IBM Security QRadar
Version 7.2.1

WinCollect User Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 97.

About This Guide

1 What's new?

2 WinCollect overview

3 Install WinCollect

4 WinCollect credential requirements

5 Manage WinCollect agents

ABOUT THIS GUIDE

The *WinCollect User Guide for* IBM Security QRadar provides you with information for installing and configuring WinCollect agents and retrieving events from Windows-based event sources.

All references to QRadar or IBM Security QRadar is intended to refer to the other products that support WinCollect, such as IBM Security QRadar Log Manager.

Intended audience

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

Conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

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

This section contains a list of new, changed, deprecated, and removed features that affect this release of WinCollect.

New features in WinCollect

The following items are a list of new features for WinCollect since the last release.

Automatic WinCollect agent updates

WinCollect now allows you to install software updates for your WinCollect agent through your QRadar Console with an RPM file. This feature allows you to update your entire WinCollect agent deployment without have to reinstall or log in to your Windows systems hosting WinCollect agents. You can enable or disable the ability for a WinCollect agent to receive an auto update through the agent list.

New plug-ins are available

A number of protocol plug-ins are now available in WinCollect. This plug-in provide WinCollect with the capability to collect, parse, and forward syslog events for other Windows-based products. WinCollect protocol plug-ins are available for download on the IBM support website. For more information, see the protocol downloads on *http://www.ibm.com/support/fixcentral/*.

Destinations

WinCollect includes a new interface that allows you to create destinations for your events.

Schedules for event forwarding

WinCollect agents can now store and forward events on a pre-determined schedule. This provides users with the ability to reduce system load and forward events during off-peak hours.

Secondary event destination

Log sources configured to use the WinCollect protocol can now forward events to managed hosts in your deployment and an additional secondary destination. The secondary destination can be an external event server.

Automatic performance adjustment

WinCollect agents now attempt to automatically balance queued events and stored events to calculate the best opportunity to forward events. WinCollect agents can also buffer up to 6GB of events to disk if the WinCollect agent becomes disconnected from the QRadar Console.

2 WinCollect overview

WinCollect is a stand-alone Windows application (agent), which resides on a host in your network to allow IBM Security QRadar to collect Windows-based events.

The Wincollect agent collects Windows-based events from local or remote Windows systems by adding individual or bulk WinCollect log sources. Your QRadar Console can provide centralized management and configuration for your Windows-based log sources for a large number of WinCollect agents. All WinCollect agents deployed in your network are managed through the **Admin** tab on your QRadar Console. Each WinCollect agent deployed in your network can collect and forward events to QRadar using syslog. The following image shows a typical WinCollect deployment of two WinCollect agents.

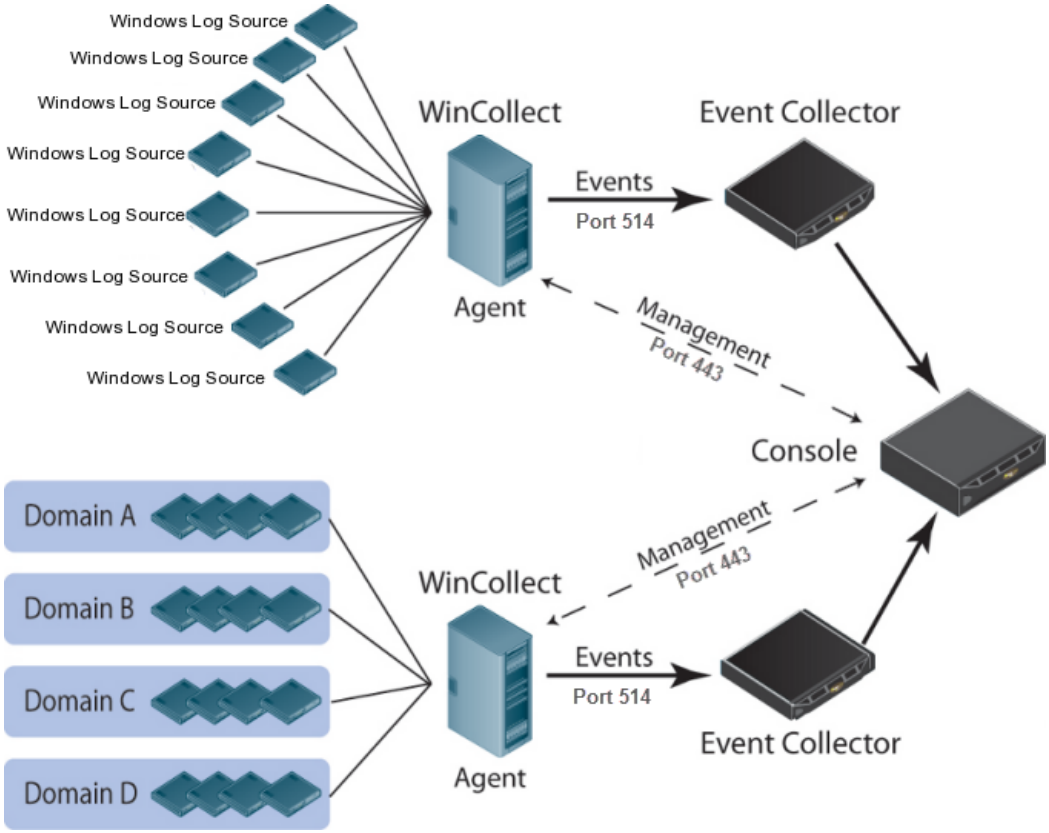

Figure 2-1 A standard WinCollect agent deployment reporting events to QRadar.

WinCollect agent overview

This section outlines the procedures that should be reviewed prior to installing WinCollect agents in your deployment.

1. Read and understand the capabilities and requirements of WinCollect. For more information, see **Before you begin**.
2. Authorize and install your WinCollect agents. For more information, see **WinCollect installation overview**.
3. Wait for your WinCollect agents to auto discover in QRadar or manually add WinCollect agents. For more information, see **Manage WinCollect agents**.
4. Create destinations for WinCollect events in your deployment. **Manage destinations**.
5. Optional. Create event schedules for your WinCollect agents. For more information, see **Manage schedules**.
6. Creat log sources to your WinCollect agents. For more information, see **Create log sources for WinCollect agents**.

3 INSTALL WINCOLLECT

The WinCollect agent can be installed on any Windows-based host in your network to collect Windows-based events for QRadar.

WinCollect agents can be distributed in your organization in a remote collection configuration or installed on the local host. The installation and number of WinCollect agent installations in your deployment is dependent on the available resources in your network, as only one WinCollect agent can be installed on a host. The following WinCollect installation methods are available:

- **Local Collection** - The WinCollect agent is installed locally and is responsible for collecting events for the host. This collection method can be used when a Windows host is busy or has limited resources, for example, domain controllers.
- **Remote Collection** - The WinCollect agent is installed on a single host, but can remotely collect events from multiple Windows systems.

  Remote collection allows you to easily scale the number of Windows log sources you can monitor by adding physical or virtual Windows hosts in your network that include a WinCollect agent. To collect from remote Windows-based operating systems, you must bulk add or individually add log sources to your WinCollect agent. The **Log Source Identifier** field determines which remote Windows sources the WinCollect agent polls for events. The log source must contain an identifier with the IP address or hostname for the remote Windows source and the proper credentials to poll for events.

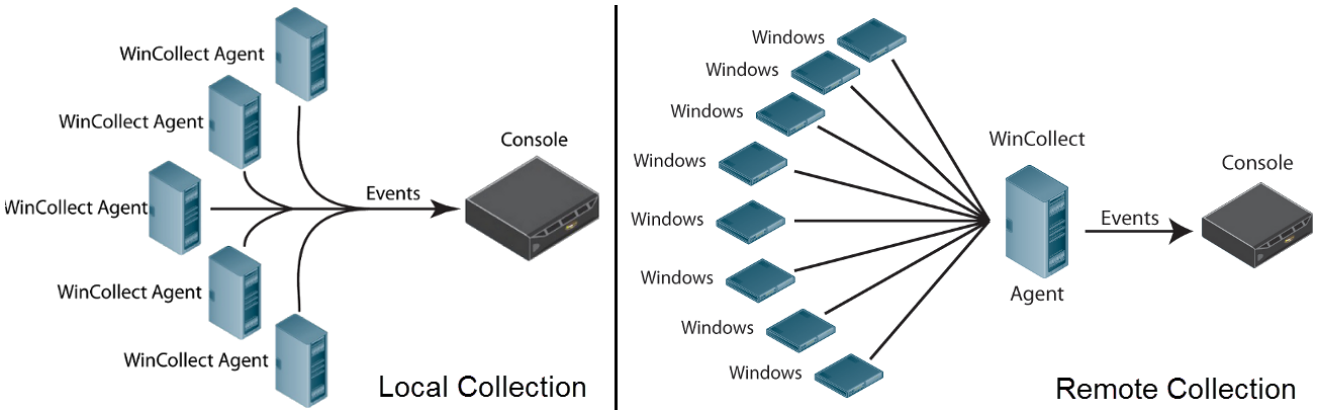

Figure 3-1 Two methods of gathering events are supported: local and remote collection.

Before you begin

Before you can begin installing WinCollect agents, you must verify your deployment meets the installation criteria.

Deployment considerations

For large WinCollect deployments, specifically large numbers of managed WinCollect agents (greater than 100), a staggered roll-out as well as modifications that may be necessary to ensure that Console stability is not impacted.

We suggest that administrators stagger the installation and deployment of WinCollect agents in to groups of 40 agents while the Console is monitored for responsiveness.

For administrators that have large WinCollect agent deployments, the recommended design is to use remote collection where one agent monitors many endpoints to reduce the total number of agents in play.

If you have any concerns about scalability, contact your sales representative for deployment best practices. Enhancements to improve WinCollect scalability are currently in development.

General requirements

Your QRadar Console must be installed with QRadar 7.1.0 Maintenance Release 2 Patch 1 (7.1.0.581477) or above to use all of the features described in this documentation.

