IBM Security QRadar
Version 7.2.2

WinCollect User Guide V7.2.2

Note
Before using this information and the product that it supports, read the information in "Notices" on page 47.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.4 and subsequent releases unless superseded by an updated version of this document.

Contents

About this WinCollect User Guide

This documentation provides you with information that you need to install and configure WinCollect agents, and retrieve events from Windows-based event sources. WinCollect is supported by IBM Security QRadar SIEM and IBM Security QRadar Log Manager.

Intended audience

System administrators who are responsible for installing WinCollect must be familiar with network security concepts and device configurations.

Technical documentation

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

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

Contacting customer support

For information about 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.

Chapter 1. What's new in WinCollect V7.2.2

WinCollect V7.2.2 includes a simplified installation and upgrade procedure.

WinCollect installation and update

You can now install and upgrade your WinCollect agents using an .SFS file.

Related concepts:

"Prerequisites for upgrading WinCollect agents" on page 9
Before you upgrade WinCollect agents, ensure that your software meets the version requirements.

Chapter 2. WinCollect overview

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

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

The following diagram shows two WinCollect agents, each communicating directly with the QRadar Console.

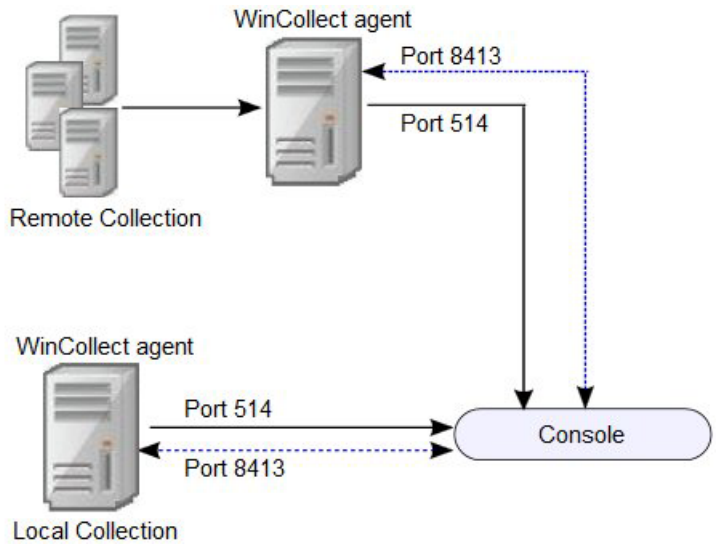

Figure 1. Deployment of multiple WinCollect agents that communicate with the QRadar Console

The following diagram shows three WinCollect agents. The agents collect events from Windows Servers and then forward the events to an Event Collector. Two of the WinCollect agents forward events to the same Event Collector. QRadar Console centrally manages the events from the Event Collectors.

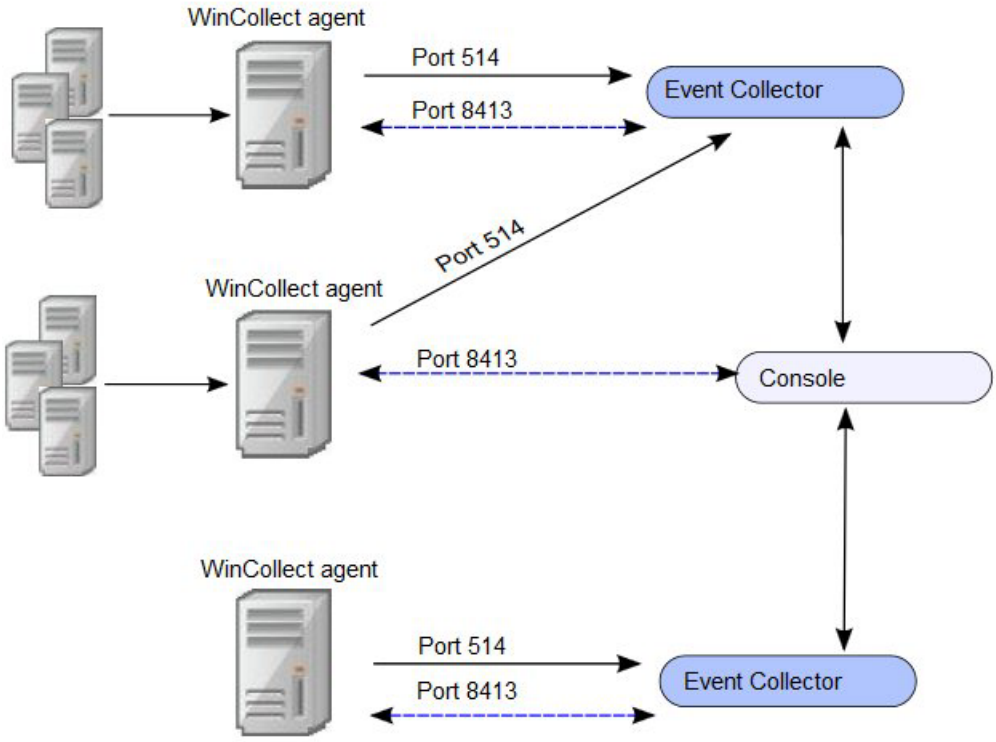

Figure 2. Deployment of multiple WinCollect agents that communicate with multiple Event Collectors

Distributed WinCollect agent installation process

You can configure multiple WinCollect agents to communicate with an Event Collector that then sends the data to your QRadar Console. To install a distributed WinCollect agent deployment, do these tasks:

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

Related concepts:

"Communication between WinCollect agents and QRadar Event Collector" on page 6

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

Related tasks:

"Installing the WinCollect agent on a Windows host" on page 13

Install the WinCollect agent on each Windows host from which you want to collect events in your network. The WinCollect agent can be configured to collect events on local host or from a remote server, or both.

