as the root user.

Step 3 Type the following command:

```
rpm -Uvh
AGENT-WINCOLLECT-<Qradar_version>-<build_number>.noarch.rpm
```

Step 4 To install the protocol files, type the following command:

```
yum groupinstall wincollect
```

Step 5 If you are prompted for configuration, type **y**.

Step 6 Log in to QRadar.

Step 7 On the **Admin** tab toolbar, select **Advanced > Deploy Full Configuration**.

Step 8 As the root user, run the following command: `service tomcat restart`

Creating an authentication token for WinCollect agents

Third-party or external applications that interact with QRadar require an authentication token. Before you install WinCollect agents in your network, you must create an authentication token. This authentication token is required for every WinCollect agent you install.

About this task

In the Manage Authorized Services window, you must select a user role that you want to use this authentication token. For most configurations, the **All** user role can be selected. The **Admin** user role provides more privileges, which can create a security concern.

The authentication token allows WinCollect agents to exchange data with QRadar appliances. Create one authentication token for all of your WinCollect agents that communicate events with your QRadar host. If the authentication token expires, the WinCollect agent cannot receive log source configuration changes.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Authorized Services** icon.

Step 4 Click **Add Authorized Service**.

In the Manage Authorized Services window, configure the parameters.

Table 4-4 Add Authorized Services parameters

Perameter	Description
Service Name	Type a name for this authorized service. The name can be up to 255 characters in length. For example, WinCollect Agent.
User Role	From the list box, select a user role. Administrators can create a user role or assign a default user role to the authorization token. For most configurations, the **All** user role can be selected. ***Note:*** *The* ***admin*** *user role provides additional privileges, which can create a security concern and should not be used.*

Table 4-4 Add Authorized Services parameters

Perameter	Description
Expiry Date	Type or select an expiry date using the calendar provided. Alternately, select the **No Expiry** check box to indicate you do not want the service token to expire. The Expiry Date field allows you to define a date when you want this service to expire. If the date defined expires, the service is no longer authorized and a new authorization token needs to be generated by an administrator. By default, the authorized service is valid for 30 days.

Step 5 Click **Create Service**.

Step 6 Record the generated authentication token value.

Installing the WinCollect agent on a WinCollect host

You can install the WinCollect agents on Windows-based hosts in your network. The WinCollect agent collects Windows-based events and sends them to your QRadar Console or QRadar Event Collector.

When you install WinCollect, you can now choose to have QRadar automatically create a log source for the WinCollect agent host that is based on the agent registration with QRadar. You can also specify a forwarding destination host for the log source data. To use this feature, your QRadar system must be updated to v7.2.1 Patch 1 or later.

Before you begin

Ensure that the following conditions are met:

- You created an authentication token for the WinCollect agent.
- You must add a WinCollect destination before you configure automatic log source creation. The WinCollect agent sends the Windows event logs to the configured destination. The destination can be the console or an Event Collector. See **Adding a destination to WinCollect**.
- If you want to automatically create a log source for this agent, you must know the name of the destination that you want to send your Windows log source to. See **Adding a destination to WinCollect**. If you do not remember the destination name, click **Admin** > **Data Sources** > **WinCollect** > **Destinations.**
- **Hardware and software requirements for the WinCollect host**
- **Communication between WinCollect agents and QRadar Event Collectors**.

Procedure

Step 1 Download the WinCollect agent setup file from the following website:

http://www.ibm.com/support

Note: If the Services window is open on the Windows host, the WinCollect agent installation fails.

Step 2 Right-click the WinCollect agent installation file and select **Run as administrator**.

Step 3 Follow the prompts in the installation wizard. The following table describes some of the parameters.

Table 4-5 WinCollect installation wizard parameters

Parameter	Description
Host Identifier	Type a name to identify the WinCollect agent to the QRadar Console. You must use a unique identifier for each WinCollect agent you install. The name you type in this field is displayed in the WinCollect agent list of the QRadar Console.
Authentication Token	Type the authentication token you created in QRadar for the WinCollect agent. For example, **af111ff6-4f30-11eb-11fb-1fc117711111** For more information on creating an authorization token for WinCollect, see **Creating an authentication token for WinCollect agents**.
Configuration console	Required for all installations, except stand-alone mode. Leave blank for stand-alone mode installations. Type the IP address or host name of your QRadar console. For example, **100.10.10.1** or **hostname**. ***Note:*** *This parameter is intended for the QRadar console only. Do not specify an Event Collector or non-console appliance in this field. To use an event collector as your configuration console, your QRadar system must be updated to V7.2.1 Patch 3 or later.*
Log Source Name	Required. The name can be up to 255 characters in length.
Log Source Identifier	Required if the Enable Automatic Log Source Creation checkbox is selected. Identifies the remote device that the WinCollect agent polls.
Event Logs	Select the Window event logs that you want the log source to collect and send to QRadar.
Target Destination	The WinCollect Destination must be configured in QRadar before proceeding.

Table 4-5 WinCollect installation wizard parameters

Parameter	Description
Advanced Tuning	**Machine Poll Interval (msec)** is the polling interval that determines the number of milliseconds (msec) between queries to the Windows host • Use a polling interval of 3500 when the WinCollect agent collects events from computers that have a low event per second rate, for example, collecting from 50 remote computers that provide 20 events per second or less. • Use a polling interval of 1000 when the WinCollect agent collects events from a small number of remote computers that have a high event per second rate, for example collecting from 10 remote computers that provide 100 events per second or less. The minimum polling interval is 100 milliseconds (.1 seconds). The default is 3000 milliseconds or 3 seconds.
Minimum number of logs to process per pass	Consult IBM Customer Support prior to changing these values.
Maximum number of logs to process per pass	Consult IBM Customer Support prior to changing these values.

If you want to enable automatic log source creation, your QRadar Console or Event Collector must be installed with QRadar 7.2.1 Maintenance Release 1 Patch 1 or later.

Installing a WinCollect agent from the command-line interface

Use the command-line interface (CLI) to install a WinCollect agent on a host without the installation wizard.

Command-line installations deploy WinCollect agents simultaneously to multiple remote systems that use third-party products remote or batch installations.

About this task

The WinCollect installer uses the following parameters:

Table 4-6 WinCollect installer parameters

Parameters	Description
/qn	Runs the WinCollect agent installation without a user interface.

Table 4-6 WinCollect installer parameters (continued)

Parameters	Description
INSTALLDIR	The installation directory for the WinCollect agent. Your directory name cannot include spaces and quotation marks enclose the directory path, for example, INSTALLDIR="C:\IBM\WinCollect\"
AUTHTOKEN=token	Authorizes the WinCollect service, for example, AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc117711111
HOSTNAME=host name	The identifiable name, IP address or host name for the WinCollect agent host. The at (@) symbol is not allowed in the host identifier field.
FULLCONSOLEADRESS=host_address	The IP address or host name of your QRadar Console or Event Collector, for example, FULLCONSOLEADRESS=100.10.10.1. Your QRadarsystem must be updated to v7.2.1 Patch 3 or later if you want to configure the agent to use an Event Collector as its FULLCONSOLEADRESS
LOG_SOURCE_AUTO_CREATION	Enables automatic log source creation. If you enable this parameter, you must configure the log source parameters. This feature requires that your QRadar system be updated to v7.2.1 Patch 1or later.
LOG_SOURCE_AUTO_CREATION_PARAMETERS	Defines the parameters that you want the log source creation process to use. Ensure that each parameter uses the format: **`Parameter_Name=`*`value`***.The parameters are separated with ampersands (&). This feature requires that your QRadar system be updated to v7.2.1 Patch 1 or later. Log source creation uses the following parameters:
Component1.AgentDevice	Required. Must be 'DeviceWindowsLog'
Component1.Action	Required. Must be 'create'
Component1.LogSourceName	Not required. The name of the log source that is created. The default is **WindowsAuthServer @ <LogSourceIdentifier>**
Component1.LogSourceIdentifier	Required. Must be the IP or hostname of the system that the agent is installed on
Component1.Destination.Name	Required if Component1.Destination.Id is not set

Table 4-6 WinCollect installer parameters (continued)

Parameters	Description
Component1.CoalesceEvents	Not required. True or False. For more information see the *Log Sources User Guide*.
Component1.StoreEventPayload	Not required. True or False. For more information see the *Log Sources User Guide*.
Component1.Encoding	Not required. The default character encoding is UTF-8.
Component1.Log.Application	Required
Component1.Log.Security	Required
Component1.Log.System	Required
Component1.Log.DNS+Server	Required
Component1.Log.Directory+Service	Required
Component1.Log.File+Replication+Service	Required

Procedure

Step 1 Download the WinCollect agent setup file from the following website:

http://www.ibm.com/support

Step 2 From the desktop, select **Start > Run**.