Port requirements

The ports required for communication of data can be divided in to two segments:

1. Communication between WinCollect agents and the QRadar Console.
2. Communication between WinCollect agents and the hosts they remotely poll for events.

WinCollect agents communicating to QRadar Consoles

All WinCollect agents installed in your network are responsible for communicating back to the QRadar Console to forward events and requests for updated information.

You must ensure any firewalls located between the QRadar Console and your WinCollect agents allow traffic on the following ports:

- **Port 443 (HTTPS)** - Port 443 is required for management of the WinCollect agent from the QRadar Console. Port 443 is used for features such as the heartbeat and configuration updates. Port 443 traffic is always initiated from the WinCollect agent.
- **Port 514 (Syslog Events)** - Port 514 is required for the WinCollect agent to forward syslog events to QRadar. WinCollect log sources can be configured to provide events using TCP or UDP. This traffic can be bi-directional depending on if you configure your log sources as 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 installed on your network that remotely polling other Windows operating systems for events include additional port requirements.

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

- **TCP port 135** - This port is used by the Microsoft Endpoint Mapper.
- **UDP port 137** - This port is used for NetBIOS name service.
- **UDP port 138** - This port is used for NetBIOS datagram service.
- **TCP port 139** - This port is used for NetBIOS session service.
- **TCP port 445** - This port is required for Microsoft Directory Services to allow files transfers using a Windows share.

Event information collected by remote polling Windows systems is completed using Dynamic RPC. To use Dynamic RPC, you must allow inbound traffic on port 135 to the Windows system that WinCollect is attempting to poll for events. Port 135 is specifically used for Endpoint Mapping by Windows. The Windows operating system is responsible for opening traffic to the requesting source IP using a dynamically allocated port. This port range is always allocated above 1024, but typically below port 5000 and the request is managed by the Windows Firewall. In Windows Vista and above operating systems the firewall only responds to an RPC request from the requester, which helps with security.

Note: If you are remotely polling to a pre-Vista operating system, such as Windows XP, 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 version of Windows Firewall, for example Windows XP. For more information, see your Windows documentation.

WinCollect host requirements

The Windows system hosting the WinCollect agent must meet the following requirements:

- 8GB of RAM (2GB reserved for the WinCollect agent)
- Intel Core 2 Duo processor 2.0 GHz or better
- 3 GB of available disk space for software and log files
- At minimum, 20% of the available processor resources
- The physical or virtual host system for the WinCollect agent must be installed with one of the following operating systems:
  - Windows Server 2003
  - Windows Server 2008 (all versions)
  - Windows Server 2012
  - Windows 7
  - Windows Vista

- Administrative privileges to install the WinCollect agent

Note: Only one WinCollect agent should be installed on a host at a time.

Collected events

The WinCollect agent can collect events from the following Windows operating systems:

- Windows Server 2003
- Windows Server 2008 (all versions)
- Windows Server 2012
- Windows 7
- Windows Vista
- Windows XP

Note: WinCollect does not support event collection from Windows 2000 operating systems.

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 3-1** represent our test network. This information can help you determine the number of WinCollect agents you need to install in your network. WinCollect supports EPS rates for the default installation and also supports tuning, which allows you to increase the performance of a single WinCollect agent. Tuning can only be performed with the help of IBM Professional Services or IBM Customer Support.

CAUTION: *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 3-1 WinCollect test environment

Installation Type	Tuning	EPS	Log Sources	Total EPS
Local Collection	Default	250	1	250
Remote Collection	Default	10	100	1000
Local Collection	Tuned	2000	1	2000
Remote Collect	Tuned	varies	varies	1000+

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.

WinCollect installation overview

This section outlines the process of installing a WinCollect agent in your network to collect Windows-based events.

Installing a WinCollect agent in your network is a two-step process:

1. **Creating an authentication token for WinCollect agents**.
2. **Installing the WinCollect agent**.

Creating an authentication token for WinCollect agents

Any third-party or external applications that interacts with QRadar requires an authentication token.

Before you install WinCollect agents in your network, you must create an authentication token. The authorization token allows WinCollect agents to exchange data with QRadar appliances. You only need to create one authorization token for all of your WinCollect agents that communicate events to your QRadar Console. If an authorization token expires, the Console is unable to make any changes to your log source configuration. This includes adding or editing your log source configurations.

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**.

Step 5 Configure the following parameters:

Table 3-2 Add Authorized Services Parameters

Parameter	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.*
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 6 Click **Create Service**.

A confirmation message is displayed when an authorized service is added to QRadar.

Step 7 Copy or write down the authentication token value.

Step 8 The authorization token is required for every WinCollect agent you install.

You are now ready to install the WinCollect agent.

Installing the WinCollect agent

After you have created the authorized token, you are ready to install the WinCollect agent on your remote host.

You must install WinCollect with a user account that includes administrative permissions.

Procedure

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

http://www.ibm.com/support

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

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

Step 3 Select **I accept the terms in the license agreement** and click **Next**.

Step 4 Optional. Type a name in the **User Name** field.

Step 5 Optional. Type a name in the **Organization** field.

Step 6 Click **Next**.

Step 7 Click **Change** to define the installation path for the WinCollect agent or click **Next** to use the default install path.

Step 8 Configure the following values:

Table 3-3 WinCollect install 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**.

Table 3-3 WinCollect install parameters (continued)

Parameter	Description
Configuration Console	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.*

Step 9 Click **Next**.

Step 10 Click **Finish**.

The WinCollect agent is installed on your host. Since the WinCollect is managed through the QRadar Console an interface is not installed on the host for the WinCollect agent.

You are now ready to manage your WinCollect agent and add log sources to QRadar. For more information on managing WinCollect agents, see **Create log sources for WinCollect agents**.

4 WINCOLLECT CREDENTIAL REQUIREMENTS

To collect events from remote systems without domain administrator credentials, you can review the following alternate configuration options for your WinCollect deployment.

How credentials work for WinCollect

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

When WinCollect agents collect from the local host, the event collection service uses the Local System credentials to collect and forward events. Local collection requires that a WinCollect agent be installed at the location where local collection occurs.

Remote event collection requires additional system credentials to remotely poll Windows hosts for their events. Remote collection inside or across a Windows domain may require domain administrator credentials to ensure that events can be collected, unless you configure your WinCollect agents with one of the three following configuration options.

WinCollect configuration options

If your corporate policies restrict the use of domain administrator credentials, then you may be required to complete additional configuration steps for your WinCollect deployment.

Option 1: Local installations

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

Local installations allow each WinCollect agent to forward events from the local host to QRadar without requiring extra credentials. After you install WinCollect, the agent automatically discovers on QRadar, then you can create a WinCollect log source with the **Local System** check box selected.

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

Option 2: Remote polling with read registry permissions

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

Remotely polling for events without domain administrator credentials requires administrators to configure a user account or group with the Manage auditing and security logs option in their Local Security Policy.

Once a local policy is configured on each system you want to remotely poll, the Windows Event Log API allows a single WinCollect agent 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.

This collection method allows the log source to 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 the message content is correctly parsed before it forwards the event to QRadar.

Procedure

Step 1 Log on to the Windows computer 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 attempt to remotely poll the host for Windows events with your WinCollect log source.

If you cannot collect events for the WinCollect log source, you can verify your group policy does not override your local policy. You can also verify that the local firewall settings on the Windows host allows Remote Event Log Management.

Option 3: Windows event subscriptions

You can leverage Microsoft Event Subscriptions (Forwarded Events) on each Windows systems to provide events to a single WinCollect agent.

To use event subscriptions, you must:

1. Configure event subscriptions on your Windows hosts.
2. Configure a log source on the WinCollect agent receiving the events.

Forwarded events are automatically discovered by QRadar and allow a single WinCollect agent to act as a pass-through for parsing and forwarding Windows events for QRadar. The WinCollect log source must have the **Local System** check box and **Forwarded Events** check box selected. Event subscriptions allows numerous Windows hosts to forward their events to QRadar without requiring administrator credentials.

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

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

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

For information on configuring event subscriptions, see your Microsoft operating system documentation.

5 MANAGE WINCOLLECT AGENTS

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

After you have installed the WinCollect agent on your Windows host, you can wait for the WinCollect agent to auto discover. If you prefer not to wait for the WinCollect agent to auto discover, you can manually add your WinCollect agent to your QRadar Console using the **Admin** tab. The WinCollect agent auto discovery process typically takes a few seconds to complete.

Viewing a list of WinCollect agents

You can use the agent list to view WinCollect agents that have been added or auto discovered.

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**.

The WinCollect agent list displays the following information for each agent in your deployment:

Table 5-1 WinCollect Agent Status

Control	Description
Name	Displays the name of the WinCollect agents in your deployment. If the WinCollect agent is auto discovered, the name contains WinCollect @ **<Host Name>**. Where **<Host Name>** is the IP address or host name of the system hosting the WinCollect agent.
Host Name	Displays the IP address or host name of the WinCollect agent.

Table 5-1 WinCollect Agent Status (continued)

Control	Description
Description	Displays the description for the WinCollect agent. If your WinCollect agent is auto discovered the description displays **`WinCollect agent installed on <Host Name>`**. Where **`<Host Name>`** is the IP address or host name of the system hosting the WinCollect agent.
Version	Displays the version of the WinCollect agent installed on the Windows host.
OS Version	Displays the Windows operating system version the WinCollect agent is installed on.
Last Heart Beat	Displays time the last time heart beat successfully communicated from the WinCollect agent to the QRadar Console.
Status	Allows you to view the status of your WinCollect agent. The options include: • **Running** - The WinCollect agent is active on the Windows host. • **Stopped** - The WinCollect agent is stopped. If the WinCollect service is stopped, then events from the log sources managed by the agent are not forwarded to the QRadar Console. • **Unavailable** - The WinCollect service that reports on the status of the WinCollect agent has been stopped or restarted, so it can no longer report the agent status. • **No Communication from Agent** - The WinCollect agent has not established communication to the QRadar Console. If you manually added the WinCollect agent, verify the **Host Name** parameter is correct. You can also verify that firewalls in your deployment are not blocking communication between the WinCollect agent and the Event Collector or QRadar Console.
Enabled	Allows you to view the status of your WinCollect agent. Click **Enable/Disable** to toggle the agent's status. The options include: • **True** - The WinCollect agent is enabled. • **False** - The WinCollect agent is disabled. All log sources managed by the WinCollect agent are also disabled.

