Engineering
Simplicity

Juniper Secure Analytics WinCollect User Guide

Published
2022-05-13

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Secure Analytics WinCollect User Guide
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

6

Log Sources for WinCollect Agents

7

Troubleshooting WinCollect Deployment Issues

About This Guide

Use this guide to understand how to can use JSA to manage and collect Windows-based events.

1

CHAPTER

What's New in WinCollect

What's New in WinCollect

IN THIS SECTION

WinCollect

WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows logs to JSA. WinCollect can collect events from systems locally or be configured to remotely poll other Windows systems for events.

Learn about the new features in each WinCollect release.

What's new in 7.3.0

NOTE: WinCollect 7.3.0 can only be installed on JSA 7.3.3 or later.

WinCollect 7.3.0 includes the following capabilities:

- You can set the Status Server setting to **Disabled** to send only a heartbeat without status messages, or set the value to **None** if you don't want to send a heartbeat or status messages.
- You can add a secondary destination to receive events from your WinCollect agents if the primary destination fails.

  NOTE: This feature is available for stand-alone deployments. This will be available for Managed agents in a future release of JSA.

What's new in 7.2.9

WinCollect 7.2.9 includes the following capabilities:

- Event Forwarding Filtering.
- Event Forwarding Sending to one log source support.
- Digitally signed installers.
- Millisecond Time format for Event Log collection.
- DHCP support for Spanish and Polish.
- CP Support for Status Messages.
- File Forwarder multi-line log support.
- Removed MMC requirement from patch installer install.

RELATED DOCUMENTATION

WinCollect Overview | 5

2

CHAPTER

WinCollect Overview

WinCollect Overview

IN THIS SECTION

WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows logs to JSA. WinCollect can collect events from systems locally or be configured to remotely poll other Windows systems for events.

WinCollect is one of many solutions for Windows event collection. For more information about alternatives to WinCollect, see the *Configuring DSMs Guide*.

How Does WinCollect Work?

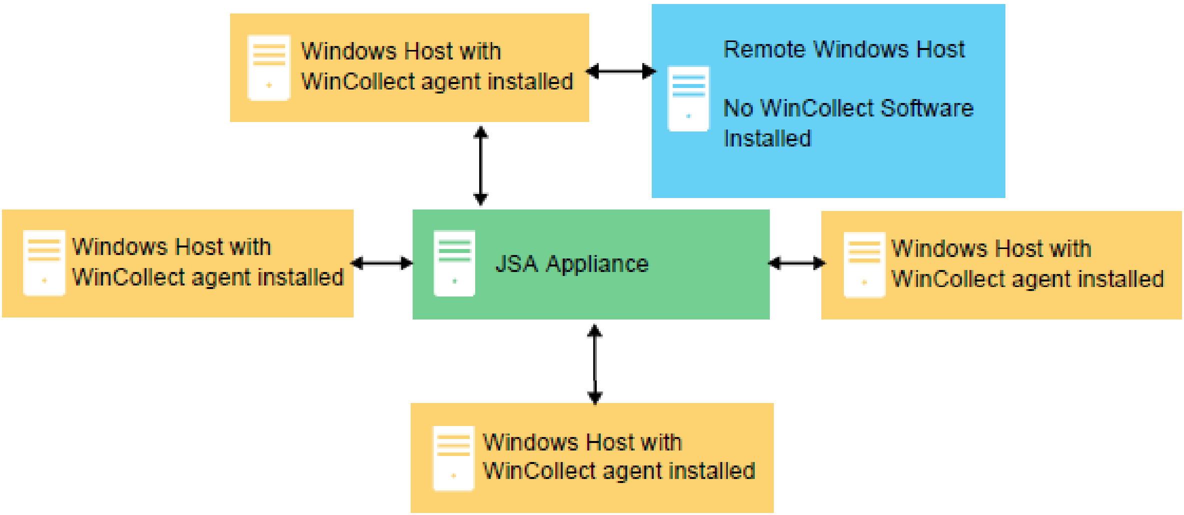
WinCollect uses the Windows Event Log API to gather events, and then WinCollect sends the events to JSA.

WinCollect Managed Deployment

A managed WinCollect deployment has a JSA appliance that shares information with the WinCollect agent installed on the Windows hosts that you want to monitor. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the

WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to JSA.

Figure 1: WinCollect Managed Deployment Example


Windows Host with WinCollect agent installed
Remote Windows Host
No WinCollect Software Installed
Windows Host with WinCollect agent installed
JSA Appliance
Windows Host with WinCollect agent installed
Windows Host with WinCollect agent installed

NOTE: In a managed deployment, the WinCollect agents that are installed on Windows hosts can be managed by any JSA console, Event Collector, or Event Processor.

In a managed deployment, WinCollect is designed to work with up to 500 Windows agents per Console and managed host. For example, if you have a deployment with a Console, an Event Processor, and an Event Collector, each can support up to 500 Windows agents, for a total of 1,500. If you want to monitor more than 500 Windows agents per Console or managed host, use the stand-alone WinCollect deployment.

For more information, see "Stand-alone WinCollect Installations" on page 33

The managed WinCollect deployment has the following capabilities:

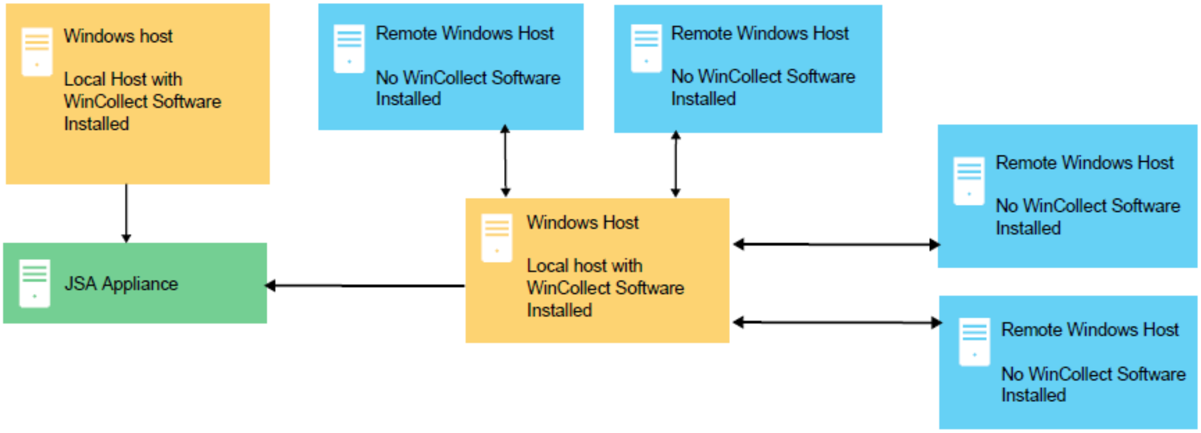
- Central management from the JSA Console or managed host.
- Automatic local log source creation at the time of installation.
- Event storage to ensure that no events are dropped.
- Collects forwarded events from Microsoft Subscriptions.
- Filters events by using XPath queries or exclusion filters.

- Supports virtual machine installations.
- Console can send software updates to remote WinCollect agents without you reinstalling agents in your network.
- Forwards events on a set schedule (Store and Forward)

WinCollect Stand-alone Deployment

If you need to collect Windows events from more than 500 hosts, use the stand-alone WinCollect deployment. A stand-alone deployment is a Windows host in unmanaged mode with WinCollect software installed. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to JSA. To save time when you configure more than 500 Windows hosts, you can use a solution such as Juniper Networks Endpoint Manager. Automation can help you manage stand-alone instances.

Figure 2: WinCollect Stand-alone Deployment Example


Windows host
Local Host with WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed
JSA Appliance
Windows Host
Local host with WinCollect Software Installed
Remote Windows Host
No WinCollect Software Installed

You can also deploy stand-alone WinCollect to consolidate event data on one Windows host, where WinCollect collects events to send to JSA.

Stand-alone WinCollect mode has the following capabilities:

- You can configure each WinCollect agent by using the WinCollect Configuration Console.
- You can update WinCollect software with the software update installer.
- Event storage to ensure that no events are dropped.

- Collects forwarded events from Microsoft Subscriptions.
- Filters events by using XPath queries or exclusion filters.
- Supports virtual machine installations.
- Sends events to JSA using TLS Syslog.
- Automatically create a local log source at the time of agent installation.

Capabilities of managed and stand-alone WinCollect deployments

Review the following table to understand which capabilities are available when using managed or standalone WinCollect agents.

Table 1: Capabilities of managed WinCollect vs. stand-alone WinCollect

Capability	Managed WinCollect	Stand-alone WinCollect
Central management from the JSA Console or managed host.	Yes	No
Automatic local log source creation at the time of installation.	Yes	Yes
Event storage to ensure that no events are dropped.	Yes	Yes
Collects forwarded events from Microsoft Subscriptions.	Yes	Yes
Filters events by using XPath queries or exclusion filters.	Yes	Yes
Supports virtual machine installations	Yes	Yes
JSA Console can send software updates to WinCollect agents.	Yes	No

Table 1: Capabilities of managed WinCollect vs. stand-alone WinCollect *(Continued)*

Capability	Managed WinCollect	Stand-alone WinCollect
Forwards events on a set schedule (Store and Forward).	Yes	No
You can configure each WinCollect agent by using the WinCollect Configuration Console.	No	Yes
You can update WinCollect software with the software update installer	No	Yes
Available with on-prem JSA	Yes	Yes

Setting Up a Managed WinCollect Deployment

For a managed deployment, follow these steps:

1. Understand the prerequisites for managed WinCollect, which ports to use, what hardware is required, how to upgrade. For more information, see "Installation Prerequisites for WinCollect" on page 13.

2. Install the WinCollect application on the JSA console that is used to monitor your Windows hosts. For more information, see "Installing and Upgrading the WinCollect Application on JSA Appliances" on page 27.

3. Create an authentication token so that the managed WinCollect agents can exchange data with JSA appliances. For more information, see "Creating an Authentication Token for WinCollect Agents" on page 30.

4. Configure a forwarding destination host for the log source data.

5. Install managed WinCollect agents on the Windows hosts. For more information, see one of the following options:

   - "Installing the WinCollect Agent on a Windows Host" on page 40

- "Installing a WinCollect Agent from the Command Prompt" on page 44, or
- "Manually Adding a WinCollect Agent " on page 56

6. If you want to configure forwarded event or event subscriptions, see Windows Event Subscriptions for WinCollect Agents..

7. If you want to use the legacy Log Source UI to bulk add log sources that will be remotely polled by a single WinCollect agent, see "Bulk Log Sources for Remote Event Collection" on page 132.

8. Tune your WinCollect log sources. For more information, see the Event Rate Tuning Profile parameter in Windows Log Source Parameters.

9. If you want a managed WinCollect agent to send events to multiple JSA destinations in case one fails, see "Adding Multiple Destinations to WinCollect Agents" on page 31.

Setting Up a Stand-alone WinCollect Deployment

For a stand-alone deployment, follow these steps:

1. Understand the prerequisites for stand-alone WinCollect, which ports to use, what hardware is required, how to upgrade. For more information, see "Installation Prerequisites for WinCollect" on page 13.

2. Install stand-alone WinCollect agents on the Windows hosts. For more information, see "Installing the WinCollect Agent on a Windows Host" on page 40.

3. If you want to add new log sources to your agent or modify existing log sources, install the WinCollect stand-alone configuration console. For more information, see "Installing the Configuration Console" on page 35 or "Silently Installing, Upgrading, and Uninstalling WinCollect Software" on page 36.

4. Configure the destination where the Windows hosts send Windows events. For more information, see "Adding a Destination to the WinCollect Configuration Console" on page 65.

5. If you want to use the stand-alone WinCollect agent to collect events from other devices using remote polling, create a credential in the WinCollect stand-alone configuration console, so that WinCollect can log in to the remote devices. See "Creating a WinCollect Credential" on page 64.

6. If you want to add additional log sources to the stand-alone WinCollect agent, do so using the WinCollect stand-alone configuration console. For more information, see "Adding a Device to the WinCollect Configuration Console" on page 67.

MSEVEN6 Protocol

MSEVEN6 is a Microsoft event protocol that collects more information from an event log, such as the task, keyword, and opcode. It also provides a better message formatting than other event protocols do.

The MSEVEN protocol uses port 445. The NETBIOS ports (137 - 139) can be used for hostname resolution. When the WinCollect agent polls a remote event log by using MSEVEN6, the initial communication with the remote computer occurs on port 135 (dynamic port mapper), which assigns the connection to a dynamic port. The default port range for dynamic ports is between port 49152 and port 65535, but might be different depending on the server type. For example, the default port range for Microsoft Exchange servers is 6005 – 58321.

XPath queries always use the MSEVEN6 event protocol.

In managed mode, you can change the protocol by editing the **Event Log Poll Protocol** field and selecting the desired protocol. For upgrades, depending on which version of WinCollect you are upgrading from, the log source continues to use MSEVEN. Use the Log Source Management app to configure multiple log sources to the desired protocol.

In a stand-alone WinCollect deployment, you can set a global Default Event Log Poll Protocol. The default value is **MSEVEN6**. To configure a single Microsoft Windows Event Log device to use the global Default Event Log Poll Protocol, select **Default from the Basic Configurations** page of the device. Otherwise, select **MSEVEN6** or **MSEVEN** to override the global Default Event Log Poll Protocol.

In a stand-alone WinCollect deployment, you can include milliseconds in the time stamp for Event Logs. This option is only compatible in a stand-alone WinCollect deployment that uses the MSEVEN6 protocol. It is not supported by the MSEVEN protocol.

3

CHAPTER

Installation Prerequisites for WinCollect

Installation Prerequisites for WinCollect

IN THIS SECTION

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

Supported Versions

Administrators should be aware that supported software versions for WinCollect is the Latest version (n) and latest minus one (n-1). This means that the two newest versions of WinCollect are the versions for which JSA Support will provide full support with any support tickets (cases) that are opened. Customers using older versions of WinCollect will receive minimal, best effort, support.. To prevent issues, it is important that administrators keep WinCollect deployments updated when new versions are posted to https://support.juniper.net/support/.

> **NOTE**: WinCollectdoes not support agents installed on Windows servers that use Network Address Translation (NAT). If you place an Event Collector in the same NAT environment as the managed agents, the agents can use the Event Collector as a configuration server, status server, and to send events. However, the Event Collector must be configured to use NAT.

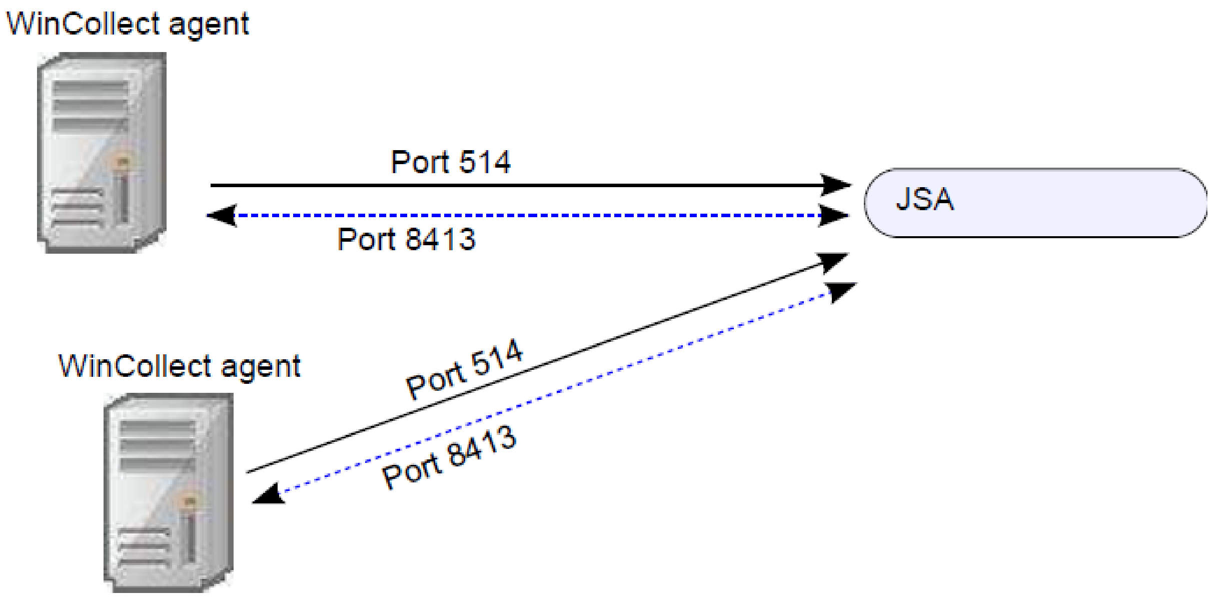
Distribution Options for WinCollect Agents

WinCollect agents can be distributed in a remote collection configuration or installed on the local host.