Chapter 3. Installation prerequisites for WinCollect

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

Distribution options for WinCollect agents

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

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

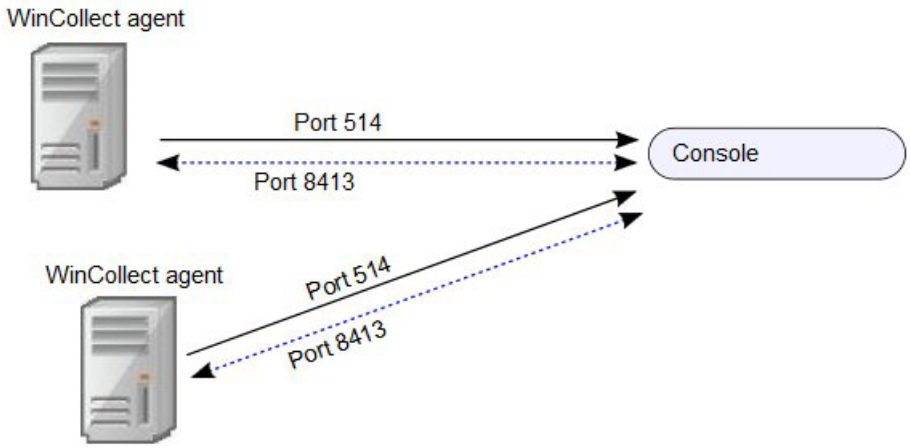

Figure 3. Local collection for WinCollect agents

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

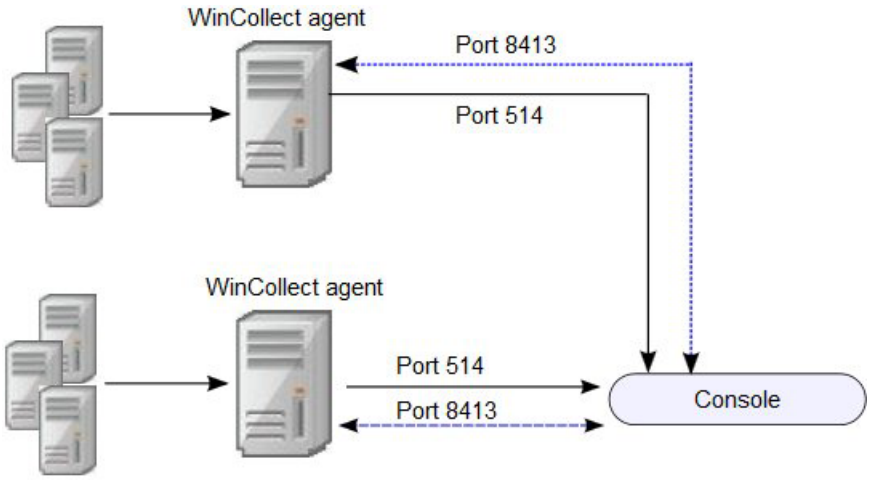

Figure 4. Remote collection for WinCollect agents

System performance and deployment strategies

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

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

Communication between WinCollect agents and QRadar Event Collector

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

WinCollect agent communication to QRadar Console and Event Collectors

All WinCollect agents communicate with the QRadar Console and Event Collectors to forward events to QRadar and request updated information. You must ensure firewalls that are between the QRadar Event Collectors and your WinCollect agents allow traffic on the following ports:

Port 8413

This port is required for managing the WinCollect agents. Port 8413 is used for features such as configuration updates. Traffic is always initiated from the WinCollect agent. This traffic is sent over TCP and communication is encrypted.

Port 514

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

WinCollect agents remotely polling Windows event sources

WinCollect agents that remotely poll other Windows operating systems for events that include extra port requirements. The following ports are used when WinCollect agents remotely poll for Windows-based events:

Table 1. Port usage for WinCollect remote polling

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

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

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

Hardware and software requirements for the WinCollect host

Ensure that the Windows-based computer that hosts the WinCollect agent meets the minimum hardware and software requirements

The following table describes the minimum hardware requirements:

Table 2. Hardware requirements for WinCollect

Requirement	Description
Memory	8 GB 2 GB reserved for the WinCollect agent
Processing	Intel Core 2 Duo processor 2.0 GHz
Disk space	3 GB of available disk space for software and log files. 6 GB might be required if events are stored on a schedule.
Available processor resources	20%

The following table describes the supported software:

Table 3. Software requirements

Requirement	Description
Operating system	Windows Server 2003 R2 Windows Server 2008 R2 Windows Server 2012 R2 Windows 7 Windows 8 Windows Vista Windows XP
Distribution	One WinCollect agent for each host.
Required user role permissions for installation	Administrator Administrative permissions are not required for remote collection.

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

WinCollect agent installations and events per second

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 the following table represent a test network. This information can help you determine the number of WinCollect agents that you need to install on your network. WinCollect supports default EPS rates and also supports tuning. Tuning can help you to improve the performance of a single WinCollect agent. You can tune local collection as part of the agent installation. Improving the performance of existing installations and remote collection must be done with the help of IBM Professional Services.

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 the test environment:

Table 4. EPS rates in a test environment

Installation type	Tuning	EPS	Log sources	Total events per second (EPS)
Local Collection	Default	250	1	250
Local Collection	Tuned	5000	1	5000
Remote Collection	Default	5 - 10	500	2500
Remote Collection	Tuned	varies	varies	2500+

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

Prerequisites for upgrading WinCollect agents

Before you upgrade WinCollect agents, ensure that your software meets the version requirements.

WinCollect and QRadar software versions

The version of the installed WinCollect depends on the version of QRadar that you are running.

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

Checking the installed version of the WinCollect agent

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

1. In QRadar, select **Help** > **About**
2. Select the **Additional Release Information** link.

You can also use ssh to log in to the QRadar Console, and run the following command:

```
rpm -qa | grep -i AGENT-WINCOLLECT
```

Checking minimum WinCollect versions before upgrade installations

Before you install the new WinCollect agent, open the **WinCollect** pane in the **Admin** tab, and ensure that all WinCollect agents are listed as version 7.1.2.

If you installed AGENT-WINCOLLECT-7.1-613263 or AGENT-WINCOLLECT-7.2-613265, but one or more agents are still listed as version 7.1.1, ensure that you wait for the V7.1.2 update to be replicated to the agents. The time that you wait depends on what you previously configured for the **Configuration Poll Interval** in the **WinCollect Agent Configuration** pane.