Table 5-1 WinCollect Agent Status (continued)

Control	Description
Automatic Updates Enabled	Allows you to specify if the Console can update the WinCollect agent with software and log source configuration changes. The options include: • **True** - The WinCollect agent can receive agent software version updates and log source configuration changes. The timing for configuration changes are determined by the **Configuration Poll Interval** field on each WinCollect agent. • **False** - Updates are disabled. The WinCollect log source configurations and software versions are kept in a static state. If updates are disabled, configuration changes to log sources are not applied to the WinCollect agent.

Adding a WinCollect Agent

If your WinCollect agent does not automatically discover, you can manually add your WinCollect agent.

The auto discovery process typically takes a few minutes to complete, but the registration request to the QRadar Console can be blocked by firewalls in your network.

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 Type values for the following parameters:

Table 5-2 Configure a WinCollect Agent Parameters

Parameter	Description
Name	Type a suitable name for your WinCollect agent. The name must be unique to the WinCollect agent. The name can be up to 255 characters in length.
Host Name	Type the IP address or host name used when installing the WinCollect agent. The host name can be up to 255 characters in length. The IP address or host name must be unique to the WinCollect agent.

Table 5-2 Configure a WinCollect Agent Parameters (continued)

Parameter	Description
Description	Optional. Type a description for the WinCollect agent. If you specified IP addresses for the WinCollect agent, you might consider adding a descriptive message to identify the WinCollect agent or the log sources the WinCollect agent is managing. These messages are often helpful for other QRadar administrators, if a WinCollect agent requires managing.
WinCollect Configuration	
Enabled	Select this check box to enable the WinCollect agent. If this check box is cleared, then events are not forwarded from the WinCollect agent to the QRadar Console for any of the log sources the WinCollect agent manages.
Automatic Updates Enabled	Select this check box to allow the QRadar Console to update the WinCollect agent with software updates, when available.
Heart Beat Interval	From the list box, select a heart beat interval for WinCollect. This option 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	From the list box, select an interval to poll for configuration updates to WinCollect agents. This option 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)	Type a numeric value to indicate the disk space the WinCollect agent can use to cache events. The cache available to the WinCollect agent is used to buffer events to disk when your event rate exceeds the event throttle or when the WinCollect agent is disconnected from the Console.
Disk Cache Root Directory	Type the location of the directory where the WinCollect agent stores cached WinCollect events.
WinCollect Details Pane	
Auto discovered	Displays if the WinCollect agent was auto discovered. • **True** - The WinCollect agent was auto discovered. • **False** - The WinCollect agent was not auto discovered or added manually.
WinCollect Version	Optional. Type the WinCollect version of the system hosting the WinCollect agent.

Table 5-2 Configure a WinCollect Agent Parameters (continued)

Parameter	Description
OS Version	Optional. Type the OS version of the system hosting the WinCollect agent.

Step 7 Click **Save**.

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

The WinCollect agent is added to the agent list.

Editing a WinCollect Agent

To edit the agent name, description, host IP address, or group of a log source, double-click a WinCollect agent from the agent 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 Click **Agents**.

Step 5 Select the WinCollect agent to edit.

Step 6 Click **Edit**.

Step 7 Edit any parameters for your WinCollect agent.

Step 8 Click **Save**.

Any configuration changes made to your WinCollect agents take place immediately when you click **Save**.

Enabling or Disabling a WinCollect Agent

Any WinCollect agent can be disabled 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 any events. Individual log sources in the log source list display enabled, but no events are collected as 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**.

When an agent is enabled, the Enabled column indicates true. When disabled, the Enabled column indicates false.

Note: If you enable a WinCollect agent, the log sources 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 not only removes the agent from the agent list, but disables all of the log sources managed by the deleted WinCollect agent.

WinCollect agents that previously auto discovered do not rediscover 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, then reinstall the agent with the same host identifier name (VMRack1), then the WinCollect agent cannot 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 any agents you want to delete.

Step 5 Click **Delete**.

Step 6 Click **OK**.

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

6 MANAGE DESTINATIONS

WinCollect destinations define the parameters on 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.

Adding a destination to WinCollect

You can create destinations for your WinCollect deployment to assign where WinCollect agents in your deployment forward their 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 Click **Destinations**.

Step 5 Click **Add**.

Step 6 Type values for the following parameters:

Table 6-1 Destination parameters

Parameter	Description
Name	Type a suitable name for the destination. The destination name must be unique and can be up to 255 characters in length.
Host Name	Type the IP address or host name for the destination. The host name can be up to 255 characters in length.
Protocol	From the list box, select a protocol for the destination. The options include: • **UDP** - The WinCollect agent assigned to the destination communicates syslog events with UDP. • **TCP** - The WinCollect agent assigned to the destination communicates syslog events with TCP.

Table 6-1 Destination parameters (continued)

Parameter	Description
Port	Type the port number of the destination. QRadar can receive events from WinCollect agents on either UDP or TCP port 514.
Store and Forward Options	
Throttle (events per second)	Optional. Type a value to define a limit to the number of events the WinCollect agent can send each second. This field must include a value. This value should not be altered, unless advised by customer support.
Queue High Water Mark (bytes)	Optional. Type a value, in bytes, to define an upper limit to the size of the event queue. This field must include a value. If the high water mark limit is reached, then the WinCollect agent attempts to prioritize events to reduce the number of queued events. This value should not be altered, unless advised by customer support.
Queue Low Water Mark (bytes)	Optional. Type a value, in bytes, to define a lower limit to the size of the event queue. This field must include a value. If the queue transitions from a high water mark to a level at or below the low water mark limit, then event prioritization returns to normal. This value should not be altered, unless advised by customer support.
Storage Interval (seconds)	Optional. Type a value in seconds to specify an interval before the WinCollect agent writes events to disk or memory. This field must include a value. This value should not be altered, unless advised by customer support.
Processing Period (microseconds)	Optional. Type a value in microseconds to specify the frequency with which the WinCollect agent evaluates the existing events in the forward queue and the events in the on disk queue to optimize event processing. This field must include a value. This value should not be altered, unless advised by customer support.

Table 6-1 Destination parameters (continued)

Parameter	Description
Schedule Mode	From the list box, select a schedule mode for the destination. The options include: • **Forward Events** - The WinCollect agent forwards events to the destination as the events are generated. If you assign a schedule with the Forward Events selected, then the WinCollect agent only forwards events when within a user defined schedule. • **Store Events** - The WinCollect agent stores events to disk and forwards events to the destination when within a user defined schedule. You must assign a schedule, if you select this option.
Schedule(s)	Optional. From the list box, select a schedule to apply to the destination.

Step 7 Click **Save**.

The destination is created. You can now assign the destination to the log sources managed by the WinCollect agents in your deployment.

Editing a destination in WinCollect

You can edit a destination to adjust the parameters the WinCollect agents uses to forward 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 Click **Destinations**.

Step 5 Select the WinCollect agent to edit.

Step 6 Click **Edit**.

Step 7 Edit any parameters for your destination.

Step 8 Click **Save**.

When you edit a destination, the change must be downloaded from the Console. The change is downloaded by the agent based on your configuration polling interval and the WinCollect service is restarted.

Deleting a destination from WinCollect

Deleting a destination removes the event forwarding parameters from the WinCollect agent.

CAUTION: *Destinations are a global parameter. If you delete a destination when log sources are assigned to the destination, then the WinCollect agent cannot forward events. Event collection is stopped for log source when an existing destination is deleted. Any events on disk that have not been 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 any destination you want to delete.

Step 6 Click **Delete**.

Step 7 Click **OK**.

The destination is deleted.

7 MANAGE SCHEDULES

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

A schedule allows you to manage when WinCollect agents forward or store events to disk in your deployment. When events are stored or forwarded by the WinCollect agent is determined by the schedule. However, schedules are not required. If a schedule does not exist, then the WinCollect agent automatically balances the event queue to forward both new events and events on disk.

Adding a schedule to WinCollect

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

Any events that are unable to be sent during the your 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 values for the following parameters:

Table 7-1 Schedule parameters

Parameter	Description
Name	Type a suitable name for the schedule. The schedule name must be unique and can be up to 255 characters in length.
Time Zone	Select the time zone that the WinCollect agent resides within.
Start Time	Select the start time for the schedule.

Table 7-1 Schedule parameters (continued)

Parameter	Description
End Time	Select the end time for the schedule.

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

Step 9 Click **Next**.

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

Step 11 Click **Next**.

Step 12 Click **Finish**.

The schedule is created.

Editing a schedule in WinCollect

You can edit a schedule to adjust the timing of when events are forwarded by WinCollect agents.

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 Select the schedule to edit.

Step 6 Click **Edit**.

Step 7 Edit any parameters for the schedule.

Step 8 Click **Finish** to save your changes.

When you edit a schedule, the change must be downloaded from the Console. The change is downloaded by the agent based on your configuration polling interval and the WinCollect service is restarted.

Deleting a schedule from WinCollect

You can delete a schedule to remove a schedule from WinCollect.

If you delete a schedule from a destination that is configured to store events, the WinCollect agent continually stores events until the disk space on the WinCollect agent reaches the disk cache limit. Each destination configured to store events requires a schedule. If you delete a schedule that is configured to forward events, the WinCollect agent forwards events when they are received.

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 Select the schedule you want to delete.

Step 6 Click **Delete**.

Step 7 Optional. Click the **Do not ask again** check box to avoid this confirmation.

Step 8 Click **OK**.

The schedule is removed and all WinCollect agents assigned to the schedule are updated.

8 CREATE 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 communicating through a WinCollect agent can be added individually or if the log sources contain similar configurations, then you can add multiple log sources using the bulk add feature. A change to an individually added log source only updates the individual log source. A change made to bulk added log sources updates all of the log sources in the bulk log source group. 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.