- **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.

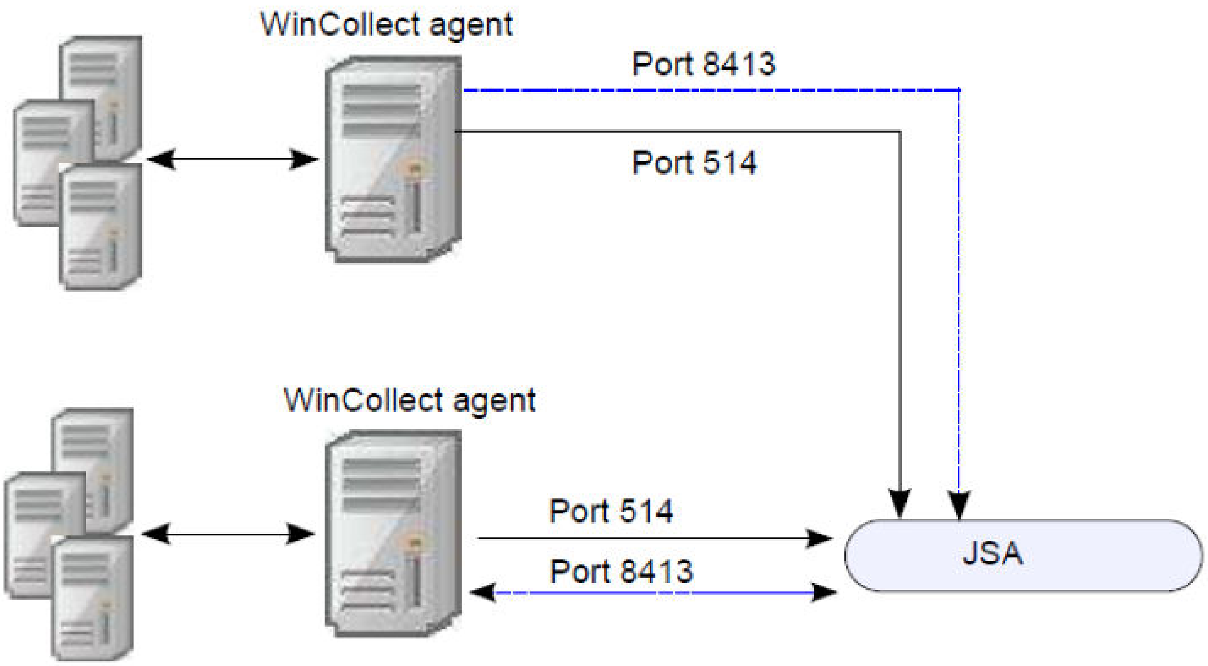
NOTE: JSA Support recommends local collection on Domain Controllers and other high EPS servers, as it is more stable than remote collection. If you are remote polling logs on potentially high EPS servers, JSA Support might require you to install an agent locally on the server.

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



Communication Between WinCollect Agents and JSA

IN THIS SECTION

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

WinCollect Agent Communication to JSA Console and Event Collectors

All WinCollect agents communicate with the JSA Console and Event Collectors to forward events to JSA and request updated information. Managed WinCollect agents also request and receive updated code and configuration changes. You must ensure firewalls that are between the JSA Event Collectors and your WinCollect agents allow traffic on the following ports:

- **Port 8413**--This port is used for managing the WinCollect agents to request and receive code and configuration updates. Traffic is always initiated from the WinCollect agent, and is sent over TCP. Communication is encrypted by using the JSA Console public key and the `ConfigurationServer.PEM` file on the agent.

  Create a bidirectional rule to allow communication from the WinCollect agent to JSA on port 8413. If the rule is not bidirectional, traffic is blocked. JSA does not send updates to the WinCollect agent on port 8413.

- **Port 514**--This port is used by the WinCollect agent to forward syslog events to JSA. You can configure WinCollect log sources to provide events by using TCP or UDP. You can decide which transmission protocol to use 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 require extra ports to be open. These ports need to be open on the WinCollect agent computer and the computer(s) that are remotely polled, but not on your JSA appliances. The following table describes the ports that are used.

Table 2: 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

Table 2: Port Usage for WinCollect Remote Polling *(Continued)*

Port	Protocol	Usage
445	TCP	Microsoft Directory Services for file transfers that use Windows share
49152 – 65535 **NOTE**: Exchange servers are configured for a port range of 6005 – 58321 by default.	TCP	Default dynamic port range for TCP/IP

The MSEVEN protocol uses port 445. The NETBIOS ports (137 - 139) can be used for host name resolution. When the WinCollect agent polls a remote event log by using MSEVEN6, the initial communication with the remote machine occurs on port 135 (dynamic port mapper), which assigns the connection to a dynamic port. The default port range for dynamic ports is between port 49152 and port 65535, but might be different dependent on the server type. For example, Exchange servers are configured for a port range of 6005 – 58321 by default.

To allow traffic on these dynamic ports, enable and allow the two following inbound rules on the Windows server that is being polled:

- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

NOTE: To limit the number of events that are sent to JSA, administrators can use exclusion filters for an event based on the EventID or Process.

Enabling Remote Log Management on Windows

You can enable 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 2012 R2 for XPath queries.

NOTE: WinCollect does not support reverting Citrix Virtual Machines that are polled remotely.

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**.

RELATED DOCUMENTATION

Hardware and Software Requirements for the WinCollect Host | 18

Prerequisites for Upgrading WinCollect Agents | 23

Hardware and Software Requirements for the WinCollect Host

IN THIS SECTION

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

Hardware/virtual Machine Requirements

The following table describes the minimum hardware requirements for local collection:

Table 3: Hardware/VM Requirements for Local Collection by Using WinCollect

Requirement	Description
Memory	The WinCollect agent has a very low memory footprint. The following numbers were generated on virtual machines (VMs) with two Logical cores and 2-4GB of memory. 1 Event per second (EPS) or less: 9 MB 100 EPS or less: 10.5 MB 2,500 EPS or less: 15 MB 5,000 EPS or less: 20 MB
Processor	Intel Core i3 or equivalent Systems were tested on VMs with two Cores and 2 - 4 GB of memory.
Available processor resources	0-35%, depending on CPU, EPS, and number of endpoints polled. See the following table for examples. Very high EPS rates have a direct effect on the Average CPU used by the WinCollect Agent.
Disk space	100 MB for software, plus up to 100 MB for files. Upto 6 GB might be required if you store events to disk.

NOTE: WinCollect CPU and memory loads depend on several factors, including the number of events per second that are being processed.

The following table shows resources that are used by WinCollect in testing environments with various hardware configurations and EPS counts.

Table 4: Comparison of Tested WinCollect Environments (local polling)

Profile	Type	OS	RAM	Cores	Avg FPS	RAM used	Avg CPU
Maximum EPS	VM	Windows 2019 Server	4 GB	2	5,000	20 MB	32%

Table 4: Comparison of Tested WinCollect Environments (local polling) ***(Continued)***

Profile	Type	OS	RAM	Cores	Avg FPS	RAM used	Avg CPU
High EPS	VM	Windows 2019 Server	4 GB	2	2,500	15 MB	18%
Meduim EPS	VM	Windows 2019 Server	4 GB	2	100	10.5 MB	1.2%
Low EPS	VM	Windows 2019 Server	4 GB	2	<1	9 MB	<1%

Similar results were found testing with Windows 2016 Server.

A lower provisioned Windows 10 VM yielded similar results.

Profile	Type	OS	RAM	Cores	Avg EPS	RAM used	Avg CPU
High EPS	VM	Windows 10	2 GB	2	2500	11 MB	22%
Medium EPS	VM	Windows 10	2 GB	2	100	5.5 MB	1.5%
Low EPS	VM	Windows 10	2 GB	2	<1	5.5 MB	<1

The following table describes the minimum hardware requirements for remote collection:

Table 5: Hardware/VM Requirements for Remote Collection by Using WinCollect

Requirement	Description
Memory	5 endpoints or less: 80 MB 250 endpoints or less: 293 MB 500 endpoints or less: 609 MB
Processor	Intel Core i3 or equivalent

Table 5: Hardware/VM Requirements for Remote Collection by Using WinCollect *(Continued)*

Requirement	Description
Available processor resources	Approximately 20%, depending on CPU, EPS, and number of endpoints polled.
Disk space	100 MB for software, plus up to 100 MB for files. Upto 6 GB might be required if you store events to disk.

WinCollect CPU and memory loads depend on several factors, including the number of events per second that are being processed and the number of remote endpoints that are being polled.

Table 6: Comparison of Tested WinCollect Environments (remote polling)

Profile	Type	OS	RAM	Cores	Avg FPS	RAM used	Avg CPU
High EPS Low Device Count	VM	Windows 2012 Server	12 GB	6	3000	78 MB	6.5%
Medium EPS and Device count	VM	Windows 2016 Server	12 GB	250	2500	290 MB	14%
High EPS High Device count	VM	Windows 2016 Server	16 GB	500	5000	605 MB	10.75%

Software Requirements

Table 7: Software Requirements

Requirement	Description
Operating system	Windows Server 2022 (including Core) Windows Server 2019 (including Core) Windows Server 2016 (including Core) Windows Server 2012 (including Core) Windows 10
Distribution	One WinCollect agent for each Windows host.
Required user role permissions for installation	Administrator, or local administrator Administrative permissions are not required for remote collection

NOTE: WinCollect is not supported on versions of Windows that are designated end-of-life by Microsoft After software is beyond the Extended Support End Date, the product might still function as expected. However, Juniper does not make code or vulnerability fixes to resolve WinCollect issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the "Extended Support End Date”. For more information, see https://support.microsoft.com/en-us/lifecycle/search (https://support.microsoft.com/en-us/lifecycle/search).

RELATED DOCUMENTATION

Prerequisites for Upgrading WinCollect Agents | 23

Communication Between WinCollect Agents and JSA | 15

Prerequisites for Upgrading WinCollect Agents

IN THIS SECTION

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

WinCollect and JSA Software Versions

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

Table 8: Software Version Matrix

JSA Version	Minimum WinCollect Version	RPM Minimum Version
2014.8	WinCollect 7.2.2 - Patch 2	AGENT-WINCOLLECT-7.2 -1018607.noarch
JSA 7.3.x	WinCollect 7.2.5	AGENT-WINCOLLECT-7.3 -20161123160813.noarch
JSA	WinCollect	AGENT-WINCOLLECT-7.3 -20161123160813.noarch

Checking the Installed Version Of the WinCollect Agent

You can check the version of the installed WinCollect agent by performing the following steps:

1. In JSA, select **Help** >**About**

2. Select the **Additional Release Information** link.

3. If you want to verify the WinCollect agent release, use ssh to log in to the JSA Console as the root user, and run the following command:

   ```
   yum list all | grep -i AGENT-WINCOLLECT
   ```

RELATED DOCUMENTATION

Communication Between WinCollect Agents and JSA | **15**

Hardware and Software Requirements for the WinCollect Host | **18**

4

CHAPTER

WinCollect installations

WinCollect installations

IN THIS SECTION

You install WinCollect agents in an environment that is managed by JSA, as a stand-alone agent, or a combination of both.

Managed WinCollect Installations

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

NOTE: WinCollect does not support cloning virtual machines (VMs) that have agents installed that are registered in JSA.

RELATED DOCUMENTATION

Installing and Upgrading the WinCollect Application on JSA Appliances | 27

Creating an Authentication Token for WinCollect Agents | 30

Installing the WinCollect Agent on a Windows Host | 40

Installing and Upgrading the WinCollect Application on JSA Appliances

To manage a deployment of WinCollect agents from the JSA user interface, you must first upgrade your JSA Console to a supported version of WinCollect by using the WinCollect Agent SFS Bundle. This bundle includes the required protocols to enable communication between JSA and the managed WinCollect agents on the Windows hosts. Both the JSA Console and managed WinCollect agents can be upgraded to newer versions of WinCollect by installing the newer version of SFS Bundle on the JSA console.

NOTE:

- For information about upgrading WinCollect versions v7.0 through v7.1.0, see https://support.juniper.net/support/downloads/.

- If WinCollect 7.2.6 or later is installed on the JSA Console, and then you upgrade JSA from 2014.8 to 7.3.0 or later, the version of WinCollect on JSA reverts to 7.2.5. The managed WinCollect agents that are running on your Windows hosts remain at their current version and continue to send events to JSA using their existing configuration information. However, they no longer receive code or configuration updates. You must reinstall a version of the WinCollect Agent SFS Bundle that is the same as or newer than your current agents' version on your JSA Console after the JSA upgrade.

After you upgrade a JSA Console, the managed WinCollect agents that are enabled to receive automatic updates automatically upgrade to the new version of WinCollect at the next configuration polling interval. If new WinCollect agent files are available for download, the agent downloads, 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 on the Windows host restarts.

NOTE: If you reinstall JSA on your Console, you must delete this file on any existing WinCollect agent installations before WinCollect can function properly: **Program Files/IBM/WinCollect/config/ConfigurationServer.PEM**

1. Download the WinCollect Agent SFS bundle installation file from https://support.juniper.net/support/downloads/.

> **NOTE**: The installation process restarts services on the Console, which creates a gap in event collection until services restart. Schedule the WinCollect upgrade during a maintenance window to avoid disrupting users.

2. Use SSH to log in to the JSA Console as the root user.

3. For initial installations, create the **/storetmp** and **/media/updates** directories if they do not exist. Type the following commands:

   ```
   mkdir /media/updates

   mkdir /storetmp
   ```

4. Using a program such as WinSCP, copy the downloaded SFS file to **/storetmp** on your JSA console.

5. To change to the /storetmp directory, type the following command:

   ```
   cd /storetmp
   ```

6. To mount the SFS file, type the following command:

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

   Example:

   ```
   mount -t squashfs -o loop 730_QRadar_wincollectupdate-7.3.0-24.sfs /media/updates
   ```

7. To run the WinCollect installer, type the following command and then follow the prompts: **/media/updates/installer**

> **NOTE**: To proceed with the WinCollect Agent update you must restart services on JSA to apply protocol updates. The following message is displayed:
>
> ```
> WARNING: Services need to be shutdown in order to apply patches.
>
> This will cause an interruption to data collection and correlation.
>
> Do you wish to continue (Y/N)?
> ```

8. Type Y to continue with the update.

   During the update, the SFS installs new protocol updates. If your Secure Shell (SSH) session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and run the installer again, the patch installation resumes. After the installation is complete, services are restarted, and the user interface is available.

> **NOTE**: During installation, the following message is displayed:

```
Patch 144249

This patch includes a new version of the WinCollect Configuration Server.

For this new version to run properly, the event collection service needs to be restarted.

If you choose to not restart the service, agents cannot get new configurations and code
updates until you restart it.

Choices:

a. Restart event collection service at the end of the patch installation, on the Console and
   on all managed hosts patched from the Console.

b. Do not restart event collection service yet. You will need to restart it in the user interface
   (Advanced > Restart Event Collection Services).

c. Abort patch.
```

After you choose an option, the patch installation continues. When it is complete, press the Enter key to exit the patch screen.

9. If you selected the second option in step 8, you must perform the following steps:
   - In the JSA admin settings, click **Advanced**>**Deploy Full Configuration**.
   - In the JSA admin settings, click **Advanced**>**Restart Event Collection Services**.
10. To unmount the SFS file from the Console, type the following command: `umount /media/updates`
11. Verify that WinCollect agents are configured to accept remote updates:
    a. Log in to JSA.

    b. On the navigation menu, click **Data Sources**.

    c. Click the WinCollect icon.

    d. Review the **Automatic Updates Enabled** column and select Wincollect agents that have a **False** value.

    e. Click **Enable/Disable Automatic Updates**.

Managed WinCollect agents with automatic updates enabled are updated and restarted. The amount of time it takes a managed agent to update depends on the configuration polling interval for the WinCollect and the speed of the network connections between the Console and the agent.

RELATED DOCUMENTATION

Creating an Authentication Token for WinCollect Agents | 30
Installing the WinCollect Agent on a Windows Host | 40
Installing a WinCollect Agent from the Command Prompt | 44

Creating an Authentication Token for WinCollect Agents

Third-party or external applications that interact with JSA require an authentication token. Before you install managed 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 managed WinCollect agents to exchange data with JSA appliances. Create one authentication token to use for all of your WinCollect agents that communicate events with JSA host. If the authentication token expires, the WinCollect agent cannot receive log source configuration changes or code updates.