Step 3 Type the following command:

```
cmd
```

Step 4 Click **OK**.

Step 5 Navigate to the download directory that contains the WinCollect agent setup file.

Note: The Services window cannot be open on the Windows host or the WinCollect agent installation fails.

Step 6 Type the following command:

```
AGENT-WinCollect-7.2.0.<build>-setup.exe /s /v"/qn
INSTALLDIR="C:\IBM\WinCollect" AUTHTOKEN=token
FULLCONSOLEADRESS=host_address HOSTNAME=hostname
LOG_SOURCE_AUTO_CREATION=true|false
LOG_SOURCE_AUTO_CREATION_PARAMETERS="parameters""
```

The following example shows an installation where the log source is automatically created.

```
AGENT-WinCollect-<version>-setup.exe /s /v"/qn
INSTALLDIR="C:\IBM\WinCollect"
AUTHTOKEN=eb59386c-e098-49b8-ba40-d6fb46bfe7d1
FULLCONSOLEADDRESS=<IP_address>:8413 HOSTNAME=<my_host>
LOG_SOURCE_AUTO_CREATION_ENABLED=True
LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice=De
```

```
viceWindowsLog&Component1.Action=create&Component1.LogSourceNam
e=LSN2&Component1.LogSourceIdentifier=<IP_address>&Component1.D
estination.Na:me=Dest1&Component1.CoalesceEvents=True&Component
1.StoreEventPayload=True&Component1.Encoding=UTF-8&Component1.L
og.Application=True&Component1.Log.Security=True&Component1.Log
.System=True&Component1.Log.DNS+Server=False&Component1.Log.Dir
ectory+Service=False&Component1.Log.File+Replication+Service=Fa
lse"""
```

The following example shows an installation where automatic log creation is not used:

```
AGENT-WinCollect-<version>-setup.exe /s /v"/qn
INSTALLDIR="C:\IBM\WinCollect"
AUTHTOKEN=eb59386c-e098-49b8-ba40-d6fb46bfe7d1
FULLCONSOLEADDRESS=<IP_address>HOSTNAME=<my_host"
```

Step 7 Press Enter.

Manually installing a WinCollect agent update

When you install an agent update RPM file, the QRadar host can automatically update all WinCollect agents that are enabled to receive automatic updates.

About this task

When enabled, WinCollect agents request updated configurations from the QRadar host based on the configuration polling interval. If new WinCollect agent files are available for download, the agent downloads and installs updates and restarts required services. No events are lost when you update your WinCollect agent because events are buffered to disk. Event collection forwarding continues when the WinCollect service starts.

After you update an agent to WinCollect V7.2.x, the agent remains configured to communicate with the QRadar host until you manually update the agent configuration to communicate with the target Event Collector.

Procedure

Step 1 Download the WinCollect agent update RPM file from the following website to your QRadar host.

http://www.ibm.com/support

Step 2 Log in to QRadar as the root user.

Step 3 Navigate to the directory with the downloaded WinCollect agent RPM file.

Step 4 Type the following command:

```
rpm -Uvh filename
```

For example, type the following command: `rpm -Uvh AGENT-WinCollect-version.noarch.rpm`

Step 5 To install the protocol files, type the following command:

```
yum groupinstall wincollect
```

Step 6 If you are prompted for configuration, type `y`.

Step 7 Log in to QRadar.

Step 8 On the **Admin** tab toolbar, select **Deploy Full Configuration**.

Step 9 As root user, run the following command: `service tomcat restart`

Step 10 On the navigation menu, click **Data Sources**.

Step 11 Click the **WinCollect** icon.

Step 12 Click **Agents**.

Step 13 Select the WinCollect agent that you want to update in your deployment.

Step 14 If the agent is disabled, click **Enable/Disable Automatic Updates**.

WinCollect agents that are enabled for automatic updates are updated and restarted. The amount of time it takes an agent to update depends on the configuration polling interval for the WinCollect agent

5 POST INSTALLATION INSTRUCTIONS FOR WINCOLLECT AGENTS

After you install a WinCollect deployment, you manage your deployment by using the IBM Security QRadar user interface. You can manage your WinCollect agents, destinations, and schedules. You can also managed configuration options for systems with restricted policies.

WinCollect agent management

The WinCollect agent is responsible for communicating with the individual log sources, parsing events, and forwarding the event information to QRadar by using syslog.

After you install the WinCollect agent on your Windows host, wait for QRadar to automatically discover the WinCollect agent.

The automatic discovery process typically takes a few minutes to complete. The registration request to the QRadar host might be blocked by firewalls in your network.

Manually adding a WinCollect Agent

If you delete your Agent and need to add it back, you can manually add your WinCollect agent.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Click **Agents**.

Step 5 Click **Add**.

Step 6 Configure the parameters.

The following table describes some of the parameters:

Table B-1 WinCollect agent parameters

Parameter	Description
Description	Optional. If you specified an IP address as the name of the WinCollect agent, add descriptive text to identify the WinCollect agent or the log sources the WinCollect agent is managing.
Enabled	If selected, events are forwarded from the WinCollect agent to the QRadar Console for the log sources that the WinCollect agent manages.
Automatic Updates Enabled	Select this check box to allow the QRadar Console to update the WinCollect agent with software and configuration updates.
Heart Beat Interval	Defines how often the WinCollect agent communicates its status to the QRadar Console. The interval ranges from 0 minutes (Off) to 20 minutes.
Configuration Poll Interval	Defines how often the WinCollect agent polls the QRadar Console for updated log source configuration information or agent software updates. The interval ranges from 0 minutes (Off) to 20 minutes.
Disk Cache Capacity (MB)	Used to buffer events to disk when your event rate exceeds the event throttle or when the WinCollect agent is disconnected from the Console. 6 GB might be required if events are stored on a schedule.
Disk Cache Root Directory	The directory where the WinCollect agent stores cached WinCollect events.

Step 7 Click **Save**.

Step 8 On the **Admin** tab, click **Deploy Changes**.

The WinCollect agent is added to the agent list.

Enabling or Disabling a WinCollect Agent

You can disable a WinCollect agent from the QRadar Console. If you disable a WinCollect agent, the event forwarder for the WinCollect agent is disabled. This prevents the agent from forwarding events. Individual log sources in the log source list show that the log sources are enabled, but no events are collected because the agent is disabled from forwarding events.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Select the WinCollect agent that you want to enable or disable.

Step 5 Click **Enable/Disable**.

Note: If you enable a WinCollect agent, the log sources that are managed by the WinCollect agent are also enabled. These log sources count toward your log source license limit. If you exceed your log source license limit, the system generates a notification.

Deleting a WinCollect Agent

If you delete a WinCollect agent, the QRadar Console removes the agent from the agent list and disables all of the log sources that are managed by the deleted WinCollect agent.