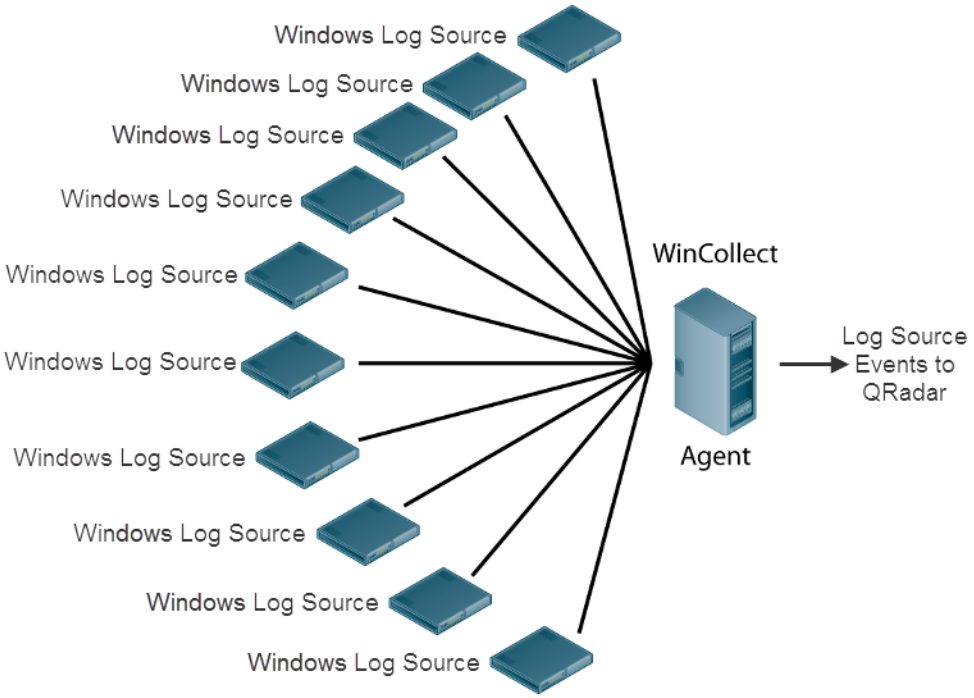

Figure 8-1 A single WinCollect agent configured for remote collection.

Viewing WinCollect log sources

You can view all of the log sources managed by a 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 Select a WinCollect agent, click **Log Sources**.

If a log source does not receive any events within the configured syslog timeout period, the Status column displays an N/A for the log source.

Adding an individual log source to a WinCollect agent

You can add a log source to a specific WinCollect agent in your 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 **Agents**.

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

Step 6 Click **Add**.

Step 7 Type a suitable name for the log source.

Step 8 Optional. Type a description for the log source.

Step 9 From the **Log Source Type** list box, select **Microsoft Windows Security Event Log**.

Step 10 From the **Protocol Configuration** list box, select **WinCollect**.

Step 11 Configure values for the following parameters:

Table 8-1 WinCollect log source parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname 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. ***Note:*** *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 Remote Machine field in the Adaptive Log Exporter.*

Table 8-1 WinCollect log source parameters (continued)

Parameter	Description
Local System	Select this check box to collect local events only. This check box disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the Console.
Domain	Type the Windows domain that includes the Windows log source. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the username required to access the Windows host.
Password	Type the password required to access the Windows host.
Confirm Password	Confirm the password required to access the Windows host.
Application or Service Log Type	Select **None**. This fields provides a specialized XPath query for products that write their events as part of the Windows application log. This allows administrators to separate Windows events from events that should be classified to a log source for another product. Without this field, products that log event exclusively in a Windows event log cannot be easily searched.
Standard Log Types	Select any check boxes for the Windows log type you want QRadar to monitor. The log types include: • Security • System • Application • DNS Server • File Replication Service • Directory Service

Table 8-1 WinCollect log source parameters (continued)

Parameter	Description
Log Filter Type	Select **Exclusion Filter** for a log type to configure the WinCollect agent to ignore specific events from the Windows Event log. Exclusion filters for events are available on the following log types: • Security • System • Application • DNS Server • File Replication Service • Directory Service Windows events can be excluded globally by specifying an event ID code or excluded by source. Global exclusions use the EventIDCode field from the event payload. Source and ID exclusions use the **Source=** field and the **EventIDCode=** field of the Windows event payload to determine the values that are excluded. Multiple sources can be separated by a semi-colon. • To filter events globally by the event ID, type the event ID. For example: **`4688, 5712, 4928-4937`**. • To filter by event ID code and source, review the following event payload: <13>Dec 09 13:59:03 [IP address] AgentDevice=WindowsLog AgentLogFile=Application PluginVersion=7.1.4.698761 **Source=CertEnroll** Computer=w2k8s User=SYSTEM Domain=NT AUTHORITY EventID=2186936384 **EventIDCode=64** EventType=0 EventCategory=0 RecordNumber=389995324 TimeGenerated=1386615656 TimeWritten=1386615656 Level=0 Keywords=0 Task=0 Opcode=0 Message=Local system To exclude CertEnroll event ID codes, type the following exclusion: **`CertEnroll(64);Software Protection Platform Service(40-50,900)`**. The filter fields support a maximum of 8192 characters and spaces for services that contain a space in the name.

Table 8-1 WinCollect log source parameters (continued)

Parameter	Description
Forwarded Events	Select this check box to allow QRadar to collect events forwarded from remote Windows event sources using subscriptions. Events forwarded using event subscriptions are automatically discovered by the WinCollect agent and forwarded as if they are a syslog event source. We suggest that when configure event forwarding from your Windows system that you enable event pre-rendering. The WinCollect agent must be installed on a Windows Vista, Windows 7, Windows 2008, or Windows 2008R2 operating system to access and forward events from a subscription. For more information on configuring event subscriptions, see your Microsoft documentation or the following website: *http://technet.microsoft.com/en-us/library/cc749183.aspx.*
Event Types	Select any check boxes for the event type you want QRadar to monitor. At least one check box must be selected. The event types include: • Informational • Warning • Error • Success Audit • Failure Audit
Enable Active Directory Lookups	Select this check box to enable lookups in networks that use Microsoft Active Directory. If the WinCollect agent is in the same domain as the domain controller responsible for the Active Directory lookup, you can select this check and leave the override domain and DNS parameters blank.
Override Domain Controller Name	Type an IP address or host name of the domain controller responsible for the Active Directory lookup. This field is required when the domain controller responsible for Active Directory lookup is outside of the domain of the WinCollect agent. This field is displayed when active directory lookups are enabled.

Table 8-1 WinCollect log source parameters (continued)

Parameter	Description
Override DNS Domain Name	Type the fully qualified domain name of the DNS server responsible for the Active Directory lookup. For example, **`wincollect.com`**. This field is displayed when active directory lookups are enabled.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Remote Machine Poll Interval (ms)	Type the polling interval, which is 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. • **7500** - A polling interval of 7500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 100 remote computers that provide 10 events per second or less. • **3500** - A polling interval of 3500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 50 remote computers that provide 20 events per second or less. • **1000** - A polling interval of 1000 should be used where 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.

Table 8-1 WinCollect log source parameters (continued)

Parameter	Description
XPath Query	XPath queries are structured XML expressions that you can include to retrieve customized events from the Microsoft Windows Security Event Log. If you specify an XPath Query to filter incoming events, any check boxes you selected from the **Standard Log Type** or **Event Type** are ignored and the events collected by QRadar use the contents of the XPath Query. You might be required to enable Remote Event Log Management on Windows 2008 to collect information using an XPath Query. For more information, see **XPath queries**. ***Note:*** *Microsoft Server 2003 does not support XPath Queries for events.*
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list box, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your events to one or more destinations you have configured in your destination list. A list box with your destinations is displayed to allow you to select additional destinations for this log source. You can forward events to any external server.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings 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.

Table 8-1 WinCollect log source parameters (continued)

Parameter	Description
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings 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.
Group	Select a check box with a log source group name to assign the log source to a group.

Step 12 Click **Save**.

Step 13 On the **Admin** tab, click **Deploy Changes**.

Repeat these steps to add additional log sources to your WinCollect agent. If the configurations are similar and only differ by IP address or hostname of the remote source, you can add multiple log sources using the bulk add feature. For more information, see **Adding bulk log sources**.

Editing a WinCollect log source

You can edit a log source to update log source parameters as your network changes.

All log source parameters are editable, with the exception of the **Log Source Type** field and the **Protocol Configuration** field. When you edit a WinCollect log source, the service on the WinCollect agent is updated and restarted. During this momentary configuration update, the WinCollect service is stopped; however, no event loss occurs. The WinCollect agent forward events after the WinCollect service restarts.

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 Select the log source to edit.

Step 7 Click **Edit**.

Step 8 Edit the log source parameters.

Step 9 Click **Save**.

The configuration is complete. The log source is updated and the WinCollect service is restarted.

Enabling or disabling a WinCollect log source

You can enable or disable an individual or group of log sources to prevent the log source from forwarding events.

If you cannot enable a log source or if log sources auto discover as disabled, then you might have exceeded your license restrictions. For more information about your license limits, see the Managing the System chapter of the *IBM Security QRadar SIEM Administration Guide*. If you require additional license limits, contact your sales representative.

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 Select the log source that you want to enable or disable.

Step 6 Click **Enable/Disable**.

When a log source is enabled, the Enabled column indicates true. When a log source is disabled, the **Status** column indicates **Disabled**.

Deleting a WinCollect log source

You can delete a WinCollect log source from QRadar to remove the log source.

The data collected by a deleted log source is still searchable in QRadar. However, you cannot search by the log source name as the reference to the log source was 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 Select the WinCollect agent, and click **Log Sources**.

Step 5 Select the log source you want to delete.

Step 6 Click **Delete**.

Step 7 Click **OK**.

You can delete multiple log sources by holding the Shift key to select multiple log sources and click **Delete**.