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 9: Add Authorized Services Parameters

Parameter	Description
Service Name	The name can be up to 255 characters in length, for example, **WinCollect Agent**.
User Role	Select **WinCollect**. For more information about user roles, see the *Juniper Secure Analytics Administration Guide*.
Expiry	Select **No Expiry**.

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

RELATED DOCUMENTATION

Installing the WinCollect Agent on a Windows Host | 40

Installing a WinCollect Agent from the Command Prompt | 44

Uninstalling a WinCollect Agent from the Command Prompt | 51

Adding Multiple Destinations to WinCollect Agents

You must create the destinations that you want to add to the WinCollect agent. See "Adding a Destination" on page 58.

In a managed WinCollect deployment, add JSA appliances as destinations for Windows events if a JSA appliance fails.

Each destination that you create for a WinCollect agent has its own disk cache for events. If Site A fails and Site B is configured as the Target External Destination, Site B continues to receive events and Site A stores events to disk. If both sites fail, both systems are caching events independently to separate disk queues. As connections return for individual log sources, the agents attempt to balance sending new events and cached events that are queued due to either bursting events, or connection issues.

If your deployment contains many log sources by using multiple destinations, increase the default disk space. Each agent is configured with 6 GB of disk space to cache events. However, if there are 50 log sources or more, each sending to multiple destinations, and a network segment fails, each log source writes two sets of events to the same cache on the Target Internal and the Target External destination. If your deployment contains segments that are unstable or a prone to outages, update the default storage capacity of the agent in the event of a long term outage.

1. In JSA, click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **WinCollect** icon.
4. Click **Agents** and select the agent that you want to edit.
5. Click **Log Sources**.
6. Select the log source that you want to edit, and click **Edit**.
7. Select the **Target External Destinations** check box.

8. Select the destinations that you want to add to the agent from the box below the **Target External Destinations** check box.
9. Click **Save**.

RELATED DOCUMENTATION

Migrating from Adaptive Log Exporter to WinCollect | 39

Uninstalling a WinCollect Agent from the Command Prompt | 51

Uninstalling a WinCollect Agent from the Control Panel | 52

Migrating WinCollect Agents After a JSA Hardware Upgrade

Migrating WinCollect agents after a JSA hardware upgrade After a JSA hardware upgrade, you need to generate a new authorization token for your WinCollect agents and update their `install_config` files.

1. Generate an authentication token. For more information, see "Creating an Authentication Token for WinCollect Agents" on page 30.
2. Update the **\WinCollect\config\install_config.txt** file with the IP address of your new Console.
3. Run the following command, where *<auth_token>* is the authentication token that you generated in 1.

   ```
   C:\Program Files\IBM\WinCollect\bin\InstallHelper.exe -T <auth_token> -a "C:\Program Files\IBM\WinCollect
   \config\install_config_autocreate.txt" C:\Program Files\IBM\WinCollect\ bin\InstallHelper.exe -T xxxxxxxx-
   xxxx-xxxx-xxxx-xxxxxxxxxxxx -a "C:\Program Files\IBM\WinCollect\config\install_config_autocreate.txt”
   ```
4. Restart the WinCollect agent.

RELATED DOCUMENTATION

Uninstalling a WinCollect Agent from the Command Prompt | 51

Uninstalling a WinCollect Agent from the Control Panel | 52

Adding Multiple Destinations to WinCollect Agents | 31

Stand-alone WinCollect Installations

A stand-alone deployment is a Windows host in unmanaged mode with WinCollect software installed. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to JSA.

WinCollect Configuration Console Overview

In stand-alone deployments, use the WinCollect Configuration Console to manage your WinCollect deployment. Use the WinCollect Configuration Console to add devices that you want WinCollect to collect agents from, and add the JSA destination where you want to send events.

Prerequisites:

Before you can install the WinCollect Collect Configuration Console, you must do the following:

- Install the WinCollect agent in stand-alone mode. For more information, see "Installing the WinCollect Agent on a Windows Host" on page 40.
- Install .net framework version 3.5
- Install Microsoft Management Console (MMC) 3.0 and later.

The following table describes the WinCollect Configuration Console.

Table 10: WinCollect Configuration Console Window

Sections	Description
Global Configuration	The Global Configuration parameter allows you to view, add and update information about the system where WinCollect data is stored.

Table 10: WinCollect Configuration Console Window *(Continued)*

Sections	Description
	Disk Manager— the path to the WinCollect Data, which is used to buffer events to disk when the event rate exceeds the event throttle. **Capacity** is the maximum capacity allowed for the contents of the Data Folder. WinCollect does not write to this folder after the maximum capacity is reached.
	Installation Information— displays information about the WinCollect agent installation. **Application Identifier**— the header of the payload messages sent to the status server. **Status Server**— where the WinCollect Agent status events, such as heart beat messages and any warnings or errors generated by the WinCollect Agent, are sent.
	Security Manager— centralized credentials, used to collect events from remote devices.
Destinations	The **Destinations** parameter defines where WinCollect device data is sent.
	Syslog TCP or **Syslog UDP** destinations include the following parameters: **Name** **Hostname** **Port** **Throttle (events per second)** You can expand a destination to view all devices that are assigned to the destination.

Table 10: WinCollect Configuration Console Window *(Continued)*

Sections	Description
Devices	The **Device** parameter contains available device types. Under each device types, you can view or update multiple device parameters.

RELATED DOCUMENTATION

Installing the Configuration Console | 35

Silently Installing, Upgrading, and Uninstalling WinCollect Software | 36

Creating a WinCollect Credential | 64

Installing the Configuration Console

- The existing WinCollect agent must be in stand-alone mode before you can install the configuration console. For more information about WinCollect agent installations, see "Installing a WinCollect Agent from the Command Prompt" on page 44.
- .NET framework 3.5 features are required.
- Microsoft Management Console (MMC) 3.0 and later is required.
- The WinCollect Stand-alone patch installer supports the following Windows software versions:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 (most recent)
  - Windows 10 (most recent)
  - Windows 8 (most recent)
  - Windows Vista (most recent)

NOTE: WinCollect is not supported on versions of Windows that have been moved to End Of Life by Microsoft. After software is beyond the Extended Support End Date the product might still function as expected, however, Juniper Networks will not make code or vulnerability fixes to resolve WinCollect issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the 'Extended Support End Date'. Any questions about this announcement can be discussed in the JSA Collecting Windows Events (WMI/ALE/WinCollect) forum. For more information, see https://support.microsoft.com/en-us/lifecycle/search (https://support.microsoft.com/en-us/lifecycle/search).

Download and install the WinCollect configuration console to manage your stand-alone deployment. You can choose an option to install just the WinCollect patch, if you are deploying WinCollect on a large number of Windows hosts that do not require the configuration console.

1. Download the patch software from https://support.juniper.net/support/downloads/ onto the Windows host where you want to install the configuration console.
2. Open the executable file on your system.
3. Follow the steps in the installation wizard. You can select an option to install both the WinCollect configuration console, and the WinCollect patch, or just the patch.

RELATED DOCUMENTATION

Silently Installing, Upgrading, and Uninstalling WinCollect Software | 36

Creating a WinCollect Credential | 64

Adding a Destination to the WinCollect Configuration Console | 65

Silently Installing, Upgrading, and Uninstalling WinCollect Software

Enter a command to complete all installation and upgrading tasks for the WinCollect stand alone patch, and the WinCollect Configuration Console, rather than using the installation wizard. You can also upgrade WinCollect agents by using the agent installer only.

1. Download the patch software from https://support.juniper.net/support/downloads/

2. Install or upgrade both the WinCollect stand alone patch and the WinCollect Configuration Console by using the following commands:

   <setup.exe> /s /v" /qn"

3. Change the installation directory of the WinCollect Configuration Console by using the following command:

   <setup.exe> /s /v" /qn ADDLOCAL=ALL INSTALLDIR=*<PATH>*"

4. Install or upgrade only the WinCollect stand-alone patch by using the following command:

   <setup.exe> /s /v" /qn ADDLOCAL=WinCollect_StandAlone_Patch"

5. If you want to uninstall the WinCollect Configuration Console, use the following command:

   <setup.exe> /s /x /v" /qn"

   For more information about stand-alone installs, see Juniper Customer Support.

RELATED DOCUMENTATION

Creating a WinCollect Credential | 64

Adding a Destination to the WinCollect Configuration Console | 65

Configuring a Destination with TLS in the WinCollect Configuration Console | 66

Setting an XPath Parameter During Automated Installation

In WinCollect 7.2.8 and later, you can add an XPath parameter to your command line installer for stand-alone WinCollect agent installations.

1. Convert your XPath to base64 encoding using https://www.base64encode.org/ or another encoding tool. For example, this XPath, needed to collect Windows PowerShell logs:

```
<QueryList>

<Query Id="0" Path="Windows PowerShell*>

<Select Path="Windows PowerShell">*</Select>

<Query>

<QueryList>
```

   results in this base64 conversion:

```
PFF1ZXJ5TGlzdD4KPFF1ZXJ5IElkPSIwIiBQYXRoP SJXaW5kb3dzIFBvd2VyU2hlbGwiPgo8U2Vs
ZWN0IFBhdGg9IldpbmRvd3MgUG93ZXJTaGVsbCI+Kjwv U2VsZWN0Pgo8L1F1ZXJ5Pgo8L1F1ZXJ5 TGlzdD4=
```

2. Add the following code to your command line installer:

   ```
   c:\wincollect-7.2.8 -91.exe /s /v"/qn STATUSSERVER=<valid IP address>LOG_SOURCE_AUTO_CREATIONENABLED=True

   LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice=DeviceWindowsLog&Component Action=create&

   Component1.LogSourceName=%COMPUTERNAME%&Component1. LogSourceIdentifier=%COMPUTERNAME
   %&Component1.Dest.Name=QRadar&Component1 .EventLogPollProtocol=MSEVEN6&Component1.Dest.Hostname=<valid IP
   address>&

   Component1.Dest.Port=514&Component1.Dest.Protocol=TCP&Component1 .Log.Security=true&Component1 .Log.System=tru
   e&

   Component1.Log.Application=true&Component1.Log.DNS+Server=false&Component1. Log.File+Replication
   +Service=false&

   Component1.Log.Directory+Service=false&Component1.RemoteMachinePollInterval=3000&

   Component1.MinLogsToProcessPerPass=1250&Component1. MaxLogsToProcessPerPass=2500&

   Component1.CustomQuery.Base64=<base64 Xpath>&

   Component1.EventRateTuningProfile=High+Event+Rate+Server"""
   ```

   > **NOTE**: Replace the following entries with valid IP addresses:
   >
   > `STATUSSERVER=`*<valid IP address>*
   >
   > Component1.Dest.Hostname=*<valid IP address>*

   `STATUSSERVER` is the location where the WinCollect agent sends status messages (such as WinCollect service starting or any agent error messages). `Component1.Dest.Hostname` is the location where the agent sends event logs (such as JSA EC or Console).

   > **NOTE**: Replace the following entry with the base64 conversion you created in 1:
   >
   > `Component1.CustomQuery.Base64=`*`<base64 Xpath>`*

3. Add or remove any of the Components or event logs you want to collect.

Migrating from Adaptive Log Exporter to WinCollect

To migrate from Adaptive Log Exporter (ALE) deployments to WinCollect, install the WinCollect agent, create a log source, and decommission ALE on the Windows host. The ALE product is end of life (EOL), and is no longer supported.

1. Install the WinCollect SFS on the JSA console.
2. Click the **Admin** tab.
3. From the **Data Sources**, click **Wincollect**.
4. On the **WinCollect** page, create a WinCollect destination by clicking **Destinations >Add**.
5. Install the WinCollect agent on the Windows host. For more information, see "Installing the WinCollect Agent on a Windows Host" on page 40.

   NOTE: You can create a log source from the WinCollect installation wizard.

6. Wait for the WinCollect agents to auto discover.
7. Optional. Create a WinCollect log source in JSA to replace the existing log source that is used by the Adaptive Log Exporter. For more information, see "Adding a Log Source to a WinCollect Agent" on page 131.

   NOTE: You can skip step 7 if **Create Log Source** was selected during the installation of WinCollect. Log sources that use the WinCollect protocol can be created individually or added in bulk for WinCollect agents that remotely poll for events.

8. In the **Log Activity** tab, verify that events are received.
9. Decommission the Adaptive Log Exporter:

   a. Close all active applications on the Windows host.

   b. Open the Windows command prompt.

   c. Go to the installation directory for the Adaptive Log Exporter.

      NOTE: ALE standard installation directory is the **Program Files** or **Program Files (x86)** directory.

   d. To uninstall the Adaptive Log Exporter, type the following command:

      ```
      unins000.exe /SILENT /VERYSILENT
      ```

RELATED DOCUMENTATION

Uninstalling a WinCollect Agent from the Command Prompt | 51

Uninstalling a WinCollect Agent from the Control Panel | 52

Adding Multiple Destinations to WinCollect Agents | 31

Installing the WinCollect Agent on a Windows Host

Install the WinCollect agent on each Windows host that you want to use for local or remote collection in your network environment.

Ensure that the following conditions are met:

- You created an authentication token for the managed WinCollect agent.

  > **NOTE**: This authentication token is required for every managed WinCollect agent you install.

  For more information, see "Creating an Authentication Token for WinCollect Agents" on page 30.

- Your system meets the hardware and software requirements.

  For more information, see "Hardware and Software Requirements for the WinCollect Host" on page 18.

- The required ports are available for WinCollect agents to communicate with JSA and remotely polled Windows computers.

  For more information, see "Communication Between WinCollect Agents and JSA" on page 15.

- To automatically create a log source for a managed WinCollect agent, you must first create a destination that your agent can use to connect to JSA and create your log source.

  The managed WinCollect agent sends the Windows event logs to the configured destination. The destination can be the JSA Console, an Event Processor, or an Event Collector.

1. Download the WinCollect Agent `.exe` file from https://support.juniper.net/support/downloads/.
2. Right-click the WinCollect Agent `.exe` file and select **Run as administrator**.
3. Follow the prompts in the installation wizard and use the following parameters for either managed or stand-alone agent setup.

Table 11: WinCollect Managed Agent Setup Type Installation Wizard Parameters

Parameter	Description
Host Identifier	Use a unique identifier for each WinCollect agent that you install. The name that you type in this field is displayed in the WinCollect agent list of the JSA Console. If you are reinstalling an agent on a Windows host and you want to use the same Host Identifier for the agent, you must first rename the existing agent in JSA. Host identifiers are unique to each installation of the agent on the same Windows host. By default, the Host Identifier is the hostname of the Windows host.
Authentication Token	The authentication token that you created in JSA, for example, **af111ff6-4f30-11eb-11fb-1fc117711111**.
Configuration Server (host and port)	The IP address or host name of your JSA Console, Event Collector, or Event Processor. For example, **192.0.2.0** or **myhost**.
Create Log Source	If this check box is selected, you must provide information about the log source and the target destination.
Log Source Name	The name can be a maximum of 255 characters.
Log Source Identifier	Identifies the device that the WinCollect agent polls. This field must use the hostname, IP address, or FQDN of the Windows host that the log source gathers events from.
Target Destination	The WinCollect destination must be configured in JSA before you continue entering information in the installation wizard. This field must contain the name of a previously created WinCollect Destination as it appears in the **Destinations** window.
Event Logs	The Window logs that you want the log source to collect events from and send to JSA.
Machine poll interval (msec)	The polling interval that determines the number of milliseconds between queries to the Windows host. The minimum polling interval is 300 milliseconds. The default is 3000 milliseconds or 3 seconds.

Table 11: WinCollect Managed Agent Setup Type Installation Wizard Parameters *(Continued)*

Parameter	Description
Event Rate Tuning Profile	Select the tuning profile: - Default (Endpoint): 100/150 This setting is suitable for Windows endpoints that are running a non-Server OS. - Typical Server: 500/750 This setting is suitable for most Windows Server endpoints. - High Event Rate Server: 1250/1875 This setting is suitable for all Windows endpoints and is ideal for Domain Controllers and other potentially high EPS endpoints.
Default Status Server Address	An alternative destination to send WinCollect status messages to, such as the heartbeat, if required. Set the value to an IP address to send status messages to any JSA Console or any Event Processor or Event Collector in your deployment. Set the value to Disabled to send only a heartbeat without status messages. Set the value to None if you don't want to send a heartbeat or status messages.
Syslog Status Server (if different from default)	An alternative destination to send WinCollect status messages to, such as the heartbeat, if required. Set the value to an IP address to send status messages to any JSA Console or any Event Processor or Event Collector in your deployment. Set the value to **Disabled** to send only a heartbeat without status messages. Set the value to **None** if you don't want to send a heartbeat or status messages.