Chapter 4. WinCollect installations

To install WinCollect, you must download and install a WinCollect agent on your QRadar system, create an authentication token, and then install a WinCollect agent on each Windows host that you want to collect events from. You can also install the WinCollect agent on a Windows host that you want to use to remotely collect events from other Windows hosts.

Installing and upgrading the WinCollect agent on QRadar appliances

To manage a deployment of WinCollect agents from the QRadar user interface, you must first install the WinCollect agent on your QRadar Console. This agent includes the required protocols to enable communication between the QRadar system and the managed WinCollect hosts. You can use the WinCollect installation file to initially install a WinCollect agent on your QRadar host and to upgrade your WinCollect agents to newer versions.

About this task

When you upgrade a WinCollect agent file, the QRadar host automatically updates all WinCollect agents that are enabled to receive automatic updates from the Console. WinCollect agents request updated configurations from the QRadar host on a frequency that is determined by the configuration polling interval. If new WinCollect agent files are available for download, the agent downloads and installs updates and restarts required services. No events are lost when you update your WinCollect agent because events are buffered to disk. Event collection forwarding continues when the WinCollect service starts.

Procedure

1. Download the WinCollect agent installation file from the IBM website: (http://www.ibm.com/support).
2. Copy the installation file to your QRadar system.
3. Log in to QRadar as the root user.
4. For initial installations, create the `/media/patch` directory. Type the following command:

   ```
   mkdir /media/patch
   ```
5. To mount the installation file, type the following command:

   ```
   mount -t squashfs -o loop Installer_file_name.sfs /media/patch
   ```

   Example:

   ```
   mount -t squashfs -o loop 720_QRadar_wincollectupdate-7.2.0.xxx.sfs /media/patch
   ```
6. To change to the `/media/patch`, type the following command:

   ```
   cd /media/patch
   ```
7. To install WinCollect, type the following command and then follow the prompts:

   ```
   ./installer
   ```
8. Optional: If you are performing a WinCollect upgrade, push the upgrade to the managed WinCollect Agent hosts. Complete the following steps:
   a. Log in to QRadar.

b. On the navigation menu, click **Data Sources**.
c. Click the **WinCollect** icon.
d. Click **Agents**.
e. Select the WinCollect agent that you want to update in your deployment.
f. If the agent is disabled, click **Enable/Disable Automatic Updates**.

Results

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

Related tasks:

"Installing the WinCollect agent on a Windows host" on page 13
Install the WinCollect agent on each Windows host from which you want to collect events in your network. The WinCollect agent can be configured to collect events on local host or from a remote server, or both.

"Installing a WinCollect agent from the command prompt" on page 15
For non-interactive installations, you can install the WinCollect agent from the command prompt. Use silent installation to deploy WinCollect agents simultaneously to multiple remote systems.

Creating an authentication token for WinCollect agents

Third-party or external applications that interact with IBM Security QRadar require an authentication token. Before you install WinCollect agents in your network, you must create an authentication token.

This authentication token is required for every WinCollect agent you install.

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Authorized Services** icon.
4. Click **Add Authorized Service**.
5. In the **Manage Authorized Services** window, configure the parameters.

Table 5. **Add Authorized Services** *parameters*

Parameter	Description
Service Name	The name can be up to 255 characters in length, for example, `WinCollect Agent`.
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 more privileges, which can create a security concern.

6. Click **Create Service**.
7. Record the token value.

Installing the WinCollect agent on a Windows host

Install the WinCollect agent on each Windows host from which you want to collect events in your network. The WinCollect agent can be configured to collect events on local host or from a remote server, or both.

Before you begin

Ensure that the following conditions are met:

- You created an authentication token for the WinCollect agent.

  For more information, see "Creating an authentication token for WinCollect agents" on page 12..
- Your system meets the hardware and software requirements.

  For more information, see "Hardware and software requirements for the WinCollect host" on page 7.
- The required ports are available to WinCollect agents to communicate with QRadar Event Collectors.

  For more information, see "Communication between WinCollect agents and QRadar Event Collector" on page 6.
- If you want to automatically create a log source for this agent, you must know the name of the destination that you want to send your Windows log source to.

  During the installation, you can configure QRadar to automatically create a log source for the WinCollect agent host. You must configure a forwarding destination host for the log source data. For more information, see "Adding a destination" on page 21. The WinCollect agent sends the Windows event logs to the configured destination. The destination can be the console or an Event Collector. To configure automatic log source creation, your QRadar system must be updated to IBM Security QRadar SIEM V7.2.1 Patch 1 or later.

Procedure

1. Download the WinCollect agent setup file from the IBM Support website (http://www.ibm.com/support).
2. If the Services window is open on the Windows host, close it to prevent failure of the WinCollect agent installation.
3. Right-click the WinCollect agent installation file and select **Run as administrator**.
4. Follow the prompts in the installation wizard.

Table 6. WinCollect installation wizard parameters

Parameter	Description
Host Identifier	Use a unique identifier for each WinCollect agent you install. The name that you type in this field is displayed in the WinCollect agent list of the QRadar Console. The value in the **Host Identifier** field must match the value in the **Host Name** field in the WinCollect Agent configuration on the QRadar Console.

Table 6. WinCollect installation wizard parameters (continued)

Parameter	Description
Authentication Token	The authentication token that you created in QRadar, for example, `af111ff6-4f30-11eb-11fb-1fc117711111`.
Configuration Console (host and port)	Required for all installations, except stand-alone mode. Leave blank for stand-alone mode installations. The IP address or host name of your QRadar Console, for example, `100.10.10.1` or `myhost` This parameter is for the your QRadar Console or Event Collector. To use an Event Collector as your Configuration Console, your QRadar system must be updated to V7.2.1 Patch 3 or later.
StatusServer	The address of the appliance to which the status events are sent. If no value is provides, the **ConfigurationServer** is used. If both values are empty, no status messages are sent.
Enable Automatic Log Source Creation	If this check box is enabled, you must provide information about the log source and the target destination.
Log Source Name	The name can be up to 255 characters in length.
Log Source Identifier	Required if the **Enable Automatic Log Source Creation** check box is selected. Identifies the remote device that the WinCollect agent polls.
Event Logs	The Window event logs that you want the log source to collect and send to QRadar.
Target Destination	Required if **Automatic Log Source Creation** is enabled. The WinCollect destination must be configured in QRadar before you continue entering information in the installation wizard.