WinCollect agents that were previously automatically discovered are not rediscovered in WinCollect. To add a deleted WinCollect agent back to the agent list in the QRadar, you must manually add the deleted agent. For example, if you delete a WinCollect agent with a host identifier name VMRack1 and reinstall the agent with the same host identifier name (VMRack1), the WinCollect agent does not automatically discover the WinCollect agent.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Select the agents that you want to delete.

Step 5 Click **Delete**.

Step 6 Click **OK**.

To delete multiple WinCollect agents, press the Ctrl key to select multiple agents, and then click **Delete**.

Destination management

WinCollect destinations define the parameters for how the WinCollect agent forwards events to the Event Collector or QRadar Console.

A destination allows you to manage how log sources for your WinCollect agents forward events in your deployment. Destination parameters assigned to a log source define where events are forwarded. Log sources can use multiple destinations for forwarding events internally or externally to your deployment. Internal destinations can include other QRadar Consoles or Event Collectors. External destinations can include non-aQRadar systems, such as syslog servers or log management solutions.

Adding a destination to WinCollect

To assign where WinCollect agents in your deployment forward their events, you can create destinations for your WinCollect deployment.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Click **Destinations**.

Step 5 Click **Add**.

Step 6 Configure the parameters.

The following table describes some of the parameters:

Table B-1 Destination parameters

Parameter	Description
Port	QRadar can receive events from WinCollect agents on either UDP or TCP port 514.
Throttle (events per second)	Defines a limit to the number of events that the WinCollect agent can send each second.
Queue High Water Mark (bytes)	Defines an upper limit to the size of the event queue. If the high water mark limit is reached, the WinCollect agent attempts to prioritize events to reduce the number of queued events.
Queue Low Water Mark (bytes)	Defines a lower limit to the size of the event queue. If the queue changes from a high water mark to a level that is at or below the low water mark limit, the event prioritization returns to normal.
Storage Interval (seconds)	Defines an interval before the WinCollect agent writes events to disk or memory.
Processing Period (microseconds)	Defines the frequency with which the WinCollect agent evaluates the events in the forward queue and the events in the on disk queue. Used to optimize event processing.
Schedule Mode	• If you assign a schedule with the **Forward Events** option selected, the WinCollect agent forwards events within a user-defined schedule. When the events are not being forwarded, they are stored until the schedule runs again. • If the **Store Events** option is selected, the WinCollect agent only stores events to disk within a user-defined schedule and then forwards events to the destination as specified.

Step 7 Click **Save**.

Deleting a destination from WinCollect

If you delete a destination, the event forwarding parameters are removed from the WinCollect agent.

Destinations are a global parameter. If you delete a destination when log sources are assigned to the destination, the WinCollect agent cannot forward events. Event collection is stopped for a log source when an existing destination is deleted. Events on disk that were not processed are discarded when the destination is deleted.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Click **Destinations**.

Step 5 Select the destination that you want to delete.

Step 6 Click **Delete**.

Step 7 Click **OK**.

Schedule management

WinCollect schedules define when the WinCollect agent forwards events to the QRadar Event Collector or QRadar Console.

Use a schedule to manage when WinCollect agents forward or store events to disk in your deployment. Schedules are not required. If a schedule does not exist, the WinCollect agent automatically forwards events and stores them only if network limitations causes delay.

You can create schedules for your WinCollect deployment to assign when the WinCollect agents in your deployment forward their events.

Events that are unable to be sent during the schedule are automatically queued for the next available interval.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Click **Schedules**.

Step 5 Click **Add**.

Step 6 Click **Next**.

Step 7 Configure the parameters.

Step 8 Select a check box for each day of the week that you want included in the schedule.

Step 9 Click **Next**.

Step 10 Optional. From the **Available Destinations** list, select a destination and click the selection (**>**) symbol to add a destination to the schedule.

Step 11 Click **Next**.

Step 12 Click **Finish**.

Configuration options for systems with restricted policies for domain controller credentials

To collect events from remote systems without using domain administrator credentials, alternative configuration options are available.

WinCollect requires credentials based on the type of collection that you are attempting to use for your WinCollect log sources.

When WinCollect agents collect events from the local host, the event collection service uses the Local System account credentials to collect and forward events. Local collection requires that you install a WinCollect agent on a host where local collection occurs.

Remote collection inside or across a Windows domain might require domain administrator credentials to ensure that events can be collected. If your corporate policies restrict the use of domain administrator credentials, you might be required to complete more configuration steps for your WinCollect deployment.

Local installations with no remote polling

You can install WinCollect locally on each host that you cannot remotely poll.

After you install WinCollect, QRadar automatically discovers the agent and you can create a WinCollect log source. You can specify to use the local system by selecting the **Local System** check box in the log source configuration.

Local installations are suitable for domain controllers where the large event per second (EPS) rates can limit the ability to remotely poll for events from these systems. A local installation of a WinCollect agent provides scalability for busy systems that send bursts of events when user activity is at peak levels.

Configuring access to the registry for remote polling

You can configure a local policy for your Windows systems to allow a WinCollect log source to remotely poll for events.

Configure a user account or group with the **Manage auditing and security logs** option in their Local Security Policy editor.

When a local policy is configured on each system that you want to remotely poll, a single WinCollect agent uses the Windows Event Log API to read the remote registry and retrieve event logs. The Windows Event Log API does not require domain administrator credentials; however, the Event API method does require an account that has access to the remote registry and to the security event log.

With this collection method, the log source can remotely read the full event log, but requires WinCollect to parse the retrieved event log information from the remote host against cached message content. WinCollect uses version information from the remote operating system to ensure that the message content is correctly parsed before it forwards the event to QRadar.

Procedure

Step 1 Log on to the Windows computer that you want to remotely poll for events.

Step 2 Select **Start > Programs > Administrative Tools**, and then click **Local Security Policy**.

Step 3 From the navigation menu, select **Local Policies > User Rights Assignment**.

Step 4 Right-click on **Manage auditing and security log** and select **Properties**.

Step 5 From the **Local Security Setting** tab, click **Add User or Group** to add your WinCollect user to the local security policy.

Step 6 Log off of the Windows host and try to poll the remote host for Windows-based events that belong to your WinCollect log source.

If you cannot collect events for the WinCollect log source, verify that your group policy does not override your local policy. You can also verify that the local firewall settings on the Windows host allow remote event log management.

Configuring Windows event subscriptions for WinCollect agents

To provide events to a single WinCollect agent, you can use Microsoft event subscriptions to forward events on each Windows system to provide events. With event subscriptions configured, numerous Windows hosts can forward their events to QRadar without administrator credentials.

To use event subscriptions, you must do these tasks:

1. Configure event subscriptions on your Windows hosts.
2. Configure a log source on the WinCollect agent that receives the events. The WinCollect log source must have the **Local System** check box and **Forwarded Events** check box selected.

The events collected are defined by the configuration of the event subscription on the remote host that sends the events. WinCollect forwards all of the events sent by the subscription configuration, regardless of what event log check boxes are selected for the log source.

Event subscriptions only apply to WinCollect agents and hosts that are configured on the following Windows operating systems:

- Windows 8
- Windows 7
- Windows Server 2008 R2
- Windows Server 2012
- Windows Vista

For more information about event subscriptions, see your Microsoft documentation or the following website: *http://technet.microsoft.com/en-us/library/cc749183.aspx.*

6 LOG SOURCES FOR WINCOLLECT AGENTS

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

Log sources that communicate through a WinCollect agent can be added individually. If the log sources contain similar configurations, you can simultaneously add multiple log sources. A change to an individually added log source updates only the individual log source. A change made to a group of log sources updates all of the log sources in the log source group.