Table 12: WinCollect Stand Alone Setup Type Installation Wizard Parameters

Parameter	Description
Create Log Source	If this check box is selected, you must provide information about the log source and the target destination.
Log Source Name	The name can be a maximum length of 255 characters.

Table 12: WinCollect Stand Alone Setup Type Installation Wizard Parameters *(Continued)*

Parameter	Description
Log Source Identifier	Identifies the device that the WinCollect agent polls. This field must use the hostname, IP address, or FQDN of the Windows host that the log source gathers events from.
Event Logs	The Window logs that you want the log source to collect events from and send to JSA.
Destination Name	Identifies where Wincollect events are sent.
Hostname / IP	The host name or IP address for the destination.
Port	The port that WinCollect uses when it communicates with the destination.
Protocol	**TCP** or **UDP**
Machine poll interval (msec)	The polling interval that determines the number of milliseconds between queries to the Windows host. The minimum polling interval is 300 milliseconds. The default is 3000 milliseconds or 3 seconds.
Event Rate Tuning Profile	Select the tuning profile: • Default (Endpoint): 100/150 This setting is suitable for Windows endpoints that are running a non-Server OS. • Typical Server: 500/750 This setting is suitable for most Windows Server endpoints. • High Event Rate Server: 1250/1875 This setting is suitable for all Windows endpoints and is ideal for Domain Controllers and other potentially high EPS endpoints.

Table 12: WinCollect Stand Alone Setup Type Installation Wizard Parameters *(Continued)*

Parameter	Description
Default Status Server Address	The IP address Destination where status messages from the WinCollect agent are sent.
Syslog Status Server (if different from default)	An alternative destination to send WinCollect status messages to, such as the heartbeat, if required. Set the value to an IP address to send status messages to any JSA Console or any Event Processor or Event Collector in your deployment. Set the value to **Disabled** to send only a heartbeat without status messages. Set the value to **None** if you don't want to send a heartbeat or status messages.
Heartbeat Interval (msecs)	The frequency that heartbeat status messages are sent. In WinCollect 7.2.8, it is displayed in milliseconds. In WinCollect 7.2.9 and later, it is displayed in minutes.
Log Monitor Socket Type	Protocol to be used to send heartbeat and status messages. **NOTE**: This option is only available in stand-alone WinCollect deployments. Availability for managed agents is planned in a later release of JSA.

The **Command Line (will be saved in config\cmdLine.txt)** field displays a command line from the configuration that you completed. You can use this command for silent, or unattended installations. For more information, see "Installing a WinCollect Agent from the Command Prompt" on page 44.

RELATED DOCUMENTATION

Installing a WinCollect Agent from the Command Prompt | 44

Uninstalling a WinCollect Agent from the Command Prompt | 51

Uninstalling a WinCollect Agent from the Control Panel | 52

Installing a WinCollect Agent from the Command Prompt

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

The WinCollect installer uses the following command options:

Table 13: Silent Installation Options for WinCollect Agents

Option	Valid entries and description
/qn	Runs the WinCollect agent installation in silent mode.
INSTALLDIR	The installation location for WinCollect. If the installation directory contains spaces, add a backslash before the quotation marks.
AUTHTOKEN=token	For managed WinCollect agents only. Uses the previously configured Authorization Token from JSA to authorize the managed agent. For example, `AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1f c1 17711111`
FULLCONSOLEADDRESS=host_address	The IP address, host name, or FQDN of the JSA Console, Event processor, or Event Collector that manages the agent. Examples: • `FULLCONSOLEADDRESS=192.0.2.0` • `FULLCONSOLEADDRESS=EPqradar` • `FULLCONSOLEADDRESS=EPqradar.myhost. com`
HOSTNAME=host name	The **Hostname** field is used to assign a name to the WinCollect agent. The values that are used in this field can be an identifiable name, hostname, or IP address. In most cases, administrators can use HOSTNAME=%COMPUTERNAME% to auto populate this field. The IP address or host name of the WinCollect agent host cannot contain the "at" sign, @.

Table 13: Silent Installation Options for WinCollect Agents *(Continued)*

Option	Valid entries and description
STATUSSERVER	An alternative destination to send WinCollect status messages to, such as the heartbeat, if required. Set the value to an IP address to send status messages to any JSA Console or any Event Processor or Event Collector in your deployment. Set the value to Disabled to send only a heartbeat without status messages. Set the value to None if you don't want to send a heartbeat or status messages.
LOG_SOURCE_AUTO_CREATION_ENABLED	Required, **True** or **False** If you enable this option, you must configure the log source parameters. JSA must be updated to 2014.1.r1.734536 or later.
LOG_SOURCE_AUTO_CREATION_ PARAMETERS	Ensure that each parameter uses the format: `Parameter_Name=value`. The parameters are separated with ampersands, &. Your JSA must be updated to 2014.1.r1.734536 or later.
LOG_MONITOR_SOCKET_TYPE=TCP	This parameter sets the protocol that is used by heartbeat and status messages to be sent by using TCP. The default protocol is UDP. **NOTE**: This option is only available in stand-alone WinCollect deployments. Availability for managed agents is planned in a later release of JSA.
Component1.Action	`create` Creates a new windows event log source during the installation.
Component1.LogSourceIdentifier	The IP address or host name of the system where the agent is installed.

Table 13: Silent Installation Options for WinCollect Agents *(Continued)*

Option	Valid entries and description
Component1.Destination.Name	The destination name is an alphanumeric value that is used to specify where a WinCollect log source sends event data. This value must be a JSA appliance capable of receiving event data, such as an Event Processor, Event Collector, or JSA Console. **NOTE**: In managed deployments, the destination must be an "internal destination", and the name must exist in the JSA user interface before the installation, otherwise the log source configuration parameters are discarded and no log sources are automatically created. **Internal Destination** - Managed hosts with an event processor component **External Destination** - Destination that you configured as the WinCollect destination and is not known to the Console as a Managed Host
Component1.Dest.Hostname (Stand alone deployments only)	The IP address or host name where you send WinCollect events.
Component1.Dest.Port (Stand alone deployments only)	The port that WinCollect uses when it communicates with the destination.
Component1.Dest.Protocol (Stand alone deployments only)	**TCP** or **UDP**
Component1.Dest.MaxPayloadSize (Stand alone deployments only)	Maximum payload size sent to the destination (Default values are 1020 UDP and 32000 TCP).
Component1.Log.Security	Required, **True** or **False** The Windows Security log contains events that are defined in the audit policies for the object.

Table 13: Silent Installation Options for WinCollect Agents *(Continued)*

Option	Valid entries and description
Component1.Log.System	Required, **True** or **False** The Windows System logs can contain information about device changes, device drivers, system changes, events, and operations provided by the operating system.
Component1.Log.Application	Required, **True** or **False** The Windows Application logs contain events that are triggered by software applications instead of the operating system. The logs can contain errors, information, and warning events.
Component1.Log.DNS+Server	Required, **True** or **False** The Windows DNS Server log contains DNS events.
Component1.Log.File+Replication+Service	Required, **True** or **False** The Windows File Replication Service log contains events about changed files that are replicated on the system.
Component1.Log.Directory+Service	Required, **True** or **False** The Windows Directory Service log contains events that are written by the active directory.
Component1.RemoteMachinePollInterval	The polling interval that determines the number of milliseconds between queries to the Windows host. The minimum polling interval is 300 milliseconds. The default is 3000 milliseconds or 3 seconds.

Table 13: Silent Installation Options for WinCollect Agents *(Continued)*

Option	Valid entries and description
Component1.EventRateTuningProfile (Managed deployments only)	Select one of the following tuning profiles: • Default+(Endpoint) • Typical+Server • High+Event+Rate+Server
Component1.MaxLogsToProcessPerPass (Stand alone deployments only)	Not required. The maximum number of logs (in binary form) that the algorithm attempts to acquire in one pass, if remaining retrievable events exist. **NOTE**: Use this parameter to improve performance for event collection, however, this parameter can also increase processor usage.
Component1.MinLogsToProcessPerPass (Stand alone deployments only)	Not required. The minimum number of logs (in binary form) that the algorithm attempts to read in one pass, if remaining retrievable events exist. **NOTE**: You can use this parameter to improve performance for event collection, but this parameter can also increase processor usage.
Component1.StoreEventPayload	Not required. Specifies that JSA event payloads are to be stored.
Component1.Secondary	Not required. Specifies the IP address or Hostname of the Secondary destination that the Agent sends events to if the Primary destination is unreachable and the failover time has elapsed.

Table 13: Silent Installation Options for WinCollect Agents *(Continued)*

Option	Valid entries and description
Component1.Failover	Not required. Specifies the failover time in seconds. If the primary destination can't be reached, the Agent starts sending events to the Secondary destination.

> **NOTE**: You need to run the command prompt as an administrative user.

1. Download the WinCollect agent setup file from https://support.juniper.net/support/downloads/
2. On the Windows host, open a command prompt by using **Run as Administrator**.

   > **NOTE**: In managed deployments, the destination name that is used during automatic log source creation must exist before the command-line installation runs. Verify the destination name in the JSA user interface before you start the installation.

3. Type the following command:

   ```
   wincollect-<Version_number>.x64.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 a silent installation for a Stand alone WinCollect agent.

   > **NOTE**: This example contains line breaks for formatting. The actual command is a single line.

   ```
   wincollect-<version_number>.x86.exe /s /v"/qn INSTALLDIR=\"C:\Program Files \IBM\WinCollect\"
   HEARTBEAT_INTERVAL=6000 LOG_SOURCE_AUTO_CREATION_ENABLED= True
   LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice=
   DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=
   %COMPUTERNAME%-1&Component1.LogSourceIdentifier=
   <ip_address>&Component1.Dest.Name=QRadar&Component1 .Dest.Hostname=<ip_address>&Com
   ponent1.Dest.Port=
   514&Component1.Dest.Protocol=TCP&Component1.Log.Security=true&Component1 .Log.System=t
   rue&Component1.Log.Application=true &Component1.Log.DNS+Server=false&Component1.Log.File
   ```

```
+Replication+ Service=false&Component1.Log.Directory+Service=false&Component1.
RemoteMachinePollInterval=3000&Component1.EventRateTuningProfile=High+ Event+Rate
+Server&Component1.MinLogs
ToProcessPerPass=1250&Component1.MaxLogsToProcessPerPass=1875
```

The following example shows a silent installation for a managed WinCollect agent.

> **NOTE**: This example contains line breaks for formatting. The actual command is a single line.