Table 6. WinCollect installation wizard parameters (continued)

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

Installing a WinCollect agent from the command prompt

For non-interactive installations, you can install the WinCollect agent from the command prompt. Use silent installation to deploy WinCollect agents simultaneously to multiple remote systems.

About this task

The WinCollect installer uses the following command options:

Table 7. Silent installation options for WinCollect agents

Option	Description
`/qn`	Runs the WinCollect agent installation in silent mode.
`INSTALLDIR`	The name of the installation directory cannot contain spaces. Use quotation marks, ", to enclose the directory, for example, `INSTALLDIR="C:\IBM\WinCollect\"`
`AUTHTOKEN=token`	Authorizes the WinCollect service, for example, `AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111`

Table 7. Silent installation options for WinCollect agents (continued)

Option	Description
HOSTNAME=host name	The IP address or host name of the WinCollect agent host cannot contain the "at" sign, @. The value in the **HOSTNAME** field must match the value in the **Host Name** field in the WinCollect Agent configuration on the QRadar Console.
FULLCONSOLEADDRESS=host_address	The IP address or host name of your QRadar Console or Event Collector, for example, FULLCONSOLEADDRESS=100.10.10.1. For your Windows hosts to communicate with your QRadar Event Cellector, all systems in your QRadar deployment must be updated to V7.2.1 Patch 3 or later.
LOG_SOURCE_AUTO_CREATION	If you enable this option, you must configure the log source parameters. QRadar systems must be updated to V7.2.1 Patch 1 or later.
STATUSSERVER	Optional. Specifies the server where the status messages from the agent are sent. **Example:** STATUSSERVER="100.10.10.255" STATUSSERVER="%COMPUTERNAME%"
LOG_SOURCE_AUTO_CREATION_ PARAMETERS	Ensure that each parameter uses the format: Parameter_Name=value. The parameters are separated with ampersands, &. Your QRadar system must be updated to V7.2.1 Patch 1 or later.

Table 8. Log source creation options.

Option	Description/Required Value
Component1.AgentDevice	DeviceWindowsLog
Component1.Action	create
Component1.LogSourceName	Optional. The name that you want to give to this log source.
Component1.LogSourceIdentifier	The IP address or host name of the system that the agent is installed on.

Table 8. Log source creation options (continued).

Option	Description/Required Value
Component1.Destination.Name	The name of the QRadar Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve QRadar Console system performance by moving the polling task to an Event Collector. Use this option only if the Component1.Destination.Id option is not set.
Component1.CoalesceEvents	Optional. Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the Log Activity tab. When this option is disabled, events are viewed individually and events are not bundled. New and automatically discovered log sources inherit the value from the System Settings configuration on the Console.
Component1.StoreEventPayload	Optional. Specifies that event payloads are to be stored.
Component1.Encoding	Optional. Use this option to change the default character encoding from UTF-8.
Component1.Log.Application	Windows Application Event Log
Component1.Log.Security	Windows Security Event Log
Component1.Log.System	Windows System Event Log
Component1.Log.DNS+Server	DNS Server service log
Component1.Log.Directory+Service	Directory Service service log
Component1.Log.File+Replication+Service	The file replication service.
Component1.MaxLogsToProcessPerPass	Consult IBM Customer Support before you change these values.
Component1.MinLogsToProcessPerPass	Consult IBM Customer Support before you change these values.

Procedure

1. Download the WinCollect agent setup file from the IBM website (www.ibm.com/support).
2. From the desktop, select **Start** > **Run**, type cmd, and click **OK**.
3. Ensure that the Services window is closed on the Windows host, otherwise the WinCollect agent installation fails.
4. Type the following command:

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

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

```
AGENT-WinCollect-<version>-setup.exe /s /v"/qn INSTALLDIR="C:\IBM\WinCollect"
AUTHTOKEN=eb59386c-e098-49b8-ba40-6fb46bfe7d1
FULLCONSOLEADDRESS=100.10.10.1:8413 HOSTNAME=my_host
LOG_SOURCE_AUTO_CREATION_ENABLED=True
LOG_SOURCE_AUTO_CREATION_PARAMETERS=
""Component1.AgentDevice=
DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=
LSN2&Component1.LogSourceIdentifier=
100.10.12.1>&Component1.Destination.Name=Dest1&Component1.CoalesceEvents=
True&Component1.StoreEventPayload=True&Component1.
Encoding=UTF-8&Component1.Log.Application=True&Component1.Log.Security=
True&Component1.Log.System=True&Component1.Log.DNS+Server=
False&Component1.Log.Directory+Service=
False&Component1.Log.FileReplication+Service=False"""
```

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

```
AGENT-WinCollect-<version>-setup.exe /s /v"/qn
INSTALLDIR="C:\IBM\WinCollect" AUTHTOKEN=eb59386c-e098-49b8-ba40-6fb46bfe7d1
FULLCONSOLEADDRESS=100.10.10.1 HOSTNAME=my_host
```

5. Press Enter.

Uninstalling a WinCollect agent from the command prompt

You can uninstall the WinCollect agent from the command prompt.

Procedure

1. From the desktop, select **Start** > **Run**, type `cmd`, and click **OK**.

   Attention: You need to run the command prompt as an administrative user.
2. Type the following command:

   ```
   msiexec /x{1E933549-2407-4A06-8EC5-83313513AE4B} /norestart /qn
   ```
3. Press Enter.

Chapter 5. Configuring WinCollect agents after installation

After you install a WinCollect deployment, you manage your deployment by using the IBM Security QRadar.