Adding bulk log sources

You can add multiple log sources to QRadar that share a common configuration protocol with your WinCollect agent.

Bulk adding log sources allows you to configure a large number of Windows-based log sources that share common configuration parameters. Bulk adding log sources allows you to simultaneously configure log sources with a text file of IP addresses,

or with a domain query, or manually typing a host names or IP addresses. A maximum of 500 log sources can be bulk added using a single protocol configuration. If you attempt to add a domain or a text file containing more then 500 IP addresses, an error message is displayed.

Note: Depending on the number of WinCollect log sources added, it can take an extended period of time for the WinCollect agent to access and collect all outstanding Windows events from the bulk 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 Using the **Bulk Actions** menu, select **Bulk Add**.

Step 6 Configure values for your log source.

A list of WinCollect log source parameters is available in **Table 8-1**.

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

Table 8-2 Bulk log source parameters

Parameter	Description
File Upload	
Bulk Import File	Select a text file containing a maximum of 500 IP addresses or host names of log sources you want to bulk add. The text file should 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, indicating a log source from the host list could not be added.
Domain Query	
Domain Controller	Type the IP address of the domain controller. To search a domain you must add the domain, username, and password for the log source before polling the domain for hosts to add.
Full Domain Name	Type the fully qualified domain name (FQDN) of the domain controller. To search a domain you must add the domain, username, and password for the log source before polling the domain for hosts to add.
Manual	
Host	Type an individual IP address or host name to add to the host list.

Table 8-2 Bulk log source parameters (continued)

Parameter	Description
Add Host	Click **Add Host** to add an IP address or host name to the host list. The **Add Host** check box is only displayed when you have at least one log source in the host list. By default, this check box is selected. Clearing the check box from the add field allows you to ignore a log source. ***Note:*** *You are not required to clear check boxes for log sources that already exist. Duplicate host names or IP addresses are ignored from the host list.*

Step 8 Click **Save**.

Step 9 Click **Continue**.

The log sources are bulk added to your WinCollect agent.

Editing bulk log sources

Log sources that share a common protocol can be edited as a group as they share a configuration.

You can use bulk edit to update host names, IP addresses, or add additional log sources to an existing log source group. This allows you to update log sources that share a configuration protocol or require updated credentials as your network changes.

When you edit a WinCollect log source, the service on the WinCollect agent is updated and restarted. During this momentary configuration update, the WinCollect service is stopped; however, no event loss occurs. The WinCollect agent forwards events after the WinCollect service restarts.

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 Select a bulk log source to edit from the list.

You must select one or more bulk log sources from your active log sources list for the **Bulk Edit** menu to be available.

Note: To edit the log source name, log source description, log source identifier, or group, double-click the bulk log source.

Step 6 Using the **Bulk Actions** menu, select **Bulk Edit**.

Step 7 Configure values for your log source.

A list of WinCollect log source parameters is available in **Table 8-1**.

Step 8 Click **Save**.

Step 9 Click **Continue**.

9 THE MICROSOFT DHCP PLUG-IN

You can use the Microsoft Dynamic Host Configuration Protocol (DHCP) plug-in for WinCollect to parse event logs from your Microsoft DHCP Server and forward DHCP events to IBM Security QRadar.

The Microsoft DHCP plug-in is available for download from the IBM support website (*https://www.ibm.com/support).*

Overview for the WinCollect Microsoft DHCP plug-in

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.

Microsoft DHCP includes a range of administrative features for managing IPv4 and IPv6 addresses in your network. QRadar uses WinCollect to collect and categorize events from Microsoft DHCP Servers in your network. DHCP event data is a reliable method to collect identity information and correlate network users, MAC addresses, or hosts with security events.

The DHCP event logs that are monitored by WinCollect are defined by the directory path you specifiy in your WinCollect DHCP log source. The following table provides you with the default directory paths for the **Root Log Directory** field in your log source.

Table 9-1 Default root log directory paths Microsoft DHCP events

Collection type	Root log directory
Local	**`c:\WINDOWS\system32\dhcp`**
Remote	**`\\DHCP IP address\c$\Windows\System32\dhcp`**

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. Any DHCP log files in the root log directory that

match either an IPv4 or IPv6 DHCP log format are monitored for new events by the WinCollect agent.

Table 9-2 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.

Supported versions of Microsoft DHCP

The Microsoft DHCP plug-in for WinCollect supports the following Microsoft DHCP software versions:

- Microsoft DHCP Server 2003
- Microsoft DHCP Server 2008
- Microsoft DHCP Server 2012

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.

Configuring a Microsoft DHCP log source for WinCollect

To collect events from your Microsoft DHCP Server, you must configure a log source in QRadar.

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 a WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

Step 6 Type a suitable name for the log source.

Step 7 Optional. Type a description for the log source.

Step 8 From the **Log Source Type** list box, select **Microsoft DHCP**.

Step 9 From the **Protocol Configuration** list box, select **WinCollect Microsoft DHCP**.

Step 10 Configure values for the following parameters:

Table 9-3 Protocol parameters for WinCollect Microsoft DHCP

Parameter	Description
Log Source Identifier	Type the IP address or host name of your Microsoft DHCP Server. The log source identifier must be unique for the log source type.
Local System	Select this check box to collect only local events. 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 Console.
Domain	Type the Windows domain that includes the Microsoft DHCP Server. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the user name that is required to remotely access the DHCP Server.
Password	Type the password that is required to remotely access the DHCP Server.
Confirm Password	Confirm the password that is required to remotely access the DHCP Server.
Root Directory	Type the directory path to your DHCP event logs. For more information, see **Table 9-1**.

Table 9-3 Protocol parameters for WinCollect Microsoft DHCP (continued)

Parameter	Description
File Monitor Type	From the list box, select one of the following options: • **Notification-based (local)** - Select this option to use the Windows file system notifications to detect changes to your event log. This option is available only with local event collection. • **Polling-based (remote)** - Select this option to monitor 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.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Enabled	Select this check box to enable the log source. By default, the log source is enabled.
Credibility	From the list box, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component that is listed in the deployment editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your Microsoft DHCP events to one or more external destinations. The external destination can be any external site or storage product.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Table 9-3 Protocol parameters for WinCollect Microsoft DHCP (continued)

Parameter	Description
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Groups	Select one or more groups for the log source.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

10 THE FILE FORWARDER PLUG-IN

The File Forwarder plug-in for WinCollect allows WinCollect agents to collect and forward event logs for Windows appliances or software.

The log files read by the File Forwarder device 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.

Configuring a File Forwarder log source

The File Forwarder device plug-in allows you 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. For example, when event files are updated or added to the root log directory.

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 a WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

Step 6 Type a suitable name for the log source.

Step 7 Optional. Type a description for the log source.

Step 8 From the **Log Source Type** list box, select **Universal DSM**.

Step 9 From the **Protocol Configuration** list box, select **WinCollect File Forwarder**.

Step 10 Configure values for the following parameters:

Table 10-1 File Forwarder protocol parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname 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. ***Note:*** *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 Remote Machine field in the Adaptive Log Exporter.*
Local System	Select this check box to collect local events only. This check box disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the Console.
Domain	Type the Windows domain that includes the Windows log source. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the username required to remotely access the Windows host.
Password	Type the password required to remotely access the Windows host.
Confirm Password	Confirm the password required to remotely access the Windows host.
Root Directory	Type 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	Type the regular expression (regex) required to filter the filenames. All matching files are included in the processing. The default file pattern is **`.*`** and matches any file in the **Root Directory** field, if not changed. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: *http://docs.oracle.com/javase/tutorial/essential/regex/*

Table 10-1 File Forwarder protocol parameters (continued)

Parameter	Description
Monitoring Algorithm	From the list box, select one of the following options: • **Continuous Monitoring** - The log files in the root directory are continually monitored for new files or changes in file size. This is intended for files systems that append data to log files by adding additional lines of events. Existing log files in the root log directory are monitored and processed every time an increase in the file size is detected. New lines that have been added to the file since the last time the file was processed are forwarded to QRadar. • **File Drop** - The log files in the root log directory are read one time, then ignored in the future as the agent assumes that the file is complete and never includes additional events.
Only Monitor Files Created Today	Select this check box if you only want to monitor files with a creation date matching the current date. If you select the **File Drop** option, then the agent ignores the **Only Monitor Files Created Today** check box.
File Monitor Type	From the list box, select one of the following options: • **Notification-based (local)** - Select this option to use Windows file system notifications to detect changes to your event log. This option is only available with local event collection. • **Polling-based (remote)** - Select this option to monitor 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, then the event log is retrieved.
File Reader Type	From the list box, select one of the following options: • **Text (file held open)** - Select this option if the system generating your event log continually leaves the file open to append events to the end of the file while writing the event log. • **Text (file open when reading)** - Select this option if the system generating your event log opens the event log from the last known position, then writes events and closes the event log. • **Memory Mapped Text (local only)** - This value should not be selected, unless advised by customer support. This option is used when the system generating your event log polls the end of the event log for changes. This option requires the **Local System** check box to be selected.

Table 10-1 File Forwarder protocol parameters (continued)

Parameter	Description
Polling Interval	Type the polling interval, which is the amount of time between queries. The default polling interval is 5000 milliseconds.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list box, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your File Forwarder events to one or more destinations you have configured in your destination list. A list box with your destinations is displayed to allow you to select additional destinations for this log source. You can forward events to any external server.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings 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. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings 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.
Groups	Select one or more groups for the log source.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

11 THE MICROSOFT IAS AND NPS PLUG-IN

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.

The Microsoft IAS plug-in is available for download from the IBM support website (*https://www.ibm.com/support).*

Supported versions of Microsoft IAS in WinCollect

The Microsoft IAS plug-in for WinCollect supports the following software versions:

- 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

Overview for the WinCollect Microsoft IAS plug-in

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

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

Supported 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 your Microsoft IAS or Microsoft NPS to write an event log file to a directory. WinCollect does not support events logged to a Microsoft SQL Server.

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 your 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 to contain your IAS and NPS event logs. For example, **`\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. This ensures that the agent do not have to search large logs for new events.