```
wincollect-<version_number>.x86.exe /s /v"/qn INSTALLDIR=\"C:\Program Files \IBM\WinCollect\"
AUTHTOKEN=1111111-aaaa-1111-aaaa-11111111 FULLCONSOLEADDRESS=<ip_address:port>
HOSTNAME=%COMPUTERNAME% LOG_SOURCE_AUTO_CREATION_ENABLED=True
LOG_SOURCE_AUTO_CREATION_PARAMETERS
=""Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create
&Component1.LogSourceName=%COMPUTERNAME%&Component1.LogSourceIdentifier=
%COMPUTERNAME%&Component1.Log.Security=true&Component1.Log.System=false
&Component1.Log.Application=false&Component1.Log.DNS+Server=false &Component1.Log.File
+Replication+Service=false&Component1.Log. Directory
+Service=false&Component1.Destination.Name=Local&
Component1.RemoteMachinePollInterval=3000&Component1.EventRate TuningProfile=High+Event
+Rate+Server"""
```

4. Press Enter.

RELATED DOCUMENTATION

Uninstalling a WinCollect Agent from the Command Prompt | 51

Uninstalling a WinCollect Agent from the Control Panel | 52

Adding Multiple Destinations to WinCollect Agents | 31

Uninstalling a WinCollect Agent from the Command Prompt

You can uninstall the WinCollect agent from the command prompt.

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

NOTE: You need to run the command prompt as an administrative user.

2. If you want to remove all files, type the following command:

   msiexec /x{1E933549-2407-4A06-8EC5-83313513AE4B} REMOVE_ALL_FILES=True /qn

3. If you want to remove just the WinCollect application, and not configuration files, stored events, and bookmarks, type the following command:

   msiexec /x{1E933549-2407-4A06-8EC5-83313513AE4B} REMOVE_ALL_FILES=False /qn

4. Press Enter.

RELATED DOCUMENTATION

Uninstalling a WinCollect Agent from the Control Panel | **52**

Adding Multiple Destinations to WinCollect Agents | **31**

Migrating from Adaptive Log Exporter to WinCollect | **39**

Uninstalling a WinCollect Agent from the Control Panel

You can uninstall the WinCollect agent from the Microsoft Windows Control Panel.

1. Click **Control Panel** >**Programs** >**Uninstall a program**.

NOTE: You need to start the control panel as an administrative user.

2. Highlight WinCollect in the program list, and click **Uninstall**.
3. If prompted by Windows, confirm that you want to remove WinCollect.

RELATED DOCUMENTATION

Adding Multiple Destinations to WinCollect Agents | **31**

Migrating from Adaptive Log Exporter to WinCollect | **39**

Uninstalling a WinCollect Agent from the Command Prompt | **51**

5

CHAPTER

Configuring WinCollect Agents After Installation

Configuring WinCollect Agents After Installation

IN THIS SECTION

In managed WinCollect deployments, you can use JSA for many agent configuration tasks. In stand-alone deployments, use the WinCollect Configuration Console to manage your WinCollect deployment.

Some WinCollect agent configurations must be performed on the Windows host where the agent is installed.

Configuring Managed WinCollect Agents

After you install a managed WinCollect deployment, you manage your deployment by using JSA.

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 JSA by using syslog.

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

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

RELATED DOCUMENTATION

Manually Adding a WinCollect Agent | 56

Deleting a WinCollect Agent | 57

WinCollect Destinations | 58

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 JSA 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 JSA, 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.

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 14: 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.

Table 14: WinCollect Agent Parameters *(Continued)*

Parameter	Description
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 Status Server. The interval ranges from 1 - 20 minutes.
Configuration Poll Interval	Defines how often the WinCollect agent polls the JSA Configuration server for updated log source configuration information or agent software updates. The interval ranges from 1 minute to 20 minutes.
Maximum TCP/UDP Payload	The WinCollect agent uses whatever setting is selected in JSA for the maximum TCP/UDP payload size.

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

   The WinCollect agent is added to the agent list.

RELATED DOCUMENTATION

Deleting a WinCollect Agent | 57

WinCollect Destinations | 58

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials | 76

Deleting a WinCollect Agent

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

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 DOCUMENTATION

WinCollect Destinations | 58

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials | 76

WinCollect Log File | 143

WinCollect Destinations

IN THIS SECTION

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

Adding a Destination

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

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 15: Destination Parameters

Parameter	Description
Name	Used on the agent side for log source creation. **NOTE**: The destination name is used during automatic log source creation and must exist before the installation runs. Verify the destination name in JSA before starting the installation.
Hostname	The host name or IP address of the destination JSA appliance.
Port	JSA receives events from WinCollect agents on either UDP or TCP port 514. For TLS protocol, the default port is 6514.
Protocol	The communication channel between JSA and WinCollect agents. Select **UDP**, or **TCP**, or **TCP/TLS (Encrypted)**.
Certificate	The TLS certificate of the destination device. Copy the certificate from **/opt/qradar/conf/trusted_certificates/syslog-tls.cert** on the destination device and paste in the **Certificate** field. **NOTE**: The **Certificate** field displays when **TCP/TLS (Encrypted)** is selected from the **Protocol** list.
Throttle (events per second)	Defines a limit to the number of events that the WinCollect agent can send each second.

Table 15: Destination Parameters *(Continued)*

Parameter	Description
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**.

Adding a Secondary Destination

You can add a secondary destination to receive events from your WinCollect agents if the primary destination fails.

NOTE: Adding a secondary destination is available in JSA 7.4.3 and later.

Use the following procedure to add a JSA host as a secondary destination to an existing primary destination. For more information about adding a secondary destination during the installation process, see "Adding a Destination" on page 58.

NOTE: To specify a secondary destination, you must select **TCP**.

1. Click the **Admin** tab.

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

3. Click **WinCollect** > **Destinations**.

4. 4. Select a destination and click **Edit**.

5. Select the TCP **Protocol**.

6. Enter the hostname or IP address of the JSA appliance you want to use as a **Secondary Destination**.

7. In the **Secondary Failover (seconds)** field, enter the number of seconds that the primary destination must be unreachable before the agent begins sending events to the secondary destination.

8. 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.

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.

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**.

RELATED DOCUMENTATION

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials | **76**

WinCollect Log File | **143**

Adding Custom Entries to WinCollect Status Messages | **62**

Adding Custom Entries to WinCollect Status Messages

You can add custom information to the WinCollect Agent status messages.

1. In the **wincollect/config** directory of the Windows host that you want to identify in LEEF logs, create a file that is called **heartbeat_custom.props**.

   > **NOTE**: You can create, update, or delete this file while your WinCollect deployment is running. Updates to the file are available in logs on the next heartbeat.

2. Enter the custom information in the **heartbeat_custom.props** file in the following format, with one entry on each line:

   keyword=value

   > **NOTE**:

- The **heartbeat_custom.props** must not exceed 10 KB.
- Custom keyword entries must be alpha-numeric and contain no spaces.
- Custom entries can't contain reserved keywords, such as **src, os, dst, sev, log, msg**.
- Custom values can't contain special characters, such as **= | [ ] { } < > / \ ' "**.
- Multiple white spaces in custom values are reduced to a single space.

RELATED DOCUMENTATION

WinCollect Destinations | **58**

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials | **76**

WinCollect Log File | **143**

Forwarding Events Identifier

If you enable a log source to collect forwarded events using Windows event subscriptions, you can specify the event source displayed for each event. Configure the Forwarded Events Identifier in the log source that collects forwarded events.

There are 3 options for setting the Forwarded Events Identifier:

Source

This is the default option. Forwarded events are identified by the IP address of the computer that generated the events.

WEC

Forwarded events are identified by the name of the WinCollect agent that collects them. All events collected by the Agent are grouped together with a single source identifier.

Other

You can choose a custom identifier as the source for the events. All events collected by the Agent are grouped together with this identifier.

NOTE: Custom identifiers cannot contain spaces.

RELATED DOCUMENTATION

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials | **76**

Adding Custom Entries to WinCollect Status Messages | **62**

Configuring Stand-alone WinCollect Agents with the Configuration Console

In stand-alone deployments, use the WinCollect Configuration Console to manage your WinCollect deployment.

Some WinCollect agent configurations must be performed on the Windows host where the agent is installed.

RELATED DOCUMENTATION

Creating a WinCollect Credential | **64**

Adding a Destination to the WinCollect Configuration Console | **65**

Configuring a Destination with TLS in the WinCollect Configuration Console | **66**

Creating a WinCollect Credential

Create a credential that contains login information. WinCollect uses the credential information to log into devices and collect logs.

1. Expand the **Global Configuration** parameter and right-click **Security Manager**.
2. Select **Add New Credential**.
3. In the **New Credential Name** box, add a name for the new credential and click **OK**.

4. Click the new credential under **Security Manager** to open the **Basic Configurations** window for the credential.
5. Enter the required properties for the new credential.
6. Click **Deploy Changes** under **Actions**.

RELATED DOCUMENTATION

Adding a Destination to the WinCollect Configuration Console | **65**

Configuring a Destination with TLS in the WinCollect Configuration Console | **66**

Adding a Device to the WinCollect Configuration Console | **67**

Adding a Destination to the WinCollect Configuration Console

Add an JSA instance as a destination for WinCollect data.

1. In the WinCollect Configuration Console, expand the **Destinations** parameter.
2. Right-click the **Syslog TCP** or **Syslog UDP** parameter, depending upon which destination type you want to add, and click **Add New Destination**.

> **NOTE**: If you want to specify a secondary destination, you must select the TCP **Protocol**.

3. In the **New Destination Name** box, add a name for the destination. Click **OK**.

> **NOTE**: It is helpful to provide a destination name that includes the IP address, such as "JSAEPI_198.x.x.x". If you have to edit the log source and change a destination in the future, you can determine the IP address for the destination.

4. Expand **Syslog TCP** or **Syslog UDP**, and select the destination that you added to view the **Properties** window.
5. Define the **Name**, **Hostname**, **Port**, and **Throttle** for the new destination.
6. If you have Data Sync and want to add a **Secondary Destination** to receive events if the primary destination fails, add the IP address or hostname.

7. If you added a **Secondary Destination**, enter the number of seconds that the primary destination must be unreachable before the agent begins sending events to the secondary destination in the **Secondary Failover (seconds)** field.
8. Click **Deploy Changes** under **Actions**.

> **NOTE**: Stand-alone deployments of WinCollect 7.3.0 and later support adding a secondary destination.

RELATED DOCUMENTATION

Configuring a Destination with TLS in the WinCollect Configuration Console | 66
Adding a Device to the WinCollect Configuration Console | 67
Sending Encrypted Events to JSA | 68

Configuring a Destination with TLS in the WinCollect Configuration Console

You can encrypt syslog traffic sent to a destination instance by configuring the destination with a Transport Layer Socket (TLS) or Secure Shell Layer (SSL) certificate.

1. In the WinCollect Configuration Console, expand the **Destinations** parameter.
2. Right-click the **Syslog TCP**, and click **Add New Destination**.
3. In the **New Destination Name** field, add a name for the destination, and click **OK**.

> **TIP**: Use a destination name that includes the IP address, such as "*<Managed_Host>*_1.2.3.4". If you need to edit the log source and change a destination in the future, this helps you determine the IP address for the destination.

4. Expand **Syslog TCP**, and select the destination that you added in step 3 to view the **Properties** window.
5. Define the **Name** and **Hostname**.
6. Change the **Port** to 6514, and set the **Throttle** rate.
7. Copy and paste the TLS certificate for the new destination in the **Certificate** field.

NOTE: Make sure that you include the "-----BEGIN CERTIFICATE-----" and the "-----END CERTIFICATE-----" when you copy the TLS certificate.

8. Click **Deploy Changes** under the **Actions** pane.

RELATED DOCUMENTATION

Adding a Device to the WinCollect Configuration Console | 67

Sending Encrypted Events to JSA | 68

Collecting Local Windows Logs | 70

Adding a Device to the WinCollect Configuration Console

Add the devices that WinCollect monitors to the WinCollect Configuration Console.

1. Under **Devices**, right-click the device type that matches the device you want to add and select **Add New Device**.
2. In the **Add New Device** box, enter a name for the destination device.
3. In the **Basic Configurations** window, complete the parameters for the new destination device.

   NOTE: On the Basic Configurations page of the Microsoft Windows Event log device type, you can set a global Default Event Log Poll Protocol. The default value is **MSEVEN6**.

   To configure a single Microsoft Windows Event Log device to use the global Default Event Log Poll Protocol, select **default** from the Basic Configurations page of the device. Otherwise, select **MSEVEN6** or **MSEVEN** to override the global Default Event Log Poll Protocol.

   The **MSEVEN6** is a Microsoft event protocol that collects more information from an event log, such as the task, keyword, and opcode. It also provides a better message formatting.
4. Click **Deploy Changes** under **Actions**.

RELATED DOCUMENTATION

Sending Encrypted Events to JSA | 68

Collecting Local Windows Logs | 70

Collecting Remote Windows Logs | 71

Sending Encrypted Events to JSA

In JSA, configure a Universal DSM that uses the TLS Syslog protocol. For more information, see the *Configuring DSMs Guide*.

The uDSM opens a port and provides the certificate that is necessary for communicating by using TLS. If you delete the uDSM, TLS communication stops.

Configure a log source in stand-alone deployments of WinCollect to send encrypted events to JSA with TLS syslog. TLS Syslog is only supported in managed WinCollect deployments in JSA 7.3.1 and later.

1. Use SSH to log in to JSA as the root user.
2. Copy the certificate, including `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` from **/opt/qradar/conf/trusted_certificates/syslog-tls.cert** to a temporary location. You will paste this certificate into the WinCollect Configuration Console.
3. In the WinCollect Configuration Console, expand **Destinations**, and click **Add Destination**.
4. In the **New Destination Name** box, add a name for the destination and then click **OK**.
5. Select the new destination and enter the IP address of the target JSA appliance in the **Hostname** field.
6. Type **6514** in the **Port** field.
7. Type the events per second (EPS) rate for your deployment in the **Throttle** field.
8. Paste the certificate that you copied from JSA into the **Certificate** field.
9. Click **Deploy Changes** under **Actions**.

RELATED DOCUMENTATION

Collecting Local Windows Logs | 70

Collecting Remote Windows Logs | 71

Adding a Device to the WinCollect Configuration Console | 67

Increasing UDP Payload Size

You can increase the payload size for UDP syslog destinations in the Agent Configuration file

The default payload size for UDP destination packages is 1,024 bytes. You can increase the payload size for a standalone WinCollect agent by adding a parameter in the Agent Configuration file.

NOTE: After you change the payload size for the WinCollect agent, you must increase the maximum UDP payload size in JSA.

1. Open the Agent Configuration XML file.

   The default path to this file is **WinCollect\config\AgentConfig.xml**.
2. Add the following parameter to the `UDPSendStage` module:

   ```
   <Parameter name="MaxPayloadSize" value="<desired value>"/>
   ```
3. Save the file, and restart the WinCollect agent.

After you change the payload size for the WinCollect agent, you must increase the maximum UDP payload size in JSA.

Include Milliseconds in Event Log Timestamp

In a stand-alone WinCollect deployment, you can include milliseconds in the timestamp for Event Logs.

NOTE: This option is only compatible in a stand-alone WinCollect deployment that uses the MSEVEN6 protocol. It is not supported by the MSEVEN protocol.

The **TimeGenerated** and **TimeWritten** payload fields in the Event Logs use seconds by default. You can set the **Timestamp Properties** to use milliseconds in the **Microsoft Windows Event Log Properties** node of the **WinCollect Configuration Console**.

NOTE: This is an Agent-level change that is set for all log sources.

Alternatively, you can change the property as part of the command line installation, using this parameter: `&Component1.TimestampFormat=Milliseconds`. You can also use a template to change the attribute in the AgentConfig.xml file. For more information, see "Changing configuration with Templates in a Stand-alone Deployment" on page 72.

RELATED DOCUMENTATION

Collecting Local Windows Logs | 70

Collecting Remote Windows Logs | 71

Changing configuration with Templates in a Stand-alone Deployment | 72

Collecting Local Windows Logs

This use case scenario describes the settings required to collect logs from the host where the WinCollect Configuration Console is installed, and send them to JSA.

1. Install the WinCollect Configuration Console on the host on which that you want to collect windows logs. Download the patch from https://support.juniper.net/support/downloads/
2. Create a destination for the JSA instance where you want to send WinCollect information. See "Adding a Destination to the WinCollect Configuration Console" on page 65.
3. Configure the local Microsoft event log device that is monitored. See "Adding a Device to the WinCollect Configuration Console" on page 67.

   NOTE: In the **Device Address** field, type the IP address or hostname of the local Windows system that you want to poll for events.

4. Click **Deploy Changes** under **Actions**.

RELATED DOCUMENTATION

Collecting Remote Windows Logs | 71

Adding a Device to the WinCollect Configuration Console | 67

Sending Encrypted Events to JSA | 68

Collecting Remote Windows Logs

This use case scenario describes the settings that are required in the WinCollect Configuration Console to collect windows logs from hosts that do not have WinCollect software installed, and send the logs to JSA.

> **NOTE**: WinCollect does not support reverting Citrix Virtual Machines that are polled remotely.

1. Install the WinCollect Configuration Console on the windows machine that collects the log information. Download the patch from https://support.juniper.net/support/downloads/
2. Create a credential to use when you log in to remote hosts. See "Creating a WinCollect Credential" on page 64.
3. Create the JSA destination where Windows events are sent. See "Adding a Destination to the WinCollect Configuration Console" on page 65.
4. Configure the devices that are monitored. See "Adding a Device to the WinCollect Configuration Console" on page 67.

   > **NOTE**: In the **Device Address** field, type the IP address or hostname of the remote Windows system that you want to poll for events.

5. Click **Deploy Changes** under **Actions**.

RELATED DOCUMENTATION

Adding a Device to the WinCollect Configuration Console | 67

Sending Encrypted Events to JSA | 68

Collecting Local Windows Logs | 70

Changing configuration with Templates in a Stand-alone Deployment

IN THIS SECTION

Supported Version: WinCollect 7.2.8 + stand-alone only. With templating, you can change the Agent configuration without making manual or scripted edits to the `AgentConfig.xml` file.

When you copy a template to the WinCollect patch directory, the Agent replaces the existing configuration with the contents of the template. Before the Agent applies the changes from the template, it makes a backup of the current configuration in the `patchcheckpoint` directory. After the changes are applied, the Agent restarts and uses the new configuration.

Four sample templates are installed with WinCollect 7.2.8 and later. They are stored in the **\JSA \WinCollect\templates** directory.

- `tmplt_AgentCore.xml`
- `tmplt_DestinationManager.xml`
- `tmplt_DeviceWindowsLog.xml`
- `tmplt_PayloadRouter.xml`

NOTE: These templates are examples only. All Agent configuration service modules are supported, so that you can create your own templates.

The following use cases are examples of how you can use templates to change Agent configurations.

Use Case 1: Change Heartbeat Interval

You want to change the heartbeat interval from 5 minutes to 1 hour on all deployed systems. Previously, this required manual or scripted changes to the agentconfig.xml file and a WinCollect service restart. With templates, you can change this interval by performing the following steps.

1. Locate the `tmplt_AgentCore.xml` template in the **\IBM\WinCollect\templates** directory. This service contains the Heartbeat Interval configuration.

2. Make a copy of the template and name it `service_AgentCore.xml`.

3. Change the value of the `HeartbeatInterval` parameter to 3,600,000 milliseconds (1 hour).

```
<Service classification="Static" type="Service" version="7.2.8"
module="AgentCore" name="AgentCore”>
<Environment>
<Parameter name="HeartbeatInterval" value="3600000"/>
<Parameter name="ConfigurationCheckInterval" value="300000"/>
<Parameter name="Enabled" value="true"/>
<Parameter name="Deleted" value="false"/>
<Environment>
</Service>
```

4. Move the `service_AgentCore.xml` file to the **\IBM\WinCollect\patch** directory. After a few seconds, the file disappears and the agent restarts. The old `agentconfig.xml` file is moved to the backup directory (**patch_checkpoint_xxxx**).

Use Case 2: Modify Event Data Storage Configuration

You want to change the location and capacity of the event data that is stored in the **\programdata \WinCollect** file. You want to store the event data in C:\WinCollect\Data and change the capacity to 20 GB. There is no default template for this change, but you can easily create one by using information in the agentconfig.xml file. The following sample shows the existing service:

```
<Service classification="Static" type="Service" version="7.2.8"
module="WinCollectCommon" name="DiskManager">
<Environment>
<Parameter name="BasePath" value="%ALLUSERSPROFILE%\WinCollect\Data"/>
<Parameter name="Capacity" value="6144"/>
```

```
<Environment>
</Service>
```

NOTE: `%ALLUSERSPROFILE%` is an environment variable. The default value is C:\ProgramData. You want to change this value to **C:\WinCollect\Data**.

1. Create an XML file named **service_DiskManager.xml** with the following contents:

   ```
   <Service classification="Static" type="Service" version="7.2.8"
   module="WinCollectCommon" name="DiskManager">
   <Environment>
   <Parameter name="BasePath" value="c:\ibm\WinCollect\Data”//>
   <Parameter name="Capacity" value="20480"/>
   <Environment>
   </Service>
   ```

2. Move the file to the **\IBM\WinCollect\patch** directory.

   After a few seconds, the file disappears and the agent restarts. Data is now written to the new directory.

Use Case 3: Send TCP instead of UDP

You want to send Syslog data to JSA over TCP rather than UDP. You must specify this option in the Destination Manager.

1. Locate the `tmplt_DestinationManager.xml` template in the \IBM\WinCollect\templates directory.

2. Make a copy of the template and name it `service_DestinationManager.xml`.

3. In `<Module order=”4"> service_name=""UDPSendStage">`, change the `service_name` parameter to **TCPSendStage**.

   ```
   <Service version="7.2.8" classification="Service" type="Service"
   module="WinCollectPlugin" name="DestinationManager">
   <Environment>
   <InstanceData>
   Instance name=”Qradar”>
   <Environment>
   ```