Adding a log source to a WinCollect agent

You can add a log source to a specific WinCollect agent in your deployment. When you add a new log source to a WinCollect agent or edit the parameters of a log source, the WinCollect service is restarted. The events are cached while the WinCollect service restarts on the agent.

Before you begin

If you want to configure a log source that uses a WinCollect plug-in, you must read the requirements and perform the necessary steps to prepare the third-party device. For more information, see **WinCollect plug-in requirements**.

About this task

Use the **Log Filter Type** parameter to configure the log source to ignore events that are filtered by log type. You can also configure WinCollect agents to ignore events globally by ID code or log source. Exclusion filters for events are available for the following log types:

- Security
- System
- Application
- DNS Server
- File Replication Service
- Directory Service

Global exclusions use the **EventIDCode** field from the event payload. To determine the values that are excluded, source and ID exclusions use the

Source= field and the **EventIDCode=** field of the Windows event payload. Separate multiple sources by using a semi-colon.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Click **Agents**.

Step 5 Select the WinCollect agent, and click **Log Sources**.

Step 6 Click **Add**.

Step 7 Choose one of the following options:

- For a WinCollect log source, select **Microsoft Windows Security Event Log** from the **Log Source Type** list and then select **WinCollect** from the **Protocol Configuration** list.
- If this log source uses a WinCollect plug-in, configure the plug-in specific parameters. For more information about these parameters, see **Configuration options for log sources that use WinCollect plug-ins**.

Step 8 Configure the common parameters.

The following table describes the common parameters:

Table C-1 WinCollect log source parameters

Parameter	Description
Log Source Identifier	The IP address or host name of a remote Windows operating system from which you want to collect Windows-based events. The log source identifier must be unique for the log source type. The **Log Source Identifier** field in a WinCollect log source is used to poll events from remote sources.
Local System	Disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the QRadar.
Domain	The Windows domain that includes the Windows log source. This parameter is optional. The following examples use the correct syntax: LAB1, server1.mydomain.com The following example uses incorrect syntax:\\mydomain.com
Application or Service Log Type	Optional. Used for XPath queries. Provides a specialized XPath query for products that write their events as part of the Windows application log. This allows you to separate Windows events from events that is classified to a log source for another product.

Table C-1 WinCollect log source parameters (continued)

Parameter	Description
Log Filter Type	Configures the WinCollect agent to ignore specific events from the Windows event log.
Forwarded Events	Enables QRadar to collect events that are forwarded from remote Windows event sources that use subscriptions. Forward events that use event subscriptions are automatically discovered by the WinCollect agent and forwarded as if they are a syslog event source. When you configure event forwarding from your Windows system, enable event pre-rendering.
Event Types	At least one event type must be selected.
Enable Active Directory Lookups	If the WinCollect agent is in the same domain as the domain controller that is responsible for the Active Directory lookup, you can select this check and leave the override domain and DNS parameters blank.
Override Domain Controller Name	The IP address or host name of the domain controller that is responsible for the Active Directory lookup. Required when the domain controller that is responsible for Active Directory lookup is outside of the domain of the WinCollect agent.
Override DNS Domain Name	The fully qualified domain name of the DNS server that is responsible for the Active Directory lookup. This example shows a fully qualified domain name: **`wincollect.com`**.
Remote Machine Poll Interval (ms)	The number of milliseconds between queries that poll remote Windows hosts for new events. The higher the expected event rate, the more frequently the WinCollect agent needs to poll remote hosts for events. • Use **7500** when the WinCollect agent collects events from a large number of remote computers that have a low event per second rate, for example, 100 remote computers that provide 10 events per second or less. • Use **3500** when the WinCollect agent collects events from a large number of remote computers that have a low event per second rate, for example, 50 remote computers that provide 20 events per second or less. • Use **1000** when the WinCollect agent collects events from a small number of remote computers that have a high event per second rate, for example, 10 remote computers that provide 100 events per second or less.

Table C-1 WinCollect log source parameters (continued)

Parameter	Description
XPath Query	Structured XML expressions that you can use to retrieve customized events from the Windows security event log. If you specify an XPath Query to filter events, the check boxes that you selected from the **Standard Log Type** or **Event Type** are ignored and the events that are QRadar collects use the contents of the XPath Query. To collect information by using an XPath Query, you might be required to enable Remote Event Log Management on Windows 2008. For more information, see **XPath queries**. Microsoft Server 2003 does not support XPath Queries for events.
Credibility	The credibility indicates the integrity of an event or offense as determined by the credibility value from the source devices. Credibility increases if multiple sources report the same event.
Target Internal Destination	Managed hosts with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Forwards your events to one or more external destinations that you have configured in your destination list.
Coalescing Events	Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the **System Settings** properties in QRadar. However, when you create or edit a log source, you can select the **Coalescing Events** check box to coalesce events for an individual log source.
Store Event Payload	Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the the **System Settings** properties in QRadar. However, when you create or edit a log source, you can select the **Store Event Payload** check box to retain the event payload for an individual log source.

Step 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.

Configuration options for log sources that use WinCollect plug-ins

Each WinCollect plug-in has a unique set of configuration options. Use this reference to configure the plug-in specific log source parameters.

Microsoft DHCP log source configuration options

The following table describes the log source configuration options for the Microsoft DHCP plug-in:

Table C-2 Protocol parameters for WinCollect Microsoft DHCP

Parameter	Description
Log Source Type	**Microsoft DHCP**
Protocol Configuration	**WinCollect Microsoft DHCP**
Local System	To collect local events, the WinCollect agent must be installed on the same host as your Microsoft DHCP Server. The log source uses local system credentials to collect and forward events to the QRadar.
Folder Path	The directory path to your DHCP event logs. • For a local directory path, use **`c:\WINDOWS\system32\dhcp`** • For a remote directory path, use **`\\DHCP IP address\c$\Windows\System32\dhcp`**
File Pattern	Type the regular expression (regex) required to filter the filenames. All files that match the pattern are included in the processing. The default file pattern is **`.*`** and matches all files in the **Folder Path** field.

Microsoft IAS log source configuration options

The following table describes the log source configuration options for the Microsoft IAS plug-in:

Table C-3 Protocol parameters for WinCollect Microsoft IAS

Parameter	Description
Log Source Type	**Microsoft IAS Server**
Protocol Configuration	**WinCollect Microsoft IAS / NPS**
Local System	To collect local events, the WinCollect agent must be installed on the same host as your Microsoft IAS server. The log source uses local system credentials to collect and forward events to the QRadar.
Root Directory	The directory path to your IAS event logs. • For a local directory path, use **`%WINDIR%\System32\Logfiles`** • For a remote directory path, use **`\\<IAS IP>\c$\Windows\System32\Logfiles`**

Table C-3 Protocol parameters for WinCollect Microsoft IAS (continued)

Parameter	Description
File Monitor Policy	• **Notification-based (local)** uses the Windows file system notifications to detect changes to your event log. • **Polling-based (remote)** monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.
Polling Interval	The polling interval, which is the amount of time between queries to the root log directory for new events.

Microsoft ISA log source configuration options

The following table describes the log source configuration options for the Microsoft ISA plug-in:

Table C-4 Protocol parameters for WinCollect Microsoft ISA

Parameter	Description
Log Source Type	**Microsoft ISA**
Protocol Configuration	**WinCollect Microsoft ISA / Forefront TMG**
Local System	To collect local events, the WinCollect agent must be installed on the same host as your Microsoft ISA or Forefront TMG server. The log source uses local system credentials to collect and forward events to the QRadar.