Table 11-2 Event log default directory structure for Microsoft IAS

Event version	Collection type	Root Log Directory
Microsoft Windows 2003	Local	\Windows\System32\Logfiles\
	Remote	\\IAS IP address\c$\Windows\System32\Logfiles\
Microsoft Windows 2008 and Windows 2008R2	Local	\Windows\System32\Logfiles\
	Remote	\\IAS IP address\c$\Windows\System32\Logfiles\
Microsoft Windows 2012	Local	\Windows\System32\Logfiles\
	Remote	\\IAS IP address\c$\Windows\System32\Logfiles\

Configuring a Microsoft IAS log source for WinCollect

To collect events, you must create a log source for 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 Select a WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

Step 6 Type a name for the log source.

Step 7 Optional. Type a description for the log source.

Step 8 From the **Log Source Type** list box, select **Microsoft IAS Server**.

Step 9 From the **Protocol Configuration** list box, select **WinCollect Microsoft IAS / NPS**.

Step 10 Configure values for the following parameters:

Table 11-3 Protocol parameters for WinCollect Microsoft IAS

Parameter	Description
Log Source Identifier	Type the IP address or host name of your Microsoft IAS server. The log source identifier must be unique for the log source type.
Local System	Select this check box to collect only local events. 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 Console.
Domain	Type the Windows domain that includes the Microsoft IAS server. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the user name that is required to remotely access the Microsoft IAS server.
Password	Type the password that is required to remotely access the Microsoft IAS server.
Confirm Password	Confirm the password that is required to remotely access the Microsoft IAS server.
Root Directory	Type the directory path to the event log files on your Microsoft IAS server.

Table 11-3 Protocol parameters for WinCollect Microsoft IAS (continued)

Parameter	Description
File Monitor Type	From the list box, select one of the following options: • **Notification-based (local)** - Select this option to use the Windows file system notifications to detect changes to your event log. This option is available only with local event collection. • **Polling-based (remote)** - Select this option to monitor 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	Type a polling interval, which is the amount of time between queries to the root log directory for new events. The default polling interval is 5000 milliseconds.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Enabled	Select this check box to enable the log source. By default, the log source is enabled.
Credibility	From the list box, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your Microsoft IAS events to one or more external destinations. The external destination can be any external site or storage product.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Table 11-3 Protocol parameters for WinCollect Microsoft IAS (continued)

Parameter	Description
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

12 THE MICROSOFT ISA PLUG-IN

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

The Microsoft ISA plug-in is available for download from the IBM support website (*https://www.ibm.com/support).*

Supported versions of Microsoft ISA

The Microsoft ISA plug-in for WinCollect supports the following software versions:

- Microsoft ISA Server 2004
- Microsoft ISA Server 2006
- Microsoft Forefront Threat Management Gateway 2010

Overview for the WinCollect Microsoft ISA plug-in

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

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

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. Events that log to a Microsoft SQL database are not supported by WinCollect.

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 IIS format (iis_web)
- Microsoft firewall service logs in IIS format (iis_fws)

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

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

Table 12-1 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.

When you specify a root log directory, 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 ISA plug-in polls the root log directory for updated event logs every five seconds.

Table 12-2 Event log default directory structure for Microsoft ISA

Version	Collection type	Root Log Directory
Microsoft ISA 2004	Local	<Program Files>\MicrosoftISAServer\ISALogs\
	Remote	\\ISA IP address\c$\Program Files\MicrosoftISAServer\ISALogs\
Microsoft ISA 2006	Local	%systemroot%\LogFiles\ISA\
	Remote	\\ISA IP address\c$\Program Files\MicrosoftISAServer\ISA\
Microsoft Threat Management Gateway	Local	<Program Files>\<Forefront Directory>\Logs\
	Remote	\\TMG IP address\c$\Program Files\<Forefront Directory>\Logs\

Configuring a Microsoft ISA log source for WinCollect

To collect events, you must create a log source for 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 Select a WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

Step 6 Type a name for the log source.

Step 7 Optional. Type a description for the log source.

Step 8 From the **Log Source Type** list box, select **Microsoft ISA**.

Step 9 From the **Protocol Configuration** list box, select **WinCollect Microsoft ISA / Forefront TMG**.

Step 10 Configure values for the following parameters:

Table 12-3 Protocol parameters for WinCollect Microsoft ISA

Parameter	Description
Log Source Identifier	Type the IP address or host name of your Microsoft ISA or Forefront TMG server. The log source identifier must be unique for the log source type.

Table 12-3 Protocol parameters for WinCollect Microsoft ISA (continued)

Parameter	Description
Local System	Select this check box to collect only local events. 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 Console.
Domain	Type the Windows domain that includes the Microsoft ISA or Forefront TMG server. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the user name that is required to remotely access the Microsoft ISA or Forefront TMG server.
Password	Type the password that is required to remotely access the Microsoft ISA or Forefront TMG server.
Confirm Password	Confirm the password that is required to remotely access the Microsoft ISA or Forefront TMG server.
Root Directory	Type the directory path to the event log files on your Microsoft ISA or Forefront TMG server.
File Monitor Type	From the list box, select one of the following options: • **Notification-based (local)** - Select this option to use the Windows file system notifications to detect changes to your event log. This option is available only with local event collection. • **Polling-based (remote)** - Select this option to monitor 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	Type a polling interval, which is the amount of time between queries to the root log directory for new events. The default polling interval is 5000 milliseconds.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Enabled	Select this check box to enable the log source. By default, the log source is enabled.

Table 12-3 Protocol parameters for WinCollect Microsoft ISA (continued)

Parameter	Description
Credibility	From the list box, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your Microsoft IIS events to one or more external destinations. The external destination can be any external site or storage product.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

13 THE MICROSOFT IIS PLUG-IN

The Microsoft Internet Information Server (IIS) plug-in for WinCollect allows WinCollect agents to parse local event logs from your Microsoft IIS Server and forward IIS events to IBM Security QRadar.

The Microsoft IIS plug-in is available for download from the IBM support website (*https://www.ibm.com/support).*

Overview for the WinCollect Microsoft IIS plug-in

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

Microsoft Internet Information Services (IIS) includes a range of administrative features for managing websites. 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 IIS 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 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.

Supported versions of Microsoft IIS

The Microsoft IIS plug-in for WinCollect supports the following Microsoft IIS software versions:

- Microsoft IIS Server 6.0
- Microsoft IIS Server 7.0

- Microsoft IIS Server 7.5
- Microsoft IIS Server 8.0

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. The log source for the individual website can be configured 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.

Table 13-1 Event log default directory structure for Microsoft IIS

Version	Monitoring Type	Root Log Directory
Microsoft IIS 6.0	Full site	%SystemRoot%\LogFiles
Microsoft IIS 6.0	Individual site	%SystemRoot%\LogFiles*site name*
Microsoft IIS 7.0-8.0	Full site	%SystemDrive%\inetpub\logs\LogFiles
Microsoft IIS 7.0-8.0	Individual site	%SystemDrive%\inetpub\logs\LogFiles*site name*

Configuring a Microsoft IIS log source for WinCollect

To collect events from your Microsoft IIS Server, you must create a log source in QRadar.

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 a WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

Step 6 Type a suitable name for the log source.

Step 7 Optional. Type a description for the log source.

Step 8 From the **Log Source Type** list box, select **Microsoft IIS**.

Step 9 From the **Protocol Configuration** list box, select **WinCollect Microsoft IIS**.

Step 10 Configure values for the following parameters:

Table 13-2 Protocol parameters for WinCollect Microsoft IIS

Parameter	Description
Log Source Identifier	Type the IP address or host name of your Microsoft IIS Server. The log source identifier must be unique for the log source type.
Root Directory	Type the directory path to your Microsoft IIS log files.
Polling Interval	Type a polling interval, which is the amount of time between queries to the root log directory for new events. The default polling interval is 5000 milliseconds.
Protocol Logs	
FTP	Select this check box to collect File Transfer Protocol (FTP) events from Microsoft IIS.
NNTP/News	Select this check box to collect Network News Transfer Protocol (NNTP) events from Microsoft IIS.
SMTP/Mail	Select this check box to collect Simple Mail Transfer Protocol (SMTP) events from Microsoft IIS.
W3C	Select this check box to collect website (W3C) events from Microsoft IIS.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Enabled	Select this check box to enable the log source. By default, the log source is enabled.
Credibility	From the list box, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your Microsoft IIS events to one or more external destinations. The external destination can be any external site or storage product.

Table 13-2 Protocol parameters for WinCollect Microsoft IIS (continued)

Parameter	Description
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Groups	Select one or more groups for the log source.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

14 THE MICROSOFT SQL SERVER PLUG-IN

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

The Microsoft SQL plug-in is available for download from the IBM support website (*https://www.ibm.com/support).*

Overview for the WinCollect Microsoft SQL plug-in

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 assist you in troubleshooting issues or alerting you to potential or existing problems. The error log output includes the time and date 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 Servers retain 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.

The SQL event logs that are monitored by WinCollect are defined by the directory path you specify in your WinCollect SQL log source. The following table provides you with the default directory paths for the **Root Log Directory** field in your log source.

Table 14-1 Default root log directory paths Microsoft SQL events

Microsoft SQL version	Collection type	Root log directory
2000	Local	**C:\Program Files\Microsoft SQL Server\Mssql\Log**
2000	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server\Mssql\Log**
2005	Local	**c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG**
2005	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG**
2008	Local	**C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log**
2008	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log**
2008R2	Local	**C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log**
2008R2	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log**

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

Supported versions of Microsoft SQL

The Microsoft SQL plug-in for WinCollect supports the following Microsoft SQL software versions:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2003
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008R2

Configuring a Microsoft SQL log source for WinCollect

To collect events from your Microsoft SQL Server, you must configure a log source in QRadar.

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 a WinCollect agent, and click **Log Sources**.

Step 5 Click **Add**.

Step 6 Type a suitable name for the log source.

Step 7 Optional. Type a description for the log source.

Step 8 From the **Log Source Type** list box, select **Microsoft SQL**.