```
<Module order="1" service_name="StoreAndForwardStage">
<Environment>
<Parameter name="DataChunkPeriod" value="10"/>
<Parameter name="DataProcessingPeriod" value="500000"/>
<Parameter name="QueueLowWaterMark" value="750000"/>
<Parameter name="QueueHighWaterMark" value="1000000"/>
<Parameter name="Schedule.Enable" value="true"/>
<Parameter name="Schedule.Invert" value="false"/>
<Parameter name="Socket.KeepAlive.Enabled" value="true"/>
<Parameter name="Socket.KeepAlive.Time" value="30000"/>
<Parameter name="Socket.KeepAlive.Interval" value="4000"/>
</Environment>
</Module>
<Module order="2" service_name="SimpleEventThrottle”>
<Environment>
<Module order="2" service_name="SimpleEventThrottle">
<Environment>
<Parameter name="EventThrottleInEPS" value="5000"/>
</Environment>
</Module>
<Module order="4" service_name="TCPSendStage”>
<Environment>
<Parameter name="TargetAddress" value="172.18.X.X"/>
<Parameter name="TargetPort" value="514"/>
<Environment>
</Module>
<Instance>
<InstanceData>
</Service>
```

4. Move the file to the **\IBM\WinCollect\patch** directory. After a few seconds, the file disappears and the agent restarts. The old `agentconfig.xml` file is moved to the backup directory (`patch_checkpoint_xxxx`).

Use Case 4: Add NSA Filtering to an Existing Log Source

You want to add NSA filtering to an existing log source. You can change this attribute by using the `tmplt_DeviceWindowsLog.xml` template.

1. Locate the `tmplt_DeviceWindowsLog.xml` template

2. Make a copy of the template and name it `service_DeviceWindowsLog.xml`.

3. Open `AgentConfig.xml` and locate the log source contained in the module `DeviceWindowsLog`.

4. Copy the model and instance information and replace the contents in `service_DeviceWindowsLog.xml` with it.

5. Modify the following lines with the bolded sample code:

```
<Parameter name="Filter.System.Type" value="NSAlist"/>
<Parameter name="Filter.System.Param">
"1,6,12,13,19,104,219,1001,1125,1126,1129,7000,7022,7023,7024,7026,7031,7032,7034,7045"/>
<Parameter name="Filter.System.Enabled" value="true"/>
```

6. Save the `service_DeviceWindowsLog.xml` file and move it to the file to the \IBM\WinCollect\patch directory. After a few seconds, the file disappears and the agent restarts. The old **agentconfig.xml** file is moved to the backup directory (`patch_checkpoint_xxxx`).

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials

IN THIS SECTION

Users with appropriate remote access permissions might be able to collect events from remote systems without using domain administrator credentials. Depending on what information you collect, the user might need extra permissions. For example, a user might need to collect Security event logs remotely. Therefore, the user that is configured in the JSA log source must have remote access to the Security event log from the server where the Agent is installed.

NOTE: For remote collection, the WinCollect user must work with their Windows administrator to ensure access to the following items:

- Logs for security, system, and application events
- The remote registry
- Any directories that contain .dll or .exe files that contain message string information

With certain combinations of Windows operating system and group policies in place, alternative configurations might not be possible.

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 need to complete more configuration steps for your WinCollect deployment.

The following permissions and credentials are required for service accounts to access remote polling log sources that WinCollect supports.

Permissions	Log Sources
The service account needs to be able to access the folder that the log file is in and open the file.	• Microsoft DHCP • Microsoft Exchange Server • DNS debug • File Forwarder • Microsoft IAS • Microsoft IIS • Microsoft ISA • Juniper Steel-Belted Radius • Microsoft SQL • Net App Data ONTAP • TLS

(Continued)

Permissions	Log Sources
The log source user must be a member of the **Event Log Readers** group. If this group is not configured, then domain administrative privileges are usually required to poll a Windows event log across a domain.	Microsoft Windows Security Event Log

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.

Changing WinCollect Configuration from the Command Line

You can change the configuration of a WinCollect agent from the command line of the Windows host.

After the initial installation of a WinCollect agent on a Windows host, you can change the configuration by using the **installhelper.exe** file that is located in the *<WinCollect_installation_path>*/bin.

The following configuration parameters can be modified:

Table 16: Modifiable Configuration Parameters

Parameter	Description
Authentication Token	Authorizes the WinCollect service, for example, `AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111`
Configuration Server (host and port)	The IP address or host name of your JSA Console, for example, 100.10.10.1 or myhost.
Default Status Server Address	Displays the IP address of the Configuration Server, where status messages from the WinCollect agent are sent.
Local IP	Use this setting to select the IP address that is displayed for all log sources on systems with multiple network interface cards (NIC).

Table 16: Modifiable Configuration Parameters *(Continued)*

Parameter	Description
Originating Computer	Use this setting to select the IP address that is displayed only for Windows events on systems with multiple NICs.

The **installHelper.exe** file has the following update flags:

-h [--help]	Provides detailed information on the installHelper.exe usage options.
-P [--update-password]	Update a password in the AgentConfig.xml configuration file. Specify the Login.Handle and new password, colon separated. For example, 1:MyNewPassword. **NOTE**: The password is in plain text.
-F [--update-password-with-file]	Update a set of passwords in the AgentConfig.xml configuration file using an external file. Specify the Login.Handle and new password, colon separated, one per line. For example, 1:MyNewPassword. **NOTE**: Make sure you erase the input file or keep it secured.
-T [--update-auth-token]	The new authentication token to be used to communicate with the configuration server.
-L [localIP]	Use this setting to select the IP address that is displayed for all log sources on systems with multiple network interface cards (NIC). For example, installerhelper.exe -L 192.0.2.0
-O [OrigComputer]	Use this setting to select the IP address that is displayed for Windows events on systems with multiple NICs. For example, installerhelper.exe -O 198.51.100.0

For example, to change an authorization token for a WinCollect agent, type the following in the command line of the Windows host:

<WinCollect_installation_path>/bin/installHelper.exe -T <authorization_token>

Local Installations with No Remote Polling

Install WinCollect locally on each host that you cannot remotely poll. After you install WinCollect, JSA 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 can 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 JSA.

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 Windows event subscriptions to forward events. When event subscriptions are configured, numerous Windows hosts can forward their events to JSA without needing administrator credentials.

Forwarded Events

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.

Windows event subscriptions, or forwarded events, are not considered local or remote, but are event listeners. The WinCollect **Forwarded Events** check box enables the WinCollect log source to identify Windows event subscriptions. The WinCollect agent displays only a single log source in the user interface, but this log source is listening and processing events for potentially hundreds of event subscriptions. One log source in the agent list is for all event subscriptions. The agent recognizes the event from the subscription, processes the content, and then sends the syslog event to JSA.

NOTE: Forwarded events can be collected with the Forwarded Events check box only. An XPATH cannot be used.

Forwarded events are displayed as *Windows Auth @ <hostname> or <FQDN>* in the **Log Activity** tab. Conversely, locally or remotely collected events appear as *Windows Auth @ IP address* or *hostname*. When WinCollect processes a locally or remotely collected event, WinCollect includes an extra syslog header that identifies the event as a WinCollect event. Because the forwarded event is a pass-through or listener, the extra header is not included, and forwarded events appear like standard and don't include the WinCollect identifier.

NOTE: WinCollect collects only those forwarded events that appear in the Windows Event Viewer.

Domain Controllers

If you have domain controllers, consider installing local WinCollect agents on the servers. Due to the potential number of generated events, use a local log source with the agent installed on the domain controller.

Supported Software Environments

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

- Windows 8 (most recent)
- Windows Server 2012 (most recent)
- Windows 10 (most recent)
- Windows Server 2016 (including Core)
- Windows Server 2019 (including Core)

> **NOTE**: WinCollect is not supported on versions of Windows that have been moved to End Of Life by Microsoft. After software is beyond the Extended Support End Date the product might still function as expected, however, Juniper Networks will not make code or vulnerability fixes to resolve WinCollect issues for older operating systems. For example, Microsoft Windows Server 2003 R2 and Microsoft Windows XP are operating systems that are beyond the 'Extended Support End Date'. Any questions about this announcement can be discussed in the JSA Collecting Windows Events (WMI/ALE/WinCollect) forum. For more information, see https://support.microsoft.com/en-us/lifecycle/search (https://support.microsoft.com/en-us/lifecycle/search).

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

Troubleshooting Event Collection

Microsoft event subscriptions don't have an alert mechanism to indicate when an event source stopped sending. If a subscription fails between the two Windows systems, the subscription appears active, but the service that is responsible for the subscription can be in an error state. With WinCollect, the remotely polled or local log sources can time out when events are not received within 720 minutes (12 hours).

Configuring Microsoft Event Subscriptions

Configure Microsoft event subscriptions to forward events to a single WinCollect agent.

WinCollect supports event subscriptions with the following parameters:

Forwarded Events - The subscription must send the logs to the forwarded event channel. Selected in the **Destination log** list.

Subscriptions - The subscription configured to use **ContentFormat**: `RenderedText` and **Locale**: `en-US`

Locale - Locale must be `en_US` for the Windows computer where WinCollect is installed.

> **NOTE**: If you are using domain controllers, consider installing local WinCollect agents on the servers. Due to the potential number of generated events, use a local log source with the agent that is installed on the domain controller.

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.

JSA Support does not support the creation or maintenance of Microsoft Subscriptions.

RELATED DOCUMENTATION

WinCollect Log File | **143**

Adding Custom Entries to WinCollect Status Messages | **62**

WinCollect Destinations | **58**

6

CHAPTER

Log Sources for WinCollect Agents

Log Sources for WinCollect Agents

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

You can add log sources that communicate through a WinCollect agent individually for remote polling. If the log sources contain similar configurations, you can simultaneously add multiple, or bulk add log sources. A change to an individually added log source updates only the individual log source. A change that you make to a group of log sources updates all of the log sources in the log source group.

You can add a local log source for local collection. You can create a log source manually, if it wasn't autocreated.

NOTE: If your deployment has the same user name accounts on different domains, ensure that you configure domain information when you create the WinCollect log source.

RELATED DOCUMENTATION

Adding a Log Source to a WinCollect Agent | 131

Windows Event Logs

IN THIS SECTION

You can collect the event logs from your Windows endpoints.

When you query a Windows event log, the query includes every event in the log. You can use event log filtering or XPath queries to limit the events that you receive.

Windows event logs are supported in the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

Windows Event Log Filtering

You can configure the WinCollect agent to ignore or to include specific events collected from the Windows event log. You can limit the total EPS (events per second) that are sent to the JSA console by using the filter types.

The WinCollect agents can be configured to ignore events globally by ID code or log source. 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 payload. Separate multiple sources by using a semi-colon. Events filters such as exclusion, inclusion, and NSA are available for the following log source types:

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

- Forwarded Events

The WinCollect agent requests all available events from the Event Collection API each time the value specified in the Polling Interval field expires.

For the exclusion filter, the agent examines all of the events retrieved from the Event Collection API and ignores events that match the exclusions defined by the administrator (either by Windows Event ID or by source). The agent then takes the remaining events and assembles the **name=value** pairs and forwards the events to either the JSA console or the Event Collector appliance. However, for the inclusion filter, the agents pulls events that matches the Event IDs specified by the administrator and forward those events to JSA console or Event Collector.

The NSA filter is a unique type of filter that includes a corresponding list of pre-defined security Event IDs, which the agent pulls from the Security, System, Application and DNS logs. These pre-defined security Event IDs are included in the events that the agent forwards to JSA console or Event Collector.

NOTE: The Forwarded Events filter requires you to identify the source or channel, with the eventIDs that you wish to filter in parentheses. Use semicolons as delimiters. For example:

```
Application(200-256,4097,34);Security(1);Symantec(1,13)
```

In this example, event IDs from 200 to 256, 4097 and 34 are filtered for the channel Application, event ID 1 is filtered for Security, and event IDs 1 and 13 are filtered for the source called Symantec.

Windows 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 17: Common WinCollect Log Source Parameters

Parameter	Description
Log Source Identifier	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. Used to poll events from remote sources

Table 17: Common WinCollect Log Source Parameters *(Continued)*

Parameter	Description
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 JSA.
Domain	Optional The domain that includes the Windows-based log source. The following examples use the correct syntax: **LAB1**, **server1.mydomain.com** The following syntax is incorrect: **\\mydomain.com**
Event Rate Tuning Profile	For the default polling interval of 3000 ms, the approximate Events per second (EPS) rates attainable are as follows: • **Default (Endpoint)**: 33-50 EPS • **Typical Server**: 166-250 EPS • **High Event Rate Server**: 416-625 EPS For a polling interval of 1000 ms the approximate EPS rates are as follows: • **Default (Endpoint)**: 100-150 EPS • **Typical Server**: 500-750 EPS • **High Event Rate Server**: 1250-1875 EPS
Polling Interval (ms)	The interval, in milliseconds, between times when WinCollect polls for new events.
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 17: Common WinCollect Log Source Parameters *(Continued)*

Parameter	Description
Event Log Poll Protocol	The protocol that JSA uses to communicate with the Windows device. The default is **MSEVEN6**.
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, and 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. **Example:** : Exclusion filters can use commas and hyphens to filter single EventIDs or ranges, such as 4609, 4616, 6400-6405
Security	Select the checkbox to enable WinCollect to forward security logs to JSA.
Security Log Filter Type	To ignore specific events ID collected from the Windows event log, select **Exclusion Filter**. To include specific events ID collected in the Windows event log, select **Inclusion Filter**. The **NSA Filter** option populates the **Security Log Filter** field with a list of event IDs recommended by National Security Agency. The default is **No Filtering**. **NOTE**: If you select a filter type from the list, a new field **Security Log Filter** displays. You must provide the event IDs that you want to include or exclude.
System	Select the checkbox to enable WinCollect to forward system logs to JSA.

Table 17: Common WinCollect Log Source Parameters *(Continued)*

Parameter	Description
System Log Filter Type	To ignore specific events ID collected from the Windows event log, select **Exclusion Filter**. To include specific events ID collected in the Windows event log, select **Inclusion Filter**. The **NSA Filter** option populates the **System Log Filter** field with a list of event IDs recommended by National Security Agency. The default is **No Filtering**. **NOTE**: If you select a filter type from the list, a new field **System Log Filter** displays. You must provide the event IDs that you want to include or exclude.
Application	Select the checkbox to enable WinCollect to forward application logs to JSA.
Application Log Filter Type	To ignore specific events ID collected from the Windows event log, select **Exclusion Filter**. To include specific events ID collected in the Windows event log, select **Inclusion Filter**. The **NSA Filter** option populates the **Application Log Filter** field with a list of event IDs recommended by National Security Agency. The default is **No Filtering**. **NOTE**: If you select a filter type from the list, a new field **Application Log Filter** displays. You must provide the event IDs that you want to include or exclude.
DNS Server	Select the checkbox to enable WinCollect to forward DNS Server logs to JSA.
DNS Server Log Filter Type	To ignore specific events ID collected from the Windows event log, select **Exclusion Filter**. To include specific events ID collected in the Windows event log, select **Inclusion Filter**. The **NSA Filter** option populates the **DNS Server Log Filter** field with a list of event IDs recommended by National Security Agency. The default is **No Filtering**. **NOTE**: If you select a filter type from the list, a new field **DNS Server Log Filter** displays. You must provide the event IDs that you want to include or exclude.

Table 17: Common WinCollect Log Source Parameters *(Continued)*

Parameter	Description
File Replication Service	Select the checkbox to enable WinCollect to forward File Replication Service logs to JSA.
File Replication Service Log Filter Type	To ignore specific events ID collected from the Windows event log, select **Exclusion Filter**. To include specific events ID collected in the Windows event log, select **Inclusion Filter**. **NOTE**: If you select a filter type from the list, a new field **File Replication Service Log Filter** displays. You must provide the event IDs that you want to include or exclude.
Directory Service	Select the checkbox to enable WinCollect to forward Directory Service logs to JSA.
Directory Service Log Filter Type	To ignore specific events ID collected from the Windows event log, select the **Exclusion Filter**. To include specific events ID collected in the Windows event log, select the **Inclusion Filter**. **NOTE**: If you select a filter type from the list, a new field **Directory Service Log Filter** displays. You must provide the event IDs that you want to include or exclude.
Forwarded Events	Enables JSA 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. **NOTE**: WinCollect supports pulling logs only from the Forwarded Events channel. Writing events from a subscription to a different channel is not supported.

Table 17: Common WinCollect Log Source Parameters *(Continued)*

Parameter	Description

Forwarded Events filter type	To ignore specific events ID collected from the Windows event log, select **Exclusion Filter**.
	To include specific events ID collected in the Windows event log, select Inclusion Filter.
	The **NSA Filter** option populates the **Forwarded Events** filter field with all channels and their respective filters, as recommended by the National Security Agency.
	The default is **No Filtering**.
	NOTE: If you select a filter type from the list, a new field **Forwarded Events Filter** displays. You must provide the event IDs that you want to include or exclude.
	The Forwarded Events filter requires you to identify the source or channel, with the eventIDs that you want to filter in parentheses. Use semicolons as delimiters. For example:
	`Application(200-256,4097,34);`
	`Security(1);Symantec(1,13)`
	In this example, event IDs 200 - 256, 4097 and 34 are filtered for the channel Application. Event ID 1 is filtered for Security. Event IDs 1 and 13 are filtered for the source called Symantec.

Event Types	At least one event type must be selected. If you need to collect specific event types, follow the instructions for creating a custom XPath with those specific event types. For more information, see "Creating a Custom View" on page 93.
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 checkbox. If you do, leave the override domain and DNS parameters blank. **NOTE**: You must enter values for the **Domain Controller Name Lookup** and **DNS Domain Name Lookup** parameters.
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 hostname of the domain controller that is responsible for the Active Directory lookup.

Table 17: Common WinCollect Log Source Parameters *(Continued)*

Parameter	Description
XPath Query	Structured XML expressions that you use to retrieve customized events from Windows event logs. If you specify an XPath query to filter events, the check boxes that you selected from the **Standard Log Type** or **Event Type** are collected along with the XPath Query. To collect information by using an XPath Query, you might be required to enable **Remote Event Log Management** on Windows 2008.
Target Internal Destination	Use any managed hosts with an event processor component as an internal destination.
Target External Destination	Forwards your events to one or more external destinations that you configured in your destination list.

Applications and Services Logs

Use XPath queries to collect events from the Applications and Services event logs.

XPath queries are structured XML expressions that you use to retrieve customized events from the Windows event logs.

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.

NOTE: Using more than 10 XPath queries can affect WinCollect performance, depending on the XPath and the number of events coming in to each channel.

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.

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 log source. You can select the source from the Event sources drop-down menu, or you can browse to a source from the Event logs drop-down menu..
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

Configure a log source with the XPath query. For more information, see Applications and Services Logs.

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.

NOTE: XPath uses only the MSEVEN6 event protocol.

Example: Monitoring Events for a Specific User

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

NOTE: XPath queries cannot filter Windows Forwarded Events.