You can manage your WinCollect agents, destinations, and schedules. You can also manage configuration options for systems with restricted policies.

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

After you install the WinCollect agent on your Windows host, wait for QRadar to automatically discover the WinCollect agent. The automatic discovery process typically takes a few minutes to complete.

Note: The registration request to the QRadar host might be blocked by firewalls in your network.

Manually adding a WinCollect agent

If you delete your WinCollect agent, you can manually add it back. To reconnect to an existing WinCollect agent, the host name must exactly match the host name that you used before you deleted the agent.

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

WinCollect agents that were previously automatically discovered are not rediscovered in WinCollect. To add a deleted WinCollect agent back to the agent list in the QRadar, you must manually add the deleted agent.

For example, you delete a WinCollect agent that has a host identifier name VMRack1. You reinstall the agent and use the same host identifier name, VMRack1. The WinCollect agent does not automatically discover the WinCollect agent.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click **Agents**.
4. Click **Add**.
5. Configure the parameters.

   The following table describes some of the parameters:

Table 9. WinCollect agent parameters

Parameter	Description
Host Name	Depending on the method that you used to install the WinCollect agent on the remote host, the value in the **Host Name** field must match one of the following values: • **HOSTNAME** field in the WinCollect agent command-line configuration • **Host Identifier** field in the WinCollect agent installer.
Description	Optional. If you specified an IP address as the name of the WinCollect agent, add descriptive text to identify the WinCollect agent or the log sources the WinCollect agent is managing.
Automatic Updates Enabled	Controls whether configuration updates are sent to the WinCollect agent.
Heart Beat Interval	This option defines how often the WinCollect agent communicates its status to the QRadar Console. The interval ranges from 0 seconds (Off) to 20 minutes.
Configuration Poll Interval	Defines how often the WinCollect agent polls the IBM Security QRadar Console for updated log source configuration information or agent software updates. The interval ranges from 0 minutes (Off) to 20 minutes.
Disk Cache Capacity (MB)	Used to buffer events to disk when your event rate exceeds the event throttle or when the WinCollect agent is disconnected from the Console. 6 GB might be required when events are stored on a schedule.
Disk Cache Root Directory	The directory where the WinCollect agent stores cached WinCollect events.

6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

   The WinCollect agent is added to the agent list.

Related tasks:

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

Deleting a WinCollect agent

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Select the agents that you want to delete and click **Delete**.
5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

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

Related tasks:

"Manually adding a WinCollect agent" on page 19
If you delete your WinCollect agent, you can manually add it back. To reconnect to an existing WinCollect agent, the host name must exactly match the host name that you used before you deleted the agent.

WinCollect destinations

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

Adding a destination

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Destinations** and then click **Add**.
5. Configure the parameters.

   The following table describes some of the parameters

Table 10. Destination parameters

Parameter	Description
Port	IBM Security QRadar receives events from WinCollect agents on either UDP or TCP port 514.
Throttle (events per second)	Defines a limit to the number of events that the WinCollect agent can send each second.
Queue High Water Mark (bytes)	Defines an upper limit to the size of the event queue. If the high water mark limit is reached, the WinCollect agent attempts to prioritize events to reduce the number of queued events.

Table 10. Destination parameters (continued)

Parameter	Description
Queue Low Water Mark (bytes)	Defines a lower limit to the size of the event queue. If the queue changes from a high water mark to a level that is at or below the low water mark limit, the event prioritization returns to normal.
Storage Interval (seconds)	Defines an interval before the WinCollect agent writes events to disk or memory.
Processing Period (microseconds)	Defines the frequency with which the WinCollect agent evaluates the events in the forward queue and the events in the on disk queue. Used to optimize event processing.
Schedule Mode	If you select the **Forward Events** option, the WinCollect agent forwards events within a user-defined schedule. When the events are not being forwarded, they are stored until the schedule runs again. If you select the **Store Events** option, the WinCollect agent stores events to disk only within a user-defined schedule and then forwards events to the destination as specified.

6. Click **Save**.

Deleting a destination from WinCollect

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

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Destinations**.
5. Select the destination that you want to delete and click **Delete**.

Scheduling event forwarding and event storage for WinCollect agent

Use a schedule to manage when WinCollect agents forward or store events to disk in your deployment.

Schedules are not required. If a schedule does not exist, the WinCollect agent automatically forwards events and stores them only when network limitations cause delays.

You can create schedules for your WinCollect deployment to assign when the WinCollect agents in your deployment forward their events. Events that are unable to be sent during the schedule are automatically queued for the next available interval.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Schedules**.
5. Click **Add** and then click **Next**.
6. Configure the parameters, and select a check box for each day of the week that you want included in the schedule.
7. Click **Next**.
8. To add a destination to the schedule, from the **Available Destinations** list, select a destination and click the selection symbol, >,
9. Click **Next** and then click **Finish**.

Configuration options for systems with restricted policies for domain controller credentials

To collect events from remote systems without using domain administrator credentials, alternative configuration options are available. WinCollect requires credentials that are based on the type of collection that you are attempting to use for your WinCollect log sources.

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

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

Local installations with no remote polling

Install WinCollect locally on each host that you cannot remotely poll. After you install WinCollect, IBM Security QRadar automatically discovers the agent and you can create a WinCollect log source.

You can specify to use the local system by selecting the Local System check box in the log source configuration.

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

Configuring access to the registry for remote polling

Before a WinCollect log source to remotely poll for events, you must configure a local policy for your Windows-based systems.

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

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

Procedure

1. Log on to the Windows computer that you want to remotely poll for events.
2. Select **Start** > **StartPrograms** > **Administrative Tools** and then click **Local Security Policy**.
3. From the navigation menu, select **Local Policies** > **User Rights Assignment**.
4. Right-click **Manage auditing and security log** > **Properties**.
5. From the **Local Security Setting** tab, click **Add User or Group** to add your WinCollect user to the local security policy.
6. Log out of the Windows host and try to poll the remote host for Windows-based events that belong to your WinCollect log source.