Table C-4 Protocol parameters for WinCollect Microsoft ISA (continued)

Parameter	Description
Root Directory	The directory path to your ISA event logs. When you specify a remote file path, use a dollar sign ($) instead of a colon (:) to represent your drive name. Microsoft ISA 2004 • For a local directory path, use **<Program Files>\MicrosoftISAServer\ISALogs** • For a remote directory path, use **<ISA server IP>\<Program Files>\MicrosoftISAServer\ISALogs** Microsoft ISA 2006 • For a local directory path, use **%systemroot%\LogFiles\ISA** • For a remote directory path, use **\<ISA server IP>\%systemroot%\LogFiles\ISA** Microsoft Threat Management Gateway • For a local directory path, use **<Program Files>\<Forefront Directory>\ISALogs** • For a remote directory path, use **\\<ISA server IP>\<Program Files>\<Forefront Directory>\ISALogs**
File Monitor Policy	• **Notification-based (local)** uses the Windows file system notifications to detect changes to your event log. • **Polling-based (remote)** monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.
Polling Interval	The amount of time between queries to the root log directory for new events.

File Forwarder log source configuration parameters

The following table describes the log source configuration options for the File Forwarder plug-in:

Table C-5 File Forwarder protocol parameters

Parameter	Description
Log Source Type	**Universal DSM**
Protocol Configuration	**WinCollect File Forwarder**
Local System	Disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the QRadar.

Table C-5 File Forwarder protocol parameters (continued)

Parameter	Description
Root Directory	The location of the log files to forward to QRadar. If the WinCollect agent remotely polls for the file, the root log directory must specify both the server and the folder location for the log files. For example, `\\server\sharedfolder\remotelogs\`.
File Pattern	The regular expression (regex) required to filter the file names. All matched files are included in the processing. The default file pattern is `.*` and matches all files in the **Root Directory** field.
Monitoring Algorithm	• **Continuous Monitoring** is intended for files systems that append data to log files. • **File Drop** is used for the log files in the root log directory that are read one time, and then ignored in the future.
File Monitor Type	• **Notification-based (local)** uses the Windows file system notifications to detect changes to your event log. • **Polling-based (remote)** monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.
File Reader Type	• **Text (file held open)** - The system that generates your event log continually leaves the file open to append events to the end of the file. • **Text (file open when reading)** - The system that generates your event log opens the event log from the last known position, and then writes events and closes the event log. • **Memory Mapped Text (local only)** - Select this option only when advised by Professional Services. This option is used when the system that generates your event log polls the end of the event log for changes. This option requires the **Local System** check box to be selected.

Microsoft IIS log source configuration options

The following table describes the log source configuration options for the Microsoft IIS plug-in:

Table C-6 Protocol parameters for WinCollect Microsoft IIS

Parameter	Description
Log Source Type	**Microsoft IIS**
Protocol Configuration	**WinCollect Microsoft IIS**

Table C-6 Protocol parameters for WinCollect Microsoft IIS (continued)

Parameter	Description
Root Directory	The directory path to your Microsoft IIS log files. • For Microsoft IIS 6.0 (full site), use **`%SystemRoot%\LogFiles`** • For Microsoft IIS 6.0 (individual site), use **`%SystemRoot%\LogFiles\site name`** • For Microsoft 7.0-8.0 (full site), use **`%SystemDrive%\inetpub\logs\LogFiles`** • For Microsoft IIS 7.0-8.0 (individual site), use %SystemDrive%\inetpub\logs\LogFiles*site name*
Polling Interval	The amount of time between queries to the root log directory for new events.
Protocol Logs	Specifies what items to collect from Microsoft IIS. Select one or more of the following options: • FTP • NNTP/News • SMTP/Mail • W3C

Microsoft SQL log source configuration options

The following table describes the log source configuration options for the Microsoft SQL plug-in:

Table C-7 Protocol parameters for WinCollect Microsoft SQL

Parameter	Description
Log Source Type	**Microsoft SQL**
Protocol Configuration	**WinCollect Microsoft SQL**

Table C-7 Protocol parameters for WinCollect Microsoft SQL (continued)

Parameter	Description
Root Directory	The directory path to your SQL event logs. Microsoft SQL 2000 • For a local directory path, use **C:\Program Files\Microsoft SQL Server\Mssql\Log** • For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\Mssql\Log** Microsoft SQL 2005 • For a local directory path, use **c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG** • For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG** Microsoft SQL 2008 • For a local directory path, use **C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log** • For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log** Microsoft SQL 2008R2 • For a local directory path, use **C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log** • For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log**
Log File Name	The name of the file that contains the SQL error log.
File Monitor Policy	• **Notification-based (local)** uses the Windows file system notifications to detect changes to your event log. • **Polling-based (remote)** monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.

Adding multiple log sources

You can add multiple log sources at one time to QRadar. The log sources must share a common configuration protocol and be associated with the same WinCollect agent.

You can upload a text file that contains a list of IP addresses or host names, run a query against a domain controller to get a list of hosts, or manually input a list of IP

addresses or host names by typing them in one at a time.

Depending on the number of WinCollect log sources that you add at one time, it can time for the WinCollect agent to access and collect all Windows events from the log source list.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Select the WinCollect agent, and click **Log Sources**.

Step 5 From the **Bulk Actions** menu, select **Bulk Add**.

Step 6 Configure values for your log sources.

Step 7 Select one of the following methods to bulk import log sources:

- Select the **File Upload** tab and then select a text file IP addresses or host names of log sources that you want to add. The maximum number of log sources you can add is 500.

  The text file must contain one IP address or host name per line. Extra characters after an IP address or host names longer than 255 characters result in an error. As a result a log source from the host list might not be added.
- Select the **Domain Controller** tab and then type the IP address and full domain name for the domain controller. To search a domain, you must add the domain, user name, and password for the log source before you poll the domain for hosts to add.
- Select the **Manual** tab and then type an IP address or host name to add to the host list. Click Add Host.

Step 8 Click **Save**.

Step 9 Click **Continue**.

The log sources are added to your WinCollect agent.

7 WINCOLLECT PLUG-IN REQUIREMENTS

Some log sources require a WinCollect plug-in to support communication between your WinCollect agent and the Microsoft Windows servers. Each plug-in has a unique set of requirements and instructions.

All plug-ins are available for download from the IBM support website (*https://www.ibm.com/support).*

WinCollect plug-ins support the following server versions:

Table D-1 Supported server versions for WinCollect plug-ins

Plug-in	Supported servers
Microsoft DHCP	Microsoft DHCP Server 2003
	Microsoft DHCP Server 2008
	Microsoft DHCP Server 2012
Microsoft IAS	Windows 2003 operating systems with Microsoft IAS Server 2003 enabled
	Windows 2008 operating systems with Microsoft Network Policy Server 2008 enabled
	Windows 2012 operating systems with Microsoft Network Policy Server 2012 enabled
Microsoft ISA	Microsoft ISA Server 2004
	Microsoft ISA Server 2006
	Microsoft Forefront Threat Management Gateway 2010
Microsoft IIS	Microsoft IIS Server 6.0
	Microsoft IIS Server 7.0
	Microsoft IIS Server 7.5
	Microsoft IIS Server 8.0
Microsoft SQL	Microsoft SQL Server 2000
	Microsoft SQL Server 2003
	Microsoft SQL Server 2008
	Microsoft SQL Server 2008R2

Microsoft DHCP plug-in requirements

WinCollect agents support local collection and remote polling for Microsoft DHCP Server installations.

To remotely poll for Microsoft DHCP Server events, you must provide administrator credentials or domain administrator credentials. If your network policy restricts the use of administrator credentials, you can install a WinCollect agent on the same host as your Microsoft DHCP Server. Local installations of WinCollect do not require special credentials to forward DHCP events to QRadar.

The DHCP event logs that are monitored by WinCollect are defined by the directory path you specify in your WinCollect DHCP log source.