```
<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> </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 18: 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 19: 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.
4743	A user account was deleted.

Example: Retrieving DNS Analytic Logs

In this example, the query retrieves all events that are captured in DNS analytic logs.

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-DNSServer/Analytical">
<Select Path="Microsoft-Windows-DNSServer/Analytical">*</Select>
</Query>
</QueryList>
```

Example: Retrieving Events with Sysinternals Sysmon

In this example, the query retrieves all events that are captured by SysInternals Sysmon.

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-DNSServer/Operational">
<Select Path="Microsoft-Windows-DNSServer/Operational">*</Select>
</Query>
</QueryList>
```

RELATED DOCUMENTATION

Microsoft DHCP Log Source Configuration Options | 97

Microsoft DHCP Log Source Configuration Options

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

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

Table 20: Microsoft DHCP Protocol Parameters

Parameter	Description
Log Source Type	**Microsoft DHCP**
Protocol Configuration	**WinCollect Microsoft DHCP**
Local System	The WinCollect agent must be installed on the Microsoft DHCP Server. The log source uses local system credentials to collect and forward events to the JSA.

For more information about DHCP log source configuration, see the *Configuring DSMs Guide*.

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

Table 21: Default Root Log Directory Paths for Microsoft DHCP Events

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

Table 22: Example Log Format for Microsoft DHCP Events

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

RELATED DOCUMENTATION

DNS Debug Log Source Configuration Options | **101**

File Forwarder Log Source Configuration Options | **105**

Microsoft Exchange Server Log Source Configuration Options

IN THIS SECTION

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

Supported versions

WinCollect supports the following versions of Microsoft Exchange :

- Microsoft Exchange 2003
- Microsoft Exchange 2007
- Microsoft Exchange 2010
- Microsoft Exchange 2013
- Microsoft Exchange 2016
- Microsoft Exchange 2019

Table 23: Microsoft Exchange Server protocol parameters

Parameter	Description
Log Source Type	Microsoft Exchange Server

Table 23: Microsoft Exchange Server protocol parameters *(Continued)*

Parameter	Description
Protocol Configuration	**WinCollect Microsoft Exchange**
Local System	The WinCollect agent must be installed on the Microsoft Exchange Server. The log source uses local system credentials to collect and forward events to the JSA.

Ensure that the firewalls that are located between the Exchange Server and the remote host allow traffic on the following ports:

- TCP port 135 for Microsoft Endpoint Mapper.
- UDP port 137 for NetBIOS name service.
- UDP port 138 for NetBIOS datagram service.
- TCP port 139 for NetBIOS session service.
- TCP port 445 for Microsoft Directory Services to transfer files across a Windows share.

For more information about Microsoft Exchange log source configuration, see the *Configuring DSMs Guide*.

The Exchange Server OWA event logs that are monitored by WinCollect are defined by the directory path that you specify in your WinCollect Exchange Server log source. Microsoft Exchange writes to two directories: W3SVC1 and W3SVC2. The Microsoft Exchange plug-in monitors all recursive files under the **C:\inetpub\logs\LogFiles\ directory**.

Table 24: Default OWA directory paths for Microsoft Exchange Server events

Collection type	Root log directory
Local	**C:\inetpub\logs\LogFiles\W3SVC1**
Remote	**\\*<Exchange_Server_IP address>*\c$\inetpub\logs\LogFiles\W3SVC1**

The Exchange Server Message Tracking event logs that are monitored by WinCollect are defined by the directory path that you specify in your WinCollect Exchange Server log source.

Table 25: Default Message Tracking directory paths for Microsoft Exchange Server events

Collection type	Root log directory
Local	**C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking**
Remote	**\\*<Exchange_Server_IP address>*\C$ \Program Files\Microsoft\Exchange Server \V15\TransportRoles\Logs\MessageTracking**

Table 26: Default SMTP/Mail directory paths for Microsoft Exchange Server events.

Collection type	Root log directory
Local	**C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog**
Remote	**\\*<Exchange_Server_IP address>*\C$ \Program Files\Microsoft\Exchange Server \V15\TransportRoles\Logs\Hub \ProtocolLog**

DNS Debug Log Source Configuration Options

IN THIS SECTION

Use the reference information to configure the WinCollect plug-in for MicrosoftWindows DNS debug logging.

NOTE: DNS debug logging can affect system performance and disk space because it provides detailed data about information that the DNS server sends and receives. Enable DNS debug logging only when you require this information.

DNS debug logging is supported on the following Windows versions:

- Windows Server 2019 (including Core)
- Windows Server 2016 (including Core)
- Windows Server 2012 R2
- Windows Server 2012

Table 27: DNS Debug Protocol Parameters

Parameter	Description
File Reader Type	Reads file contents. Both options have basic Unicode encoding support for byte-order marks. If you choose the **Text (file held open)** option, then WinCollect maintains a shared read and write lock on the monitored log file. If you choose the **Text (file open when reading)** option, then WinCollect maintains a shared read and write lock on the log file only when it reads the file.
File Monitor Type	Detects file and directory changes: The **Notification-based (local)** option uses the Windows file system notifications to detect changes to your DNS log. The **Polling-based (remote)** option monitors changes to remote files and directories. The agent polls the remote DNS log and compares the file to the last polling interval. If the log contains new entries, the entries are retrieved.
File Pattern	The regular expression (regex) required to match the DNS debug log file set in the DNS manager.

Table 27: DNS Debug Protocol Parameters *(Continued)*

Parameter	Description
Root Directory	The directory where WinCollect monitors files. The directory must be Local File System for local collection, or a valid MicrosoftWindows universal naming convention (UNC) path for remote collection. This value must match the file path that is configured in your DNS manager. **NOTE**: Due to restrictions in distributed systems, the path can't be verified in the user interface.
Include DNS Details	Includes DNS details in the Windows Server DNS debugging log.

For more information about Microsoft DNS Debug specifications, see the *Configuring DSMs Guide*.

Enabling DNS Debugging on Windows Server

Enable DNS debugging on Windows Server to collect information that the DNS server sends and receives.

The DNS role must be installed on the Windows Server.

1. Open the DNS Manager with the following command:

   dnsmgmt.msc

2. Right-click the DNS server and click **Properties**.
3. Click the **Debug Logging** tab.
4. Select **Log packets for debugging**.
5. In the log file, type the file path and name, and the maximum size.

   > **NOTE**: The file path and name, must align with the **Root Directory** and **File Pattern** that you provided when you configured the Microsoft DNS log source in JSA.

6. If you want to include DNS details in the log, select **Details** in the **Other options** section, and then select **Include DNS Details** in the log source.

7. Click **Apply** and then click **OK**.

RELATED DOCUMENTATION

File Forwarder Log Source Configuration Options | **105**

Microsoft IAS Log Source Configuration Options | **107**

WinCollect Microsoft IIS Log Source Configuration Options | **110**

Collecting DNS Analytic Logs by Using XPath

To collect DNS Analytic logs by using WinCollect, you must first configure Windows to collect analytic logs and then add an XPath to the WinCollect Agent log source to collect the logs and send them to JSA.

DNS debug logging is supported on the following Windows versions:

Use Event Viewer to configure Windows to collect DNS Server analytic logs.

1. To open the Event Viewer, type `eventvwr.msc` at an elevated command prompt, and press **Enter**.

2. Go to Applications and Services **Logs\Microsoft\Windows\DNS-Server**.

3. Right-click **DNS-Server**, and then click **View > Show Analytic and Debug Logs**.

4. Right-click the **Analytical** log, and then click **Properties**.

5. In the **When maximum event log size is reached** section, choose **Do not overwrite events (Clear logs manually)**, select **Enable logging**, and then click **OK** on the resulting dialog box.

   NOTE: you do not select this option, the WinCollect Agent can't collect the Analytical log, because the logs are stored in etl format.

6. Click **OK** to enable the DNS Server Analytic event log.

   NOTE: You must manually clear the logs and restart the agent when the event log is full