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

Windows event subscriptions for WinCollect agents

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

To use event subscriptions, you must do these tasks:

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

   You must select the **Local System** check box and **Forwarded Events** check box for the WinCollect log source.

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

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

- Windows 8
- Windows 7

- Windows Server 2008 R2
- Windows Server 2012
- Windows Vista

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

Chapter 6. WinCollect Configuration Console for stand-alone agents

Use the WinCollect Configuration Console to manage a stand-alone WinCollect agent. A stand-alone WinCollect agent collects events from specified Windows-based devices and then forwards the events to your QRadar Console or Event Collector.

Troubleshooting

If you uninstall a WinCollect Agent and then reinstall the agent on a different host, you must change the `WinCollectConsole.config` file to specify the new installation directory and installation language. You can also uninstall the WinCollect Configuration Console and then reinstall it to update the location of the WinCollect Agent.

Installing a WinCollect Configuration Console

Install a WinCollect Configuration Console on a Windows operating system.

Before you begin

Ensure that the following applications are installed on the Microsoft Windows system:

- Microsoft .NET Framework 3.5
- Microsoft Management Console 3.0
- WinCollect Agent 7.2 or newer (32-bit or 64-bit)

About this task

You can install a WinCollect Configuration Console on the following 32-bit and 64-bit Windows operating systems:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1

Procedure

1. Download the WinCollect Configuration Console Setup installer from IBM Fix Central (http://www-933.ibm.com/support/fixcentral/).
2. Right-click the `WinCollect Configuration Console Setup.exe` icon, and select then **Run as administrator**.

   Important: For Windows Server 2003 and 2008, you might need to clear the **Run this program with restricted access** option.

3. Follow the instructions in the installation program.

Configuring the WinCollect Configuration Console

Use the WinCollect Configuration Console to add the devices that you want the WinCollect agent to collect events from and add the destination QRadar systems you want to forward the events to.

Procedure

1. On your Microsoft Window host, double-click the `WinCollect Configuration Console.msc` file or click the **WinCollect Configuration Console** shortcut from the Start menu.
2. For each QRadar system that you want to forward events to, add a *Destination*:
   a. On the left pane, select **Destinations**.
   b. Right-click a destination type that is listed under **Destinations** and select **Add New Destination**.
   c. Provide a name for the destination and click **Ok**.
   d. Under the destination type, double-click the destination that you added.
   e. In the **Hostname** field, type the host name or IP address of the QRadar Console or Event Collector.
   f. Optional: If you want to change the default information, configure the remaining parameters.
3. Configure the *Devices* from which you want the WinCollect agent to collect log files:
   a. On the left pane, select **Devices**.
   b. Right-click a device type that is listed under **Devices**, and then select **Add New Device**.
   c. Provide a name for the device and click **Ok**.
   d. Double-click the destination that you added.
   e. Optional: If you want the WinCollect Console to collect events from the device it is hosted on, select the **Local System** check box.
   f. If you leave the **Local System** check box clear, configure the **Domain**, **Username**, **Password**, and **Confirm Password** parameters for the device that you want to add.
   g. Configure the **Root Directory** and **Filename Pattern** fields to enable the WinCollect Agent to read the log file from the device.
   h. To add a destination to the device, click the **Add** icon that is beside the **Destination** list and select a destination.
4. On the right pane, select **Deploy Changes**.

What to do next

For troubleshooting your configuration, you can use the **Export Files** option on the right pane to create a package that contains information from WinCollect Agent installation directory and the program data folder.

Chapter 7. Log sources for WinCollect agents

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

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

Common WinCollect log source parameters

Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

Table 11. Common WinCollect log source parameters

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

Table 11. Common WinCollect log source parameters (continued)

Parameter	Description
Log Filter Type	Configures the WinCollect agent to ignore specific events from the Windows event log. You can also configure WinCollect agents to ignore events globally by ID code or log source. Exclusion filters for events are available for the following log source types: Security, System, Application, DNS Server, File Replication Service, Directory Service Global exclusions use the **EventIDCode** field from the event payload. To determine the values that are excluded, source and ID exclusions use the `Source=` field and the `EventIDCode=` field of the Windows event payload. Separate multiple sources by using a semi-colon.
Forwarded Events	Enables QRadar to collect events that are forwarded from remote Windows event sources that use subscriptions. Forward events that use event subscriptions are automatically discovered by the WinCollect agent and forwarded as if they are a syslog event source. When you configure event forwarding from your Windows system, enable event pre-rendering.
Event Types	At least one event type must be selected.
Enable Active Directory Lookups	If the WinCollect agent is in the same domain as the domain controller that is responsible for the Active Directory lookup, you can select this check and leave the override domain and DNS parameters blank.
Override Domain Controller Name	Required when the domain controller that is responsible for Active Directory lookup is outside of the domain of the WinCollect agent. The IP address or host name of the domain controller that is responsible for the Active Directory lookup.
Override DNS Domain Name	The fully qualified domain name of the DNS server that is responsible for the Active Directory lookup, for example, `wincollect.com`

Table 11. Common WinCollect log source parameters (continued)

Parameter	Description
Remote Machine Poll Interval (ms)	The number of milliseconds between queries that poll remote Windows hosts for new events. The higher the expected event rate, the more frequently the WinCollect agent needs to poll remote hosts for events. Use 7500 when the WinCollect agent collects events from many remote computers that have a low event per second rate, for example, 100 remote computers that provide 10 events per second or less. Use 3500 when the WinCollect agent collects events from many remote computers that have a low event per second rate, for example, 50 remote computers that provide 20 events per second or less. Use 1000 when the WinCollect agent collects events from a few remote computers that have a high event per second rate, for example, 10 remote computers that provide 100 events per second or less.
XPath Query	Structured XML expressions that you can use to retrieve customized events from the Windows security event log. If you specify an XPath query to filter events, the check boxes that you selected from the **Standard Log Type** or **Event Type** are ignored. The events that QRadar collects use the contents of the XPath Query. To collect information by using an XPath Query, you might be required to enable **Remote Event Log Management** on Windows 2008. Microsoft Server 2003 does not support XPath Queries for events.
Credibility	Indicates the integrity of an event or offense as determined by the credibility value from the source devices. Credibility increases if multiple sources report the same event.
Target Internal Destination	Managed hosts with an event processor component in the QRadar Deployment Editor can be the target of an internal destination.
Target External Destination	Forwards your events to one or more external destinations that you configured in your destination list.