WinCollect evaluates the root log directory folder to automatically collect new DHCP events that are written to the event log. As described in the following table, DHCP event logs start with DHCP, contain a three-character day of the week abbreviation, and end with .log. DHCP log files in the root log directory that match either an IPv4 or IPv6 DHCP log format is monitored for new events by the WinCollect agent.

Table D-2 Example log format for Microsoft DHCP events

Log type	Example log file format
IPv4	`DhcpSrvLog-Mon.log`
IPv6	`DhcpV6SrvLog-Wed.log`

Log files that do not match the DHCP event log format are not parsed or forwarded to QRadar.

Enabling DHCP event logs on your Microsoft Windows Server

To write DHCP events to a file for WinCollect, you must enable DHCP event logs on your Microsoft Windows Server.

Procedure

Step 1 Log in to your Microsoft Windows Server.

Step 2 Click **Control Panel > Administrative Tools > DHCP**.

Step 3 Choose one of the following options:

- **Windows Server 2003** - Right-click on your DHCP server and select **Properties**.
- **Microsoft Server 2008R2 and above** - Right-click on **IPv4** or **IPv6** and select **Properties**.

Step 4 Click the **General** tab.

Step 5 Click **Enable DHCP Audit Logging**.

Step 6 Click **Apply**.

Step 7 Click **OK**.

Windows 2008R2 Servers use DHCP logs that are enabled independently. You might be required to repeat this procedure to enable both IPv4 and IPv6 audit logs.

Microsoft IAS and NPS plug-in requirements

The Microsoft Internet Authentication Service (IAS) plug-in for WinCollect forwards RADIUS and authentication, authorization, and accounting (AAA) events from Microsoft IAS or Network Policy (NPS) Servers to IBM Security QRadar.

Configuring the Microsoft IAS plug-in for WinCollect

WinCollect agents support local event collection and remotely poll for Microsoft IAS and NPS events that log to a file.

To configure a WinCollect plug-in for Microsoft IAS, do these steps:

1. On your Microsoft IAS or NPS server, configure the system to generate W3C event logs.
2. On your QRadar Console, install the WinCollect plug-in for the Microsoft IAS protocol.
3. On your QRadar Console, configure a WinCollect log source to collect event logs.
4. On your QRadar Console, verify that the events are forwarded from your WinCollect agent.
5. If you do not receive events or status messages, verify that the WinCollect agent can communicate by either TCP or UDP on port 514 to the QRadar Console or QRadar Event Collector.

Microsoft IAS or NPS server log formats

Microsoft IAS and NPS installations write RADIUS and authentication events to a common log directory.

To collect these events with WinCollect, you must configure Microsoft IAS or Microsoft NPS to write an event log file to a directory.

WinCollect supports the following event log formats:

- Data Transformation Service (DTS)
- Open Database Connectivity (ODBC)
- Internet Authentication Service (IAS)

Microsoft IAS directory structure for event collection

The event logs that are monitored by WinCollect are defined by the configuration of the root directory in your log source.

When you specify a root log directory, you must point the WinCollect agent to the folder that contains Microsoft ISA or NPS events. The root log directory does not recursively search sub-directories for event files.

To increase performance you can create a sub folder for your IAS and NPS event logs. For example, you can create a directory similar to the following: **`\Windows\System32\Logfiles\NPS`**. When you create a specific event folder

the agent does not have to evaluate a large number of files to locate your event logs.

If your system generates large amounts of IAS or NPS events, you can configure your Windows system to create a new event log at daily intervals. Creating new logs ensures that the agent does not have to search large logs for new events.

Microsoft ISA plug-in requirements

The WinCollect plug-in for Microsoft Internet Security and Acceleration (ISA) forwards network proxy and firewall events from Microsoft ISA or Microsoft Forefront Threat Management Gateway (TMG) servers to IBM Security QRadar.

Configuring the Microsoft ISA plug-in

WinCollect agents support local event collection and remotely poll for Microsoft ISA and TMG events that log to a file.

To configure a WinCollect plug-in for Microsoft ISA, do these steps:

1. On your Microsoft ISA or TMG server, configure the system to generate W3C event logs.
2. On your QRadar Console, install the WinCollect plug-in for the Microsoft ISA protocol.
3. On your QRadar Console, configure a WinCollect log source to collect event logs.
4. On your QRadar Console, verify that the events are forwarded from your WinCollect agent.
5. If you do not receive events or status messages, verify that the WinCollect agent can communicate by either TCP or UDP on port 514 to the QRadar Console or QRadar Event Collector.

Supported Microsoft ISA or TMG server log formats

Microsoft ISA and Forefront Threat Management Gateway installations create individual firewall and web proxy event logs in a common log directory. To collect these events with WinCollect, you must configure your Microsoft ISA or Microsoft TMG to write event logs to a log directory.

WinCollect supports the following event log formats:

- Web proxy logs in WC3 format (w3c_web)
- Microsoft firewall service logs in WC3 format (w3c_fws)
- Web Proxy logs in ISA format (isa_web)
- Microsoft firewall service logs in ISA format (isa_fws)

The W3C event format is the preferred event log format. The W3C format contains a standard header with the version information and all of the fields that are expected in the event payload. You can customize the W3C event format for the firewall service log and the web proxy log to include or exclude fields from the event logs.

You can use the default W3C format fields. If the W3C format is customized, the following fields are required to properly categorize events:

Table D-1 W3C format required fields

Required field	Description
Client IP (c-ip)	Source IP address
Action	Action that is taken by the firewall
Destination IP (r-ip)	Destination IP address
Protocol (cs-protocol)	Application protocol name, for example, HTTP or FTP
Client user name (cs-username)	User account that made the data request of the firewall service
Client user name (username)	User account that made the data request of the web proxy service

Microsoft ISA directory structure for event collection

The event logs that are monitored by WinCollect are defined by the configuration of the root directory in your log source.

WinCollect evaluates the directory folder and recursively searches the subfolders of the root log directory to determine when new events are written to the event log. By default, the WinCollect plug-in polls the root log directory for updated event logs every five seconds.

File Forwarder plug-in requirements

With the WinCollect plug-in for File Forwarder, WinCollect agents can collect and forward event logs for Windows appliances or software.

Use the plug-in to configure a root directory that the WinCollect agent can monitor for Windows-based event log files.

After you configure your device, you can map your File Forwarder to a syslog destination. WinCollect evaluates the root log directory to determine when file changes occur.

The log files that are read by the plug-in must be text-based, single-line events. Multi-line events are not supported. The File Forwarder plug-in requires a Universal DSM to parse and categorize events.

Microsoft IIS plug-in requirements

With the WinCollect plug-in for Microsoft Internet Information Server (IIS), WinCollect agents can parse local event logs from your Microsoft IIS server and forward IIS events to IBM Security QRadar.

To collect Microsoft IIS events, a WinCollect agent must be installed on your Microsoft IIS server. Remote polling for Microsoft IIS events is not supported by the WinCollect plug-in for Microsoft IIS.

Microsoft Internet Information Services (IIS) includes a range of administrative features for website management. You can monitor attempts to access your websites to determine whether attempts were made to read or write to your files. You can create a single Microsoft IIS log source to record events from your entire website directory or individual websites.

The Microsoft IIS device plug-in can read and forward events for the following logs:

- Website (W3C) logs
- File Transfer Protocol (FTP) logs
- Simple Mail Transfer Protocol (SMTP) logs
- Network News Transfer Protocol (NNTP) logs

The WinCollect plug-in can monitor W3C, IIS, and NCSA formatted event logs. However, the IIS and NCSA event formats do not contain as much event information in their event payloads as the W3C event format. To collect the maximum information that is available, you can configure your Microsoft IIS server

to write events in W3C format. WinCollect can collect both ASCII and UTF-8 encoded event log files.