Step 9 From the **Protocol Configuration** list box, select **WinCollect Microsoft SQL**.

Step 10 Configure values for the following parameters:

Table 14-2 Protocol parameters for WinCollect Microsoft SQL

Parameter	Description
Log Source Identifier	Type the IP address or host name of your Microsoft SQL Server. The log source identifier must be unique for the log source type.
Local System	Select this check box to collect only local events. To collect local events, the WinCollect agent must be installed on the same host as your Microsoft SQL Server. The log source uses local system credentials to collect and forward events to the Console.
Domain	Type the Windows domain that includes the Microsoft SQL Server. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the user name that is required to remotely access the SQL Server.
Password	Type the password that is required to remotely access the SQL Server.
Confirm Password	Confirm the password that is required to remotely access the SQL Server.
Root Directory	Type the directory path to your SQL event logs. For more information, see **Table 14-1**.
Log File Name	Type the name of the file that contains the SQL error log. The default value is ERRORLOG.
File Monitor Type	From the list box, select one of the following options: • **Notification-based (local)** - Select this option to use the Windows file system notifications to detect changes to your event log. This option is available only with local event collection. • **Polling-based (remote)** - Select this option to monitor 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.
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.

Table 14-2 Protocol parameters for WinCollect Microsoft SQL (continued)

Parameter	Description
Enabled	Select this check box to enable the log source. By default, the log source is enabled.
Credibility	From the list box, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component that is listed in the deployment editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your Microsoft SQL events to one or more external destinations. The external destination can be any external site or storage product.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

A XPATH QUERIES

An XPath Query is a new log source parameter that allows you to filter (or path to) specific events when communicating with a Windows 2008-based event log.

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

Note: We do not recommend that you create your XPath queries manually unless you are proficient with XPath 1.0 and creating XPath queries.

Enable remote log management

The procedure to enable remote log management is only required when your log source is configured to remotely poll other Windows systems.

If the WinCollect log source is configured to only collect local system events, then this procedure is optional. Local system log sources that use Xpath queries do not require a remote log management firewall exception for locally collected events.

Select your operating system to configure remote event log management:

- **Windows 2008**
- **Windows 2008R2**
- **Windows 7**

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**.

Remote event log management is now enabled for Windows 2008.

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 may need to correct or select additional network types.

Step 7 Click **OK**.

Remote event log management is now enabled for Windows 2008R2.

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.

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

Step 7 Click **OK**.

Remote event log management is now enabled for Windows 7.

Creating a custom view

The Microsoft Event Viewer allows you 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 count against the limit.

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

CAUTION: *XPath queries used with the WinCollect protocol do not support the filtering of events by time range using the TimeCreated notation. Filtering events by a time range can lead to events not collecting properly.*

Procedure

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

Step 2 Type the following:

```
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**.

CAUTION: *When creating a custom view, do not select a time range from the* ***Logged*** *list box. The* ***Logged*** *list box 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 you want to include in your custom view.

Step 7 Select one of the following event sources:

- **By Log** - From the **Event Logs** list box, select the log types you want to monitor.
- **By Source** - From the **Event Sources** list box, select the event sources you want to monitor.

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

Event IDs can be typed individually using comma-separated IDs or as a range. For example 4133, 4511-4522.

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

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

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

Step 12 Type the computer or computers you want 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 that for your log source, only the events specified in the query are retrieved by the WinCollect protocol and forwarded to QRadar. Any check boxes you select from the **Standard Log Type** or **Event Type** are ignored by the log source configuration.

What to do next

You are now ready to configure a log source with the XPath query.

Adding an XPath log source

Administators 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 Type a suitable name for the log source.

Step 8 Optional. Type a description for the log source.

Step 9 From the **Log Source Type** list box, select **Microsoft Windows Security Event Log**.

Step 10 From the **Protocol Configuration** list box, select **WinCollect**.

Step 11 Configure values for the following parameters:

Table B-1 WinCollect log source parameters

Parameter	Description
Log Source Identifier	Type the IP address or hostname 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. ***Note:*** *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 Remote Machine field in the Adaptive Log Exporter.*

Table B-1 WinCollect log source parameters (continued)

Parameter	Description
Local System	Select this check box to collect local events only. This check box disables remote collection of events for the log source. The log source uses local system credentials to collect and forward events to the Console.
Domain	Type the Windows domain that includes the Windows log source. This parameter is optional. For example: • Correct - LAB1 • Correct - server1.mydomain.com • Incorrect - \\mydomain.com
User Name	Type the username required to access the Windows host.
Password	Type the password required to access the Windows host.
Confirm Password	Confirm the password required to access the Windows host.
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.
Event Types	Clear this check box. The XPath query defines the log types for the log source.
Enable Active Directory Lookups	Select this check box to enable lookups in networks that use Microsoft Active Directory. If the WinCollect agent is in the same domain as the domain controller responsible for the Active Directory lookup, you can select this check and leave the override domain and DNS parameters blank.
Override Domain Controller Name	Type an IP address or host name of the domain controller responsible for the Active Directory lookup. This field is required when the domain controller responsible for Active Directory lookup is outside of the domain of the WinCollect agent. This field is displayed when active directory lookups are enabled.
Override DNS Domain Name	Type the fully qualified domain name of the DNS server responsible for the Active Directory lookup. For example, **`wincollect.com`**. This field is displayed when active directory lookups are enabled.

Table B-1 WinCollect log source parameters (continued)

Parameter	Description
WinCollect Agent	From the list box, select the WinCollect agent to manage this log source.
Remote Machine Poll Interval (ms)	Type the polling interval, which is 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. • **7500** - A polling interval of 7500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 100 remote computers that provide 10 events per second or less. • **3500** - A polling interval of 3500 should be used where the WinCollect agent collects events from a large number of remote computers that have a low event per second rate. For example, collecting from 50 remote computers that provide 20 events per second or less. • **1000** - A polling interval of 1000 should be used where 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.
XPath Query	Type the XPath query you defined in the Event Viewer. You might be required to enable Remote Event Log Management on Windows 2008 to collect information using an XPath Query. For more information, see **XPath queries**. ***Note:*** *Microsoft Server 2003 does not support XPath Queries for events.*
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list box, select the credibility of the log source. The range is 0 to 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.

Table B-1 WinCollect log source parameters (continued)

Parameter	Description
Target Internal Destination	From the list box, select a managed host in your deployment. Any managed host with an event processor component in the Deployment Editor can be the target of an internal destination.
Target External Destination	Select this check box to forward your events to one or more destinations you have configured in your destination list. A list box with your destinations is displayed to allow you to select additional destinations for this log source. You can forward events to any external server.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list box from the System Settings 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	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list box from the System Settings 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.
Group	Select a check box with a log source group name to assign the log source to a group.

Step 12 Click **Save**.

Step 13 On the **Admin** tab, click **Deploy Changes**.

XPath query examples

The following information contains XPath examples you might use with the WinCollect protocol.

There are thousands of examples that can be created and customized for your specific network policy. We suggest you only use these Xpath examples as reference information. For more information on using XPath queries, see your Microsoft documentation.

Monitor events for a specific user

This example retrieves events from all Windows event logs for the user Guest.

```
<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

This example retrieves events from the security log for Information level events pertaining to the account authentication in Windows 2008 using, specific event IDs.

```
<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 B-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.

Account creation on a sensitive ssset

This example looks at event IDs to pull specific events when a user account 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 B-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 an account's password.
4724	An attempt was made to reset an account's password.
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.

B MANUALLY INSTALL A WINCOLLECT AGENT UPDATE

The QRadar Console can now automatically update all WinCollect agents that have automatic updated enabled in your deployment when you install an agent update RPM file.

Each WinCollect agent can have the auto update feature enabled or disabled. When enabled, WinCollect agents request updated configurations from the Console based on their configuration polling interval. If new WinCollect agent files are available for download, the agent downloads and installs any updates and restarts any required services. No event loss occurs when you update your WinCollect agent as events are buffered to disk and event collection forwarding continues when the WinCollect service starts.

Installing a WinCollect agent update

You can manually install a WinCollect agent update to your QRadar Console to update all WinCollect agents deployed in your network.

Procedure

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

http://www.ibm.com/support

Step 2 Using SSH, log in to QRadar as the root user.

Username: **`root`**

Password: **`<password>`**

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

Step 4 Type the following command:

`rpm -Uvh <filename>`

For example: **`rpm -Uvh AGENT-WinCollect-<version>.noarch.rpm`**

The installation is complete.

Step 5 Log in to QRadar.

https://**`<IP Address>`**

Where **`<IP Address>`** is the IP address of the your QRadar.

Step 6 Click the **Admin** tab.

Step 7 On the navigation menu, click **Data Sources**.

Step 8 Click the **WinCollect** icon.

Step 9 Click **Agents**.

Step 10 Select any WinCollect agent you want to update in your deployment.

Step 11 Click **Enable/Disable Automatic Updates**.

Any WinCollect agent with an auto update status of true is updated and restarted. The amount of time it takes an agent to update is dependent on the configuration polling interval for the WinCollect agent.

There is no need to install the RPM a second time. If you toggle the update status to true, then the Console can update the WinCollect agent.

C INSTALL A WINCOLLECT AGENT WITH THE COMMAND-LINE

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

Command-line installations allow you to deploy WinCollect agents simultaneously to multiple remote systems using any third-party products that provide remote or batch installs.

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 containing the WinCollect agent.

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

Step 6 Type the following command from the directory containing the WinCollect setup file:

```
AGENT-WinCollect-7.1.1.<build>-setup.exe /s /v"/qn
AUTHTOKEN=<token> CONFIGCONSOLE=<QRadar Console> HOSTNAME=<host
name> INSTALLDIR="C:\IBM\WinCollect"
```

Where:

<build> is the version number associated with the WinCollect agent software.

<token> is the authorized token created for your WinCollect agents.

<host name> is the host name or IP address of the Windows system where the WinCollect agent is going to be installed.

<QRadar Console> is the IP address of your QRadar Console.

Table D-1 WinCollect CLI installation parameters

Parameter	Description
/v	This command removes the installation progress indicators from the remote installation. This command is required.

Table D-1 WinCollect CLI installation parameters (continued)

Parameter	Description
/s	This command suppresses popup message boxes from the installation. This command is required.
/qn	This command allows the WinCollect agent to install without the user interface. This command is required.
AUTHTOKEN=<token>	This command is required by QRadar to authorize the WinCollect service. This parameter is required to install the WinCollect agent. For example, **AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc117711111** For more information on creating an authorization token for WinCollect, see **Creating an authentication token for WinCollect agents**. ***Note:*** *If the AUTHTOKEN command is not present, the CLI installation is cancelled.*
HOSTNAME=<host name>	This command sets the installation location for the WinCollect agent. This parameter is required to install the WinCollect agent. We recommend you use a unique identifier, such as an identifiable name, IP address, or host name. It is important to clearly identify your WinCollect agents, so you can manage large WinCollect agent deployments. For example, **HOSTNAME=100.10.10.255** or **HOSTNAME=%COMPUTERNAME%** or **HOSTNAME=VMRack2** ***Note:*** *The at symbol (@) is not allowed in the host identifier field.*
CONFIGCONSOLE=<QRadar Console>	This command sets the IP address of your QRadar Console. This parameter is required to install the WinCollect agent. For example, **CONFIGCONSOLE=100.10.10.1** or **CONFIGCONSOLE=hostname** ***Note:*** *This parameter is intended for the QRadar Console only. Do not specify an Event Collector or non-Console appliance in this field. If the CONFIGCONSOLE is not present, the installation is cancelled.*

Table D-1 WinCollect CLI installation parameters (continued)

Parameter	Description
INSTALLDIR	This command allows you to specify the installation directory for the WinCollect agent. Your directory name cannot include spaces and quotes should be included around the directory path. For example, INSTALLDIR="C:\IBM\WinCollect\" This command is required.

Step 7 Press Enter to install the WinCollect agent on the remote Windows host.

The WinCollect agent is installed on your host.

D TROUBLESHOOTING WINCOLLECT

Log files created by the WinCollect agent during configuration or installation contain failure message and pertinent information.

You should review the error logs before contacting support to determine the root cause of your error.

Troubleshooting WinCollect agent installations

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

Viewing the installation log

You can 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

Where:

<Date> is the installation date of the WinCollect agent.

<#00X> is the incremental log number file. Incremental log files are created with every installation, regardless of success or failure.

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

You can find several examples of installation error messages in the next section.

Installation log examples

The installation log captures the install process for WinCollect and includes information on finding the installation failure.

The information contained in the setup log file is required to troubleshoot WinCollect installations with Customer Support.

This section includes the following installation error examples:

- **Missing Authorization or Console IP Address**
- **Installation Aborted by User**
- **Installation File in Use Error**

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:

```
2012-01-27 14:40:29.189   Log opened. (Time zone: UTC-04:00)
2012-01-27 14:40:29.189   Setup version: Inno Setup version
2012-01-27 14:40:29.189   Original Setup EXE: C:\AGENT-WinCollect-setup.exe
2012-01-27 14:40:29.189   Setup command line:
/SL5="$231104,11092567,54272,C:\AGENT-WinCollect-setup.exe" /SILENT
/CONFIG_CONSOLE_ADDRESS=100.100.100.100
2012-01-27 14:40:29.189   Windows version: 6.1.7601 SP1(NT platform: Yes)
2012-01-27 14:40:29.189   64-bit Windows: Yes
2012-01-27 14:40:29.189   Processor architecture: x64
2012-01-27 14:40:29.189   User privileges: Administrative
2012-01-27 14:40:29.191   64-bit install mode: No
2012-01-27 14:40:29.192   Created temporary directory:
C:\Users\IBM_AD~1\AppData\Local\Temp\is-OPP3D.tmp
2012-01-27 14:40:29.261  INFO: Host identifier not specified; generating appropriate
default...
2012-01-27 14:40:29.261   INFO: Generated default host identifier of WinUser
2012-01-27 14:40:29.261   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)
2012-01-27 14:40:29.261   InitializeSetup returned False; aborting.
2012-01-27 14:40:29.261   Got EAbort exception.
2012-01-27 14:40:29.261   Deinitializing Setup.
2012-01-27 14:40:29.262   Log closed.
```

Installation Aborted by User

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

```
2012-03-01 18:29:49.619   Log opened. (Time zone: UTC-04:00)
2012-03-01 18:29:49.619   Setup version: Inno Setup version 5.4.2 (a)
2012-03-01 18:29:49.619   Original Setup EXE:
C:\Users\jonathan.pechta\Desktop\AGENT-WinCollect-7.0.0.beta-setup.exe
2012-03-01 18:29:49.619   Setup command line:
/SL5="$70132,11199106,54272,C:\AGENT-WinCollect-setup.exe"
2012-03-01 18:29:49.619   Windows version: 6.1.7601 SP1 (NT platform: Yes)
2012-03-01 18:29:49.619   64-bit Windows: Yes
2012-03-01 18:29:49.619   Processor architecture: x64
2012-03-01 18:29:49.619   User privileges: Administrative
2012-03-01 18:29:49.619   64-bit install mode: No
2012-03-01 18:29:49.619   Created temporary directory:
C:\Users\Admin\AppData\Local\Temp\is-AF5L2.tmp
2012-03-01 18:29:56.510   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?
2012-03-01 18:29:57.870   User chose Yes.
2012-03-01 18:29:57.870   Deinitializing Setup.
2012-03-01 18:29:57.916   Log closed.
```

Installation File in Use Error

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

```
2012-03-01 18:37:02.021   Log opened. (Time zone: UTC-04:00)
2012-03-01 18:37:02.021   Setup version: Inno Setup version 5.4.2 (a)
2012-03-01 18:37:02.021   Original Setup EXE: C:\AGENT-WinCollect-setup.exe
2012-03-01 18:37:02.021   Setup command line:
/SL5="$90134,11199106,54272,C:\AGENT-WinCollect-setup.exe" /VERYSILENT
/SUPPRESSMSGBOXES /CONFIG_CONSOLE_ADDRESS 10.100.125.101
2012-03-01 18:37:02.037   Windows version: 6.1.7601 SP1  (NT platform: Yes)
2012-03-01 18:37:02.037   64-bit Windows: Yes
2012-03-01 18:37:02.037   Processor architecture: x64
2012-03-01 18:37:02.037   User privileges: Administrative
2012-03-01 18:37:02.037   64-bit install mode: No
2012-03-01 18:37:02.037   Created temporary directory:
C:\Users\Admin\AppData\Local\Temp\is-2DKPC.tmp
2012-03-01 18:37:02.130   Starting the installation process.
2012-03-01 18:37:02.130   Directory for uninstall files: C:\Program Files
(x86)\WinCollect
2012-03-01 18:37:02.130   Will append to existing uninstall log: C:\Program Files
(x86)\WinCollect\unins000.dat
2012-03-01 18:37:02.130   -- File entry --
2012-03-01 18:37:02.130   Dest filename: C:\Program Files
(x86)\WinCollect\unins000.exe
2012-03-01 18:37:02.130   Time stamp of our file: 2012-03-01 18:37:01.927
2012-03-01 18:37:02.130   Dest file exists.
2012-03-01 18:37:02.130   Time stamp of existing file: 2012-03-01 18:30:07.010
2012-03-01 18:37:02.146   Version of our file: 51.52.0.0
2012-03-01 18:37:02.146   Version of existing file: 51.52.0.0
2012-03-01 18:37:02.146   Installing the file.
2012-03-01 18:37:02.146   Uninstaller requires administrator: Yes
2012-03-01 18:37:02.146   Leaving temporary file in place for now.
2012-03-01 18:37:02.146   -- File entry --
2012-03-01 18:37:02.146   Dest filename: C:\Program Files
(x86)\WinCollect\bin\WinCollect.exe
2012-03-01 18:37:02.146   Time stamp of our file: 2012-03-01 09:52:18.000
2012-03-01 18:37:02.146   Dest file exists.
2012-03-01 18:37:02.146   Time stamp of existing file: 2012-03-01 09:52:18.000
2012-03-01 18:37:02.146   Installing the file.
2012-03-01 18:37:02.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:03.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:04.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:05.162   The existing file appears to be in use (5). Retrying.
2012-03-01 18:37:06.162   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.
2012-03-01 18:37:06.162   User canceled the installation process.
2012-03-01 18:37:06.162   Rolling back changes.
2012-03-01 18:37:06.162   Starting the uninstallation process.
2012-03-01 18:37:06.162   Uninstallation process succeeded.
2012-03-01 18:37:06.162   Deinitializing Setup.
2012-03-01 18:37:06.162   Log closed.
```

Troubleshooting device configuration issues

The WinCollect agent creates an device log that stores configuration information and warnings about log sources 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 timestamps to assist you with locating the most recent log file.

Viewing the device log

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

The information contained in the device log file can be helpful when troubleshooting log source with Customer Support.

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 location can be the following:

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

Step 3 Open the following file:

`WinCollect_Device.<date> <identifier>.txt`

Where:

`<date>` indicates the date the device log is created.

`<version>` indicates the version of the device log file. The version increments by one each time the WinCollect Service is restarted or when adding or changing the configuration of a log source managed by the WinCollect agent.

Device Polling Overdue

The following warning for device polling overdue is displayed when the WinCollect agent is waiting to remotely collect events from a log source managed by the WinCollect agent, but the device is in queue.

This warning message can occur when adding or editing a WinCollect agent with a large number of remotely collected log sources. Each time 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 this occurs, then the following message is displayed in the device log:

```
2012-09-02 12:50:11,328 WARN Device.WindowsLog.EventLogMonitor.OnTimerExpired :
Event log 10.100.100.10 [\\10.100.100.10:Application] is seriously overdue to be
polled (interval approx 500 millisec, overdue = 45005 millisec).
```

This message does not indicate that any events are dropped, but that the WinCollect agent is waiting to poll the remote log source for events.

E 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

T

U

V

W

X