Table 11. Common WinCollect log source parameters (continued)

Parameter	Description
Coalescing Events	Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the **System Settings** properties in QRadar. However, when you create or edit a log source, you can select the **Coalescing Events** check box to coalesce events for an individual log source.
Store Event Payload	Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the **System Settings** properties in QRadar. However, when you create or edit a log source, you can select the **Store Event Payload** check box to retain the event payload for an individual log source.

Adding a log source to a WinCollect agent

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

Before you begin

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Agents**.
5. Select the WinCollect agent, and click **Log Sources** and then click **Add**.
6. Choose one of the following options:
   - For a WinCollect log source, select **Microsoft Windows Security Event Log** from the **Log Source Type** list and then select WinCollect from the **Protocol Configuration** list.
   - Select a WinCollect plug-in option from the **Log Source Type** list , and then configure the plug-in specific parameters. For information about these parameters, see the configuration options for log sources that use WinCollect plug-ins.
7. Configure the generic log source parameters.
8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.

Microsoft DHCP log source configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft DHCP.

Restriction: The WinCollect Agent must be in the same time zone as the remote DHCP server that it is configured to poll.

You must also configure parameters that are not specific to this plug-in.

Table 12. Microsoft DHCP protocol parameters

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

Related reference:

"Common WinCollect log source parameters" on page 29
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

File Forwarder log source configuration options

Use the reference information to configure the WinCollect plug-in for File Forwarder log source.

You must also configure parameters that are not specific to this plug-in.

Table 13. File Forwarder protocol parameters

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

Table 13. File Forwarder protocol parameters (continued)

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

Related reference:

"Common WinCollect log source parameters" on page 29
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

Microsoft IAS log source configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft IAS.

You must also configure parameters that are not specific to this plug-in.

Table 14. Microsoft IAS protocol parameters

Parameter	Description
Log Source Type	**Microsoft IAS Server**
Protocol Configuration	**WinCollect Microsoft IAS / NPS**
Local System	To collect local events, the WinCollect agent must be installed on the same host as your Microsoft DHCP Server. The log source uses local system credentials to collect and forward events to the QRadar
Folder Path	For a local directory path, use the`%WINDIR%\System32\Logfiles`directory. For a remote directory path, use the `\\<IASIP>\c$\Windows\System32\Logfiles` directory.
File Monitor Policy	The **Notification-based (local)** option uses the Windows file system notifications to detect changes to your event log. The **Polling-based (remote)** option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.
Polling Interval	The amount of time between queries to the root log directory for new events.

Related reference:

"Common WinCollect log source parameters" on page 29
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

Microsoft IIS protocol configuration options

You can configure a log source to use the Microsoft IIS protocol. This protocol supports a single point of collection for W3C format log files that are on a Microsoft IIS web server.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft IIS protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Restriction: The Microsoft authentication protocol NTLMv2 is not supported by the Microsoft IIS protocol.

You must also configure parameters that are not specific to this plug-in.

Table 15. Microsoft IIS protocol parameters

Parameter	Description
Protocol Configuration	**Microsoft IIS**
File Pattern	The regular expression (regex) that identifies the event logs.
Root Directory	The directory path to your Microsoft IIS log files. • For Microsoft IIS 6.0 (full site), use %SystemRoot%\LogFiles • For Microsoft IIS 6.0 (individual site), use %SystemRoot%\LogFiles\site name • For Microsoft 7.0-8.0 (full site), use %SystemDrive%\inetpub\logs\LogFiles • For Microsoft IIS 7.0-8.0 (individual site), use %SystemDrive%\inetpub\logs\LogFiles\site name
Protocol Logs	The items that you want to collect from Microsoft IIS.

Microsoft ISA log configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft ISA.

You must also configure parameters that are not specific to this plug-in.

Table 16. WinCollect Microsoft DHCP protocol parameters

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

Table 16. WinCollect Microsoft DHCP protocol parameters (continued)

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

Related reference:

"Common WinCollect log source parameters" on page 29
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

Juniper Steel-Belted Radius log source configuration options

Use the reference information to configure the WinCollect plug-in for Juniper Steel-Belted Radius.

You must also configure parameters that are not specific to this plug-in.

Table 17. WinCollect Juniper Steel-Belted Radius protocol parameters.

Parameter	Description
Log Source Type	**Juniper Steel-Belted Radius**
Protocol Configuration	**WinCollect SBR**
Local System	To collect local events, the WinCollect agent must be installed on the same host as the Juniper Steel-Belted Radius server. The log source uses local system credentials to collect and forward events to the IBM Security QRadar.
Root Directory	The directory that contains the files that you want to monitor. Due to the restrictions in the distributed system, the QRadar user interface does not verify the path to the root directory. Ensure that you enter a valid local Windows path.
File Monitor Policy	The **Notification-based (local)** option uses the Windows file system notifications to detect changes to your event log. The **Polling-based (remote)** option monitors changes to remote files and directories. The agent polls the remote event log and compares the file to the last polling interval. If the event log contains new events, the event log is retrieved.
Polling Interval	The amount of time between queries to the root log directory for new events.

Microsoft SQL Server log source configuration options

Use the reference information to configure the WinCollect plug-in for Microsoft SQL Server.

You must also configure parameters that are not specific to this plug-in.

Table 18. Microsoft SQL Server protocol parameters

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

Table 18. Microsoft SQL Server protocol parameters (continued)

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

Related reference:

"Common WinCollect log source parameters" on page 29
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

NetApp Data ONTAP configuration options

Use this reference information to configure the WinCollect plug-in for NetApp ONTAP.

You must also configure parameters that are not specific to this plug-in.

Table 19. WinCollect NetApp Data ONTAP protocol parameters.