Microsoft IIS directory structure for event collection

WinCollect can monitor your entire IIS directory structure.

The sites and event logs that are monitored by WinCollect are defined by the configuration of the root directory in your log source. When you specify a root log directory, WinCollect evaluates the directory folder and all subfolders to determine when new events are written to the event log. When you monitor the IIS root website, WinCollect can use one log source to collect all of your IIS server events.

If you want to monitor individual websites, you must configure a log source for each website in your directory. You can configure the log source for the individual website to monitor the root log directory in your IIS directory structure.

By default, Microsoft IIS installations update event logs every 30 seconds. Depending on the number of sites that you monitor, you might notice that your WinCollect agent uses more resources during event log update intervals.

Microsoft SQL Server plug-in

You can use the WinCollect plug-in for Microsoft SQL Server to parse event logs from the Microsoft SQL Server and forward the event information to IBM Security QRadar.

The error log is a standard text file that contains SQL Server information and error messages.

WinCollect monitors the SQL error log for new events and forwards the event to QRadar. The error log can provide meaningful information to help you to troubleshoot issues or alert you to potential or existing problems. The error log output includes the time and date that the message was logged, the source of the message, and the description of the message. If an error occurs, the log contains the error message number and a description. Microsoft SQL Server retains backups of the last six error log files.

WinCollect can collect SQL error log events. To collect Microsoft SQL Server audit and authentication events, you can configure the Microsoft SQL Server DSM. For more information, see the *IBM Security QRadar DSM Configuration Guide*.

WinCollect agents support local collection and remote polling for Microsoft SQL Server installations. To remotely poll for Microsoft SQL Server events, you must provide administrator credentials or domain administrator credentials. If your network policy restricts the use of administrator credentials, you can install a WinCollect agent on the same host as your Microsoft SQL Server. Local installations of WinCollect do not require special credentials to forward SQL events to QRadar.

8 XPATH QUERIES

An XPath query is a log source parameter that filters specific events when the query communicates with a Windows 2008-based event log.

XPath queries use XML notation and are available in QRadar when you retrieve events by using the WinCollect protocol. The most common method of creating an XPath query is to use Microsoft Event Viewer to create a custom view. The custom view that you create for specific events in Event Viewer can generate XPath notations. You can then copy this generated XPath notation in your XPath query to filter your incoming log source events for specific event data.

Note: To manually create your own XPath queries, you must be proficient with XPath 1.0 and XPath queries.

Enabling remote log management on a Windows operating system

Enables remote log management only when your log source is configured to remotely poll other Windows systems.

Local system log sources that use XPath queries do not require a remote log management firewall exception for locally collected events.

Windows 2008

You can enable remote log management on Windows Server 2008 for XPath queries.

Procedure

Step 1 On your desktop, select **Start > Control Panel**.

Step 2 Click the **Security** icon.

Step 3 Click **Allow a program through Windows Firewall**.

Step 4 If prompted by User Account Control, click **Continue**.

Step 5 From the **Exceptions** tab, select **Remote Event Log Management**.

Step 6 Click **OK**.

Windows 2008R2 You can enable remote log management on Windows Server 2008R2 for XPath queries.

Procedure

Step 1 On your desktop, select **Start > Control Panel**.

Step 2 Click the **Windows Firewall** icon.

Step 3 From the menu, click **Allow a program or feature through Windows Firewall**.

Step 4 If prompted by User Account Control, click **Continue**.

Step 5 Click **Change Settings**.

Step 6 From the Allowed programs and features pane, select the **Remote Event Log Management** check box.

This also selects a check box for a network type. Depending on your network, you might need to correct or select additional network types.

Step 7 Click **OK**.

Windows 7 You can enable remote log management on Windows 7 for XPath queries.

Procedure

Step 1 On your desktop, select **Start > Control Panel**.

Step 2 Click the **System and Security** icon.

Step 3 From the Windows Firewall pane, click **Allow a program through Windows Firewall**.

Step 4 If prompted by User Account Control, click **Continue**.

Step 5 Click **Change Settings**.

Step 6 From the Allowed programs and features pane, select the **Remote Event Log Management** check box.

Depending on your network, you might need to correct or select additional network types.

Step 7 Click **OK**.

Creating a custom view

Use the Microsoft Event Viewer to create custom views, which can filter events for severity, source, category, keywords, or specific users.

WinCollect supports up to 10 selected event logs in the XPath query. Event IDs that are suppressed do not contribute towards the limit.

WinCollect log sources can use XPath filters to capture specific events from your logs. To create the XML markup for your XPath Query parameter, you must create a custom view. You must log in as an administrator to use Microsoft Event Viewer.

XPath queries that use the WinCollect protocol the TimeCreated notation do not support filtering of events by a time range. Filtering events by a time range can lead to errors in collecting events.

Procedure

Step 1 On your desktop, select **Start > Run**.

Step 2 Type the following command:

```
Eventvwr.msc
```

Step 3 Click **OK**.

Step 4 If you are prompted, type the administrator password and press Enter.

Step 5 On the **Action** menu, select **Create Custom View**.

When you create a custom view, do not select a time range from the **Logged** list. The **Logged** list includes the TimeCreated element, which is not supported in XPath queries for the WinCollect protocol.

Step 6 In **Event Level**, select the check boxes for the severity of events that you want to include in your custom view.

Step 7 Select an event source:

Step 8 Type the event IDs to filter from the event or log source.

Use commas to separate IDs. for example, the following list contains an individual ID and a range: 4133, 4511-4522.

Step 9 From the **Task Category** list, select the categories to filter from the event or log source.

Step 10 From the **Keywords** list, select the keywords to filter from the event or log source.

Step 11 Type the user name to filter from the event or log source.

Step 12 Type the computer or computers to filter from the event or log source.

Step 13 Click the **XML** tab.

Step 14 Copy and paste the XML to the **XPath Query** field of your WinCollect log source configuration.

Note: If you specify an XPath query for your log source, only the events that are specified in the query are retrieved by the WinCollect protocol and forwarded to

QRadar. Check boxes that you select from the **Standard Log Type** or **Event Type** are ignored by the log source configuration.

What to do next

Configure a log source with the XPath query.

Adding an XPath log source

You can create a log source that includes the XPath query from the Event Viewer.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **WinCollect** icon.

Step 4 Click **Agents**.

Step 5 Select the WinCollect agent, and click **Log Sources**.

Step 6 Click **Add**.

Step 7 From the **Log Source Type** list, select **Microsoft Windows Security Event Log**.

Step 8 From the **Protocol Configuration** list, select **WinCollect**.

Step 9 Configure the parameters:

Table E-1 WinCollect log source parameters

Parameter	Description
Log Source Identifier	The IP address or host name of a remote Windows operating system from which you want to collect Windows-based events. The log source identifier must be unique for the log source type. The **Log Source Identifier** field in a WinCollect log source is used for polling events from remote sources. This field is used in the same manner as the **RemotMachine** field in the Adaptive Log Exporter.
Local System	Disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the QRadar.
Domain	The Windows domain that includes the Windows log source. This parameter is optional. The following examples use the correct syntax: LAB1, server1.mydomain.com The following example uses incorrect syntax:\\mydomain.com
Standard Log Types	Clear all of the log type check boxes. The XPath query defines the log types for the log source.
Forwarded Events	Clear this check box.

Table E-1 WinCollect log source parameters (continued)

Parameter	Description
Event Types	Clear this check box. The XPath query defines the log types for the log source.
Enable Active Directory Lookups	If the WinCollect agent is in the same domain as the domain controller that is responsible for the Active Directory lookup, you can select this check and leave the override domain and DNS parameters blank.
Override Domain Controller Name	The IP address or host name of the domain controller that is responsible for the Active Directory lookup. Required when the domain controller that is responsible for Active Directory lookup is outside of the domain of the WinCollect agent.
Override DNS Domain Name	The fully qualified domain name of the DNS server that is responsible for the Active Directory lookup. For example, the following domain name uses the correct syntax: **`wincollect.com`**.
WinCollect Agent	The WinCollect agent to manage this log source.
Remote Machine Poll Interval (ms)	The number of milliseconds between queries to the remote Windows host to poll for new events. The higher the expected event rate, the more frequently the WinCollect agent needs to poll remote hosts for events. • Use **7500** when the WinCollect agent collects events from a large number of remote computers that have a low event per second rate, for example, 100 remote computers that provide 10 events per second or less. • Use **3500** when the WinCollect agent collects events from a large number of remote computers that have a low event per second rate, for example, 50 remote computers that provide 20 events per second or less. • Use **1000** when the WinCollect agent collects events from a small number of remote computers that have a high event per second rate, for example, 10 remote computers that provide 100 events per second or less.
XPath Query	The XPath query that you defined in Microsoft Event Viewer. To collect information by using an XPath query, you might be required to enable Remote Event Log Management on Windows 2008. ***Note:*** *Microsoft Server 2003 does not support XPath Queries for events.*

Step 10 Click **Save**.

Step 11 On the **Admin** tab, click **Deploy Changes**.

XPath query examples

Use these XPath examples as a reference when you create XPath queries. For more information about XPath queries, see your Microsoft documentation.

Example: Monitor events for a specific user

In this example, the query retrieves events from all Windows event logs for the guest user.

```
<QueryList>
<Query Id="0" Path="Application">
<Select Path="Application">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="Security">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="Setup">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="System">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="ForwardedEvents">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
</Query>
</QueryList>
```

Credential logon for Windows 2008

In this example, the query retrieves specific event IDs from the security log for Information-level events that are associated with the account authentication in Windows 2008.

```
<QueryList>
<Query Id="0" Path="Security">
      <Select Path="Security">*[System[(Level=4 or Level=0) and
( (EventID &gt;= 4776 and EventID &lt;= 4777) )]]</Select>
</Query>
</QueryList>
```

Table E-1 Event IDs in this example

ID	Description
4776	The domain controller attempted to validate credentials for an account.
4777	The domain controller failed to validate credentials for an account.

In this example, the query examines event IDs to retrieve specific events for a user account that is created on a fictional computer that contains a user password database.

```
<QueryList>
  <Query Id="0" Path="Security">
<Select Path="Security">*[System[(Computer='Password_DB') and
(Level=4 or Level=0) and (EventID=4720 or  (EventID &gt;= 4722
and EventID &lt;= 4726)  or  (EventID &gt;= 4741 and EventID
&lt;= 4743) )]]</Select>
  </Query>
</QueryList>
```

Table E-2 Event IDs in this example

ID	Description
4720	A user account was created.
4722	A user account was enabled.
4723	An attempt was made to change the password of an account.
4724	An attempt was made to reset password of an account.
4725	A user account was disabled.
4726	A user account was deleted.
4741	A computer account was created.
4742	A computer account was changed.
4743	A computer account was deleted.

A TROUBLESHOOTING A WINCOLLECT AGENT

Log files created by the WinCollect agent during configuration or installation contain error messages and other valuble information. To determine the root cause of your error, review the error logs.

The WinCollect agent creates an installation log file during the installation process for both standard and command-line installations.

The **Status** parameter might indicate that there is an issue with a WinCollect agent. The **Status** parameter is located in the WinCollect window in IBM Security QRadar SIEM. The WinCollect agent might report the following statuses:

- **Running** indicates that the WinCollect agent is active on the Windows host.
- **Stopped** indicates that the WinCollect agent is stopped. If the WinCollect service is stopped, events from the log sources that are managed by the agent are not forwarded to the QRadar Console.
- **Unavailable** indicates that the WinCollect service that reports on the status of the WinCollect agent is stopped or restarted. The services can no longer report the agent status.
- **No Communication from Agent** indicates that the WinCollect agent has not established communication with the QRadar Console. If you manually added the WinCollect agent, verify that the **Host Name** parameter is correct. Also verify that firewalls in your deployment are not blocking communication between the WinCollect agent and the Event Collector or QRadar Console.

You can also view the installation log for error information about your WinCollect agent installation.

Procedure

Step 1 Log in to the host of your WinCollect agent.

Step 1 On the desktop, select **Start > Run**.

Step 2 Type the following:

```
%TEMP%
```

Step 3 Click **OK**.

The Windows Explorer displays the temporary directory.

Step 4 Open the WinCollect installation log from the temporary directory.

```
Setup Log <Date> <#00X>.txt
```

Step 5 Review the log file to determine the cause of the installation failure.

Installation log examples

The installation log captures the install process for WinCollect and includes information about the installation failure. The information contained in the setup log file is required to troubleshoot WinCollect installations with Customer Support.

Example: Missing authorization or Console IP address

The following text shows the error message generated when the AUTH_TOKEN or CONFIG_CONSOLE_ADDRESS is missing from the command-line installation:

```
ERROR: Installation was aborted because only one of /AUTH_TOKEN
and /CONFIG_CONSOLE_ADDRESS were specified. Both must be
specified (for remote configuration management) or neither
specified (for stand-alone operation)
```

Example: Installation stopped by user

The following text shows the message generated when a standard installation is stopped by the user:

```
Message box (Yes/No):
Setup is not complete. If you exit now, the program will not be
installed.
You may run Setup again at another time to complete the
installation.

Exit Setup?
```

Example: Installation file in use error

The WinCollect agent cannot be installed while the WinCollect service is running. To avoid an installation issue, stop the WinCollect service before you attempt to reinstall the WinCollect agent on your host. The following text displays the message error message when an installation file is in use:

```
Defaulting to Abort for suppressed message box
(Abort/Retry/Ignore):
C:\Program Files (x86)\WinCollect\bin\WinCollect.exe

An error occurred while trying to replace the existing file:

DeleteFile failed; code 5.

Access is denied.

Click Retry to try again, Ignore to skip this file (not
recommended), or Abort to cancel installation.
```

Troubleshooting device configuration issues

The WinCollect agent creates a device log that stores configuration information and warnings about log sources that are configured for each WinCollect agent.

Each time the WinCollect service is restarted or the date changes, a new log is created on the Windows host for the WinCollect agent. All device logs contain time stamps to help you find the most recent log file.

The device log captures log source configuration information for WinCollect and includes information about log source issues.

Procedure

Step 1 Log in to the host of your WinCollect agent.

Step 2 Navigate to the following directory on the WinCollect host:

`C:\Program Files\IBM\WinCollect\logs\`

On 64-bit operating systems, this file is the following location:

`C:\Program Files (x86)\WinCollect\IBM\logs\`

Step 3 Open the following file:

`WinCollect_Device.`*`date identifier`*`.txt`

Device Polling Overdue

A warning message that indicates that device polling is overdue occurs when the WinCollect agent is waiting to remotely collect events from a log source that is managed by the WinCollect agent, but the device polling is in the queue.

This warning message can occur when you add or edit a large number of remotely collected log sources for a WinCollect agent with a large number of remotely collected log sources. Each time that the log source is edited, the service is restarted on the WinCollect agent and each log source is polled for updated events. Log sources near the bottom of the list can be in queue waiting to be polled. If log sources are waiting to be polled, the following message is displayed in the device log:

```
WARN Device.WindowsLog.EventLogMonitor.OnTimerExpired : Event
log 10.100.100.10 [\\10.100.100.10:Application] is seriously
overdue to be polled (interval 500 millisec, overdue = 45005
millisec).
```

This message indicates that the WinCollect agent is waiting to poll the remote log source for events.

B NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

INDEX