Parameter	Description
Log Source Type	NetApp Data ONTAP
Protocol Configuration	WinCollect NetApp Data ONTAP
User Name	The account name that is used to log in to the Windows domain or system.
Domain	The network domain to which the user name belongs.
Target Directory	The network path to the directory where you want to monitor files. **Attention:** Due to the restrictions in the distributed system, this path is not verified by the QRadar user interface. Ensure that you type a valid Windows UNC path that is shared by the NetApp appliance.
Polling Interval	The interval, in milliseconds, at which the remote directory is checked for new event log files. Even though the remote device does not generate new files on a period of less than 60 seconds, the optimal polling interval is less than 60 seconds. This practice ensures the collection of files that might be when WinCollect is restarted.
WinCollect Agent	The WinCollect Agent that you want to use to collect NetApp Data ONTAP events.
Target Internal Destination	The QRadar Event Collector that you want to use.
Target External Destinations	To enable the use of an external event collector, select the check box and then select an external destination.

XPath log source configuration options

Use the reference information to create a log source that includes the XPath query from the Event Viewer

You must also configure parameters that are not specific to this plug-in.

Table 20. Microsoft SQL Server protocol parameters

Parameter	Description
Log Source Type	**Microsoft Windows Security Event Log**
Protocol Configuration	**WinCollect**
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.
WinCollect Agent	The WinCollect agent that manages this log source.

Table 20. Microsoft SQL Server protocol parameters (continued)

Parameter	Description
XPath Query	The XPath query that you defined in Microsoft Event Viewer. To collect information by using an XPath query, you might be required to enable the **Remote Event Log Management** option on Windows 2008. **Note:** Microsoft Server 2003 does not support XPath Queries for events.

Related reference:

"Common WinCollect log source parameters" on page 29
Common parameters are used when you configure a log source for a WinCollect agent or a WinCollect plug-in. Each WinCollect plug-in also has a unique set of configuration options.

XPath queries

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

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

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

Enabling remote log management on Windows 7

Enables remote log management only when your log source is configured to remotely poll other Windows operating systems. You can enable remote log management on Windows 7 for XPath queries.

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

Procedure

1. On your desktop, select **Start** > **Control Panel**.
2. Click the **System and Security** icon.
3. Click **Allow a program through Windows Firewall**.
4. If prompted, click **Continue**.
5. Click **Change Settings**.
6. From the Allowed programs and features pane, select **Remote Event Log Management**.

   Depending on your network, you might need to correct or select more network types.
7. Click **OK**.

Enabling remote log management on Windows 2008

Enables remote log management only when your log source is configured to remotely poll other Windows operating systems. You can enable remote log management on Windows Server 2008 for XPath queries.

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

Procedure

1. On your desktop, select **Start** > **Control Panel**.
2. Click the **Security** icon.
3. Click **Allow a program through Windows Firewall**.
4. If prompted, click **Continue**.
5. From the **Exceptions** tab, select **Remote Event Log Management** and click **OK**.

Enabling remote log management on Windows 2008R2

Enables remote log management only when your log source is configured to remotely poll other Windows operating systems. You can enable remote log management on Windows 2008R2 for XPath queries.

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

Procedure

1. On your desktop, select **Start** > **Control Panel**.
2. Click the **Window Firewall** icon.
3. Click **Allow a program through Windows Firewall**.
4. If prompted, click **Continue**.
5. Click **Change Settings**.
6. From the Allowed programs and features pane, select **Remote Event Log Management** check box.

   Depending on your network, you might need to correct or select more network types.
7. Click **OK**.

Creating a custom view

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

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

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

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

Procedure

1. On your desktop, select **Start** > **Run**.
2. Type the following command:

```
Eventvwr.msc
```

3. Click **OK**.
4. If you are prompted, type the administrator password and press Enter.
5. Click **Action** > **Create Custom View**.

   When you create a custom view, do not select a time range from the **Logged** list. The **Logged** list includes the **TimeCreated** element, which is not supported in XPath queries for the WinCollect protocol.
6. In **Event Level**, select the check boxes for the severity of events that you want to include in your custom view.
7. Select an event source.
8. Type the event IDs to filter from the event or log source.

   Use commas to separate IDs. The following list contains an individual ID and a range: 4133, 4511-4522
9. From the **Task Category** list, select the categories to filter from the event or log source.
10. From the **Keywords** list, select the keywords to filter from the event or log source.
11. Type the user name to filter from the event or log source.
12. Type the computer or computers to filter from the event or log source.
13. Click the **XML tab**.
14. Copy and paste the XML to the **XPath Query** field of your WinCollect log source configuration

    Note: If you specify an XPath query for your log source, only the events that are specified in the query are retrieved by the WinCollect protocol and forwarded to IBM Security QRadar. Check boxes that you select from the **Standard Log Type** or **Event Type** are ignored by the log source configuration.

What to do next

Configure a log source with the XPath query. For more information, see "XPath log source configuration options" on page 40.

XPath query examples

Use XPath examples for monitoring events and retrieving logon credentials, as a reference when you create XPath queries.

For more information about XPath queries, see your Microsoft documentation.

Example: Monitoring events for a specific user

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

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

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

Example: Credential logon for Windows 2008

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

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

Table 21. Event IDs used in credential logon 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.

Example: Retrieving events based on user

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

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

Table 22. Event IDs used in database example.

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

Table 22. Event IDs used in database example (continued).

ID	Description
4743	A user account was deleted.

Adding multiple log sources

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

You can upload a text file that contains a list of IP addresses or host names, run a query against a domain controller to get a list of hosts, or manually enter a list of IP addresses or host names by typing them in one at a time.

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Select the WinCollect agent, and click **Log Sources**.
5. From the **Bulk Actions** menu, select **Bulk Add**.
6. Configure values for your log sources.
7. Select one of the following methods to bulk import log sources:
   - Select the **File Upload** tab and then select a text file IP addresses or host names of log sources that you want to add. The maximum number of log sources you can add is 500.

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

Related tasks:

"Adding a log source to a WinCollect agent" on page 32
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.

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 Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.