7. In the log source, add the following XPath to the WinCollect Agent:

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-DNSServer/Analytical”>
<Select Path="Microsoft-Windows-DNSServer/Analytical”>*</Select>
</Query>
</QueryList>
```

File Forwarder Log Source Configuration Options

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

You must also configure parameters that are not specific to this plug-in. The File Forwarder plug-in can be used with Universal DSM to poll many types of logs from the Windows host.

Table 28: File Forwarder Protocol Parameters

Parameter	Description
Log Source Type	**Universal DSM**
Protocol Configuration	Select **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 JSA.
Root Directory	The location of the log files to forward to JSA. 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.
Filename Pattern	The regular expression (regex) that is 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 Root Directory.

Table 28: File Forwarder Protocol Parameters *(Continued)*

Parameter	Description
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.
Only Monitor Files Created Today	Enabled by default. Clear this option to monitor files from before the current day.
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. Select the **Memory Mapped Text (local only)** option only when advised by Juniper Customer Support. This option is used when the system that generates your event log polls the end of the event log for changes. This option requires that you also select the **Local System** check box.
File Reader Encoding	For files without a BOM, select **ANSI** if you want the files converted to UTF8. Otherwise, select **UTF8** if the files are already in UTF8 and no conversion is needed. **NOTE**: This option is only available on the WinCollect Configuration Console.

Table 28: File Forwarder Protocol Parameters *(Continued)*

Parameter	Description
File Parser Type	Files can be parsed in two ways: Single Line or Multi Line. **Single Line** - Parses a file and creates an event for each line. **Multi Line** - Parses an XML file and creates an event that comprises multiple lines from the point that a specified starting token is parsed, until the next time the specified starting token is parsed. **NOTE**: Multi Line parsing currently only supports XML file types.
Multi Line "Starts With" Regex Token	The Multi Line File Parser Type requires a "Starts With" token. The "Starts With" token should be the regex that is required to identify every character from the beginning of the line you want to start a multi line event with. It is important to make your regex as accurate as possible to avoid combining events due to similar whitespace before the characters, and to avoid not parsing the file at all due to not finding a "Starts With" token.

RELATED DOCUMENTATION

Microsoft IAS Log Source Configuration Options | 107

WinCollect Microsoft IIS Log Source Configuration Options | 110

Microsoft ISA Log Configuration Options | 113

Microsoft IAS Log Source Configuration Options

IN THIS SECTION

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

Table 29: Supported Windows Versions and Log Formats

Microsoft IAS	Supported Versions
MicrosoftWindows support	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2
NPS log server log formats	Data Transformation Service Open Database Connectivity Internet Authentication Service

NOTE: WinCollect does not support events that are logged to a Microsoft SQL Server.

Microsoft IAS Directory Structure for Event Collection

The event logs that are monitored by WinCollect are defined by the root directory that you should configure in your log source.

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

To improve performance, you can create a sub folder for 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 many files to locate your event logs.

If your system generates a large number of IAS or NPS events, you can configure your Windows system to create a new event log at daily intervals. This action ensures that agents do not have to search large logs for new events.

Table 30: Event Log Default Directory Structure for Microsoft IAS

Event version	Root Log Directory
MicrosoftWindows Server 2019	**\Windows\System32\Logfiles\**
MicrosoftWindows Server 2016	**\Windows\System32\Logfiles\**
MicrosoftWindows Server 2012 R2	**\Windows\System32\Logfiles\**

Microsoft IAS Protocol Parameters

Table 31: Microsoft IAS 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 JSA.
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 DOCUMENTATION

WinCollect Microsoft IIS Log Source Configuration Options | 110

Microsoft ISA Log Configuration Options | 113

Juniper Steel-Belted Radius Log Source Configuration Options | 116

WinCollect Microsoft IIS Log Source Configuration Options

IN THIS SECTION

You can configure a log source to use the Microsoft Internet Information Services (IIS). This WinCollect plugin supports a single point of collection for W3C format log files that are on a Microsoft IIS web server.

Overview for the WinCollect Plug-in for Microsoft IIS

You can use one of two methods to collect Microsoft IIS logs with WinCollect. You can install an agent locally on your Microsoft IIS server and configure it accordingly. Or, with WinCollect 7.2.8 and later, you can configure a WinCollect agent to remotely poll the IIS logs. See Table 1 for setting up the directory paths based off your method of log collection.

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

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

- Network News Transfer Protocol (NNTP) logs

The WinCollect plug-in for Microsofct IIS 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, 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 7.0
- Microsoft IIS Server 7.5
- Microsoft IIS Server 8.0
- Microsoft IIS Server 8.5
- Microsoft IIS Server 10

WinCollect Microsoft IIS Parameters

Table 32: Microsoft IIS parameters

Parameter	Description
Protocol Configuration	Select **WinCollect Microsoft IIS**.
Log Source Identifier	The IP address or host name of your Microsoft IIS server. It must be unique for the log source type.

Table 32: Microsoft IIS parameters *(Continued)*

Parameter	Description
Root Directory	The directory path to your Microsoft IIS log files. For Microsoft 7.0-10.0 (full site), use: • Local: %SystemDrive%\inetpub\logs\LogFiles • Remote: \\HostnameorIP\c$\inetpub\logs\LogFiles For Microsoft IIS 7.0-10.0 (individual site), use: • Local: %SystemDrive%\inetpub\logs\LogFiles\site name • Remote: \\HostnameorIP\c$\inetpub\logs\LogFiles \site name
Polling Interval	The amount of time between queries to the root log directory for new events. The default polling interval is 5000 milliseconds.
FTP	Collects File Transfer Protocol (FTP) events from Microsoft IIS.
NNTP/News	Collects Network News Transfer Protocol (NNTP) events from Microsoft IIS.
SMTP/Mail	Collects Simple Mail Transfer Protocol (SMTP) events from Microsoft IIS.
W3C	Collects website (W3C) events from Microsoft IIS.
WinCollect Agent	Manages the WinCollect agent log source.

For more information about configuring a Microsoft IIS log source, see the *Configuring DSMs Guide*.

RELATED DOCUMENTATION

Microsoft ISA Log Configuration Options | 113

Juniper Steel-Belted Radius Log Source Configuration Options | 116

Microsoft SQL Server Log Source Configuration Options | 117

Microsoft ISA Log Configuration Options

IN THIS SECTION

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

Supported Versions Of Microsoft ISA

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

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

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 Time Management Gateway to write event logs to a log directory.

NOTE: Events that log to a Microsoft SQL server 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. You can customize the W3C event format for the firewall service log and the web proxy log to include or exclude fields from the event logs.

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 33: W3C Format Required Fields

Required field	Description
Client IP (c-ip)	The source IP address.
Action	Action that is taken by the firewall.
Destination IP (r-ip)	The destination IP address.
Protocol (cs-protocol)	The application protocol name, for example, HTTP or FTP.
Client user name (cs-username)	The User account that made the data request of the firewall service.
Client user name (username)	The 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 root directory that you configure in your log source.

When you specify a root log directory, WinCollect evaluates the directory folder and recursively searches the subfolders to determine when new events are written to the event log. By default, the WinCollect plug-in for Microsoft ISA polls the root log directory for updated event logs every 5 seconds.

Table 34: Event Log Default Directory Structure for Microsoft ISA

Version	Root Log Directory
Microsoft ISA 2006	**%systemroot%\LogFiles\IAS\**
Microsoft Threat Management Gateway	***<Program Files>*\<Forefront Directory>\ISALogs\**

Microsoft ISA Protocol Parameters

Table 35: Microsoft ISA 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 JSA.
Root Directory	When you specify a remote file path, use a dollar sign, $, instead of a colon, :, to represent your drive name. 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\\

Table 35: Microsoft ISA Protocol Parameters *(Continued)*

Parameter	Description
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 DOCUMENTATION

Juniper Steel-Belted Radius Log Source Configuration Options | **116**

Microsoft SQL Server Log Source Configuration Options | **117**

NetApp Data ONTAP Configuration Options | **122**

Juniper Steel-Belted Radius Log Source Configuration Options

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

Table 36: Juniper Steel-Belted Radius Protocol Parameters

Parameter	Description
Log Source Type	Juniper Steel-Belted Radius
Protocol Configuration	WinCollect Juniper SBR

Table 36: Juniper Steel-Belted Radius Protocol Parameters *(Continued)*

Parameter	Description
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 JSA.
Root Directory	The directory that contains the files that you want to monitor. The JSA 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.

RELATED DOCUMENTATION

Microsoft SQL Server Log Source Configuration Options | 117

NetApp Data ONTAP Configuration Options | 122

Microsoft SQL Server Log Source Configuration Options

IN THIS SECTION

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

Microsoft SQL Server Error Logs

The error log is a standard text file that contains Microsoft SQL Server information and error messages. WinCollect monitors the error log for new events and forwards the event to JSA. The error log provides 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 Microsoft SQL server error log events. To collect Microsoft SQL Server audit and authentication events, you configure the Microsoft SQL Server DSM. For more information, see the *Configuring DSMs 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 events to JSA.

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

Table 37: Default Root Log Directory Paths Microsoft SQL Events

Microsoft SQL version	Collection type	Root log directory
2012	Local	**C:\Program Files\Microsoft SQL Server \MSSQL11.MSSQLSERVER\MSSQL\LOG 2012 Remote \\SQL IP address\c$\Program Files\Microsoft SQL Server \MSSQL11.MSSQLSERVER\MSSQL\LOG**
2012	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server \MSSQL11.MSSQLSERVER\MSSQL\LOG**

Table 37: Default Root Log Directory Paths Microsoft SQL Events *(Continued)*

Microsoft SQL version	Collection type	Root log directory
2014	Local	**Local C:\Program Files\Microsoft SQL Server \MSSQL12.MSSQLSERVER\MSSQL\LOG 2014 Remote \\SQL IP address\c$\Program Files\Microsoft SQL Server \MSSQL12.MSSQLSERVER\MSSQL\LOG**
2014	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server \MSSQL12.MSSQLSERVER\MSSQL\LOG**
2016	Local	**C:\Program Files\Microsoft SQL Server \MSSQL13.MSSQLSERVER\MSSQL\LOG 2016 Remote \\SQL IP address\c$\Program Files\Microsoft SQL Server \MSSQL13.MSSQLSERVER\MSSQL\LOG**
2016	Remote	**\\SQL IP address\c$\Program Files\Microsoft SQL Server \MSSQL13.MSSQLSERVER\MSSQL\LOG**
2017	Local	**C:\PROGRAM FILES\MICROSOFT SQL SERVER \MSSQL14.MSSQLSERVER\MSSQL\LOG**
2017	Remote	**\\HOSTNAME\C$\PROGRAM FILES\MICROSOFT SQL SERVER\MSSQL14.MSSQLSERVER\MSSQL\LOG**
2019	Local	**C:\PROGRAM FILES\MICROSOFT SQL SERVER \MSSQL15.MSSQLSERVER\MSSQL\LOG**
2019	Remote	**\\HOSTNAME\C$\PROGRAM FILES\MICROSOFT SQL SERVER\MSSQL15.MSSQLSERVER\MSSQL\LOG**

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

Supported Versions Of Microsoft SQL Server

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

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

The following table describes the Microsoft SQL server protocol parameters.

Table 38: Microsoft SQL Server Protocol Parameters

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

Table 38: Microsoft SQL Server Protocol Parameters *(Continued)*

Parameter	Description
Root Directory	Microsoft SQL 2012 - For a local directory path, use **C:\Program Files\Microsoft SQL Server \MSSQL11.MSSQLSERVER\MSSQL\Log** - For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Log** Microsoft SQL 2014 - For a local directory path, use **C:\Program Files\Microsoft SQL Server \MSSQL12.MSSQLSERVER\MSSQL\Log** - For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Log** Microsoft SQL 2016 - For a local directory path, use **C:\Program Files\Microsoft SQL Server \MSSQL13.MSSQLSERVER\MSSQL\LOG** - For a remote directory path, use **\\SQL IP address\c$\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Log** Microsoft SQL 2017 - For a local directory path, use **C:\PROGRAM FILES\MICROSOFT SQL SERVER \MSSQL14.MSSQLSERVER\MSSQL\LOG** - For a remote directory path, use **\\HOSTNAME\C$ \PROGRAM FILES\MICROSOFT SQL SERVER \MSSQL14.MSSQLSERVER\MSSQL\LOG** Microsoft SQL 2019 - For a local directory path, use C:\PROGRAM FILES\MICROSOFT SQL SERVER \MSSQL15.MSSQLSERVER\MSSQL\LOG - For a remote directory path, use \\HOSTNAME\C$\PROGRAM FILES\MICROSOFT SQL SERVER\MSSQL15.MSSQLSERVER \MSSQL\LOG

Table 38: Microsoft SQL Server Protocol Parameters *(Continued)*

Parameter	Description
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 DOCUMENTATION

NetApp Data ONTAP Configuration Options | 122
Bulk Log Sources for Remote Event Collection | 132

NetApp Data ONTAP Configuration Options

IN THIS SECTION

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

Table 39: NetApp Data ONTAP Parameters

Parameter	Description
Log Source Type	NetApp Data ONTAP
Protocol Configuration	WinCollect NetApp Data ONTAP

Table 39: NetApp Data ONTAP Parameters *(Continued)*

Parameter	Description
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. This path is not verified by Juniper Secure Analytics (JSA) user interface. Ensure that you type a valid Windows UNC path that is shared by the NetApp appliance.
Polling Interval	The amount of time between queries to the remote directory for new event log files. Even though the remote device does not generate new files in a period of less than 60 seconds, the optimal polling interval is less than 60 seconds. This practice ensures that the collection of files resumes when WinCollect is restarted.
WinCollect Agent	The WinCollect Agent that you want to use to collect NetApp Data ONTAP events.

Version and File Type Support

- Version:
  - NetApp Data ONTAP 8.x
  - NetApp Data ONTAP 9.x
- Filetype:
  - Windows Event Log (EVT) and (EVTX)

RELATED DOCUMENTATION

Bulk Log Sources for Remote Event Collection | 132

Microsoft SQL Server Log Source Configuration Options | 117

Configuring a TLS Log Source

IN THIS SECTION

To encrypt events and send to JSA, you must configure a log source with a TLS Syslog protocol to establish communication with JSA on port 6514.

1. Log in to JSA.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click **Log Sources** > **Add**.
5. Configure the following parameters:

Table 40: TLS Log Source for Wincollect Destination

Parameter	Description
Protocol Configuration	TLS Syslog
Log Source Identifier	An IP address or host name to identify the log source.
TLS Listen Port	The default TLS listen port is 6514.
Authentication Mode	The mode by which your TLS connection is authenticated. If you select the **TLS and Client Authentication** option, you must configure the certificate parameters.
Client Certificate Path	The absolute path to the client-certificate on disk. The certificate must be stored on the JSA Console or Event Collector for this log source.

Table 40: TLS Log Source for Wincollect Destination *(Continued)*

Parameter	Description
Certificate Type	The type of certificate to use for authentication for the server certificate and server key. Select one of the following options from the **Certificate Type** list: • **Generated Certificate** • **Single Certificate and Private Key** • **PKCS12 Certificate and Password**
Generated Certificate	This option is available when you configure the **Certificate Type**. If you want to use the default certificate and key that is generated by JSA for the server certificate and server key, select this option.
Single Certificate and Private Key	This option is available when you configure the **Certificate Type**. If you want to use a single PEM certificate for the server certificate, select this option and then configure the following parameters: • **Provided Server Certificate Path** - The absolute path to the server certificate. • **Provided Private Key Path** - The absolute path to the private key. **NOTE**: The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.

Table 40: TLS Log Source for Wincollect Destination *(Continued)*

Parameter	Description
PKCS12 Certificate and Password	This option is available when you configure the **Certificate Type**. If you want to use a PKCS12 file that contains the server certificate and server key, select this option and then configure the following parameters: • **PKCS12 Certificate Path** - Type the file path for the PKCS12 file that contains the server certificate and server key. • **PKCS12 Password** - Type the password to access the PKCS12 file. • **Certificate Alias** - If there is more than one entry in the PKCS12 file, an alias must be provided to specify which entry to use. If there is only one alias in the PKCS12 file, leave this field blank.
Max Payload Length	The maximum payload length (characters) that is displayed for TLS Syslog message.
Maximum Connections	The **Maximum Connections** parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. There is a limit of 1000 connections across all TLS syslog log source configurations for each Event Collector. The default for each device connection is 50. **NOTE**: Automatically discovered log sources that share a listener with another log source. For example, if you use the same port on the same event collector, it counts only one time towards the limit.

Table 40: TLS Log Source for Wincollect Destination *(Continued)*

Parameter	Description
TLS Protocols	The TLS Protocol to be used by the log source. Select one of the following options: • TLS 1.2 and above • TLS 1.1 and above • TLS 1.0 and above To avoid security vulnerabilities, use TLS 1.2 and above.
Use As A Gateway Logsource	Sends collected events through the JSA Traffic Analysis Engine to automatically detect the appropriate log source. You must select this in order for JSA to detect/create the correct log source for events. When this option is not selected and **Log Source Identifier Pattern** is not configured, JSA receives events as unknown generic log sources.

Table 40: TLS Log Source for Wincollect Destination *(Continued)*

Parameter	Description

Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, use this option to define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, JSA receives events as unknown generic log sources.
	Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key.
	Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier displays.
	The following examples show multiple key-value pair functions.
	Patterns
	`VPC=\sREJECT\sFAILURE`
	`$1=\s(REJECT)\sOK`
	`VPC-$1-$2=\s(ACCEPT)\s(OK)`
	Events
	`{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}`
	Resulting custom log source identifier
	`VPC-ACCEPT-OK`

Table 40: TLS Log Source for Wincollect Destination *(Continued)*

Parameter	Description
Enable Multiline	Aggregate multiple messages into single events based on a Start/End Matching or an ID-Linked regular expression.
Aggregation Method	This parameter is available when **Enable Multiline** is turned on. • **ID-Linked** - Processes event logs that contain a common value at the beginning of each line. • **Start/End Matching** - Aggregates events based on a start or end regular expression (regex).
Event Start Pattern	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **Start/End Matching**. The regular expression (regex) that is required to identify the start of a TCP multiline event payload. Syslog headers typically begin with a date or timestamp. The protocol can create a single-line event that is based on solely on an event start pattern, such as a timestamp. When only a start pattern is available, the protocol captures all the information between each start value to create a valid event.
Event End Pattern	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **Start/End Matching**. This regular expression (regex) that is required to identify the end of a TCP multiline event payload. If the syslog event ends with the same value, you can use a regular expression to determine the end of an event. The protocol can capture events that are based on solely on an event end pattern. When only an end pattern is available, the protocol captures all the information between each end value to create a valid event.

Table 40: TLS Log Source for Wincollect Destination *(Continued)*

Parameter	Description
Message ID Pattern	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **id-Linked**. This regular expression (regex) required to filter the event payload messages. The TCP multiline event messages must contain a common identifying value that repeats on each line of the event message.
Time Limit	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **id-Linked**. The number of seconds to wait for more matching payloads before the event is pushed into the event pipeline. The default is 10 seconds.
Retain Entire Lines during Event Aggregation	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **id-Linked**. If you set the **Aggregation Method** parameter to **ID-Linked**, you can enable **Retain Entire Lines during Event Aggregation** to discard or keep the part of the events that comes before **Message ID Pattern** when concatenating events with the same ID pattern together.
Flatten Multiline Events Into Single Line	This parameter is available when **Enable Multiline** is turned on. Shows an event in one single line or multiple lines.
Event Formatter	This parameter is available when **Enable Multiline** is turned on. Use the **Windows Multiline** option for multiline events that are formatted specifically for Windows.

6. Click **Save**.

Creating a TLS Log Source Destination for Managed Agents

Create a TLS destination if you want to send encrypted events to JSA appliances. For any existing log sources that are using WinCollect you must ensure that they use the TLS destination you created so that the events are encrypted.

1. Click the **Admin** tab.
2. Create a TLS log source destination.
   a. Click **Data Sources** > **WinCollect**.

   b. In the **WinCollect** window, click **Destinations** > **Add**.

   c. Give the destination a name, and specify the IP address or hostname of the console.

   d. In the **Protocol** menu, select **TCP/TLS (Encrypted)**.

   e. Paste the certificate, including the BEGIN and END lines.

      Find the self-signed certificate in **/opt/qradar/conf/trusted_certificates/syslog-tls.cert**.

   f. Click **Save**.
3. Create a TLS Syslog log source where the log source type is **Universal DSM** and the protocol type is **TLS Syslog**.

RELATED DOCUMENTATION

NetApp Data ONTAP Configuration Options | 122

Bulk Log Sources for Remote Event Collection | 132

Adding a Log Source to a WinCollect Agent

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

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.

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.
   - For a WinCollect plug-in select the WinCollect plug-in option from the **Log Source Type** list, and then configure the 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**.

RELATED DOCUMENTATION

Microsoft DHCP Log Source Configuration Options | **97**

DNS Debug Log Source Configuration Options | **101**

File Forwarder Log Source Configuration Options | **105**

Bulk Log Sources for Remote Event Collection

IN THIS SECTION

Bulk log sources are designed for systems that have multiple log sources with the same protocol configuration.

1. Create a destination for Windows events on each JSA appliance that you want to use for Windows event collection. See "Adding a Destination" on page 58.

> **NOTE**: It is helpful to provide a destination name that includes the IP address, such as "Agent1_1.2.3.4". If you have to edit the log source and change a destination in the future, you can determine the IP address for the destination. Also, set the throttle value to 5000 EPS, which is the max EPS rate for a WinCollect agent.

2. Create bulk log sources. See "Adding Log Sources in Bulk for Remote Collection" on page 133.

3. Wait for the configurations to be pushed to the remote agents.

4. Verify in the **Log Activity** tab that events being received.

Adding Log Sources in Bulk for Remote Collection

You can add multiple log sources at one time in bulk to JSA. 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 take time for the WinCollect agent to access and collect all Windows events from the log source list.

Ensure that you created destinations so that WinCollect agents can send Windows events to JSA appliances. Ensure that you created one destination for each JSA Event Collector 16xx or 18xx appliance.

Plan your bulk collection strategy with the WinCollect Event Log Report tool.

You can have a maximum of 500 log sources for each managed WinCollect agent. You must also remain under 5,000 EPS for local collection and 2,500 EPS for remote polling on the WinCollect Agent. You can review the Event Viewer on the Windows systems to determine how many EPS are generated in each hour. Divide that value by 3600 seconds to get the EPS rate. This calculation helps you to plan how many agents you need to install. Alternately, look at events over a 24-hour period to see how busy each Windows server is. This helps determine how to tune agents and avoid minimum and maximum EPS rates that you see only when reviewing hour-by-hour.

1. On the **Admin** tab navigation menu, click **Data Sources**, and then click the **WinCollect** icon.

2. Select the WinCollect agent that you want to assign log sources to, and click **Log Sources**.

3. Click **Bulk Actions >Bulk Add**.

4. Provide a name for the bulk log source. To make it easy to locate, specify the name as the WinCollect agent that does remote collection.

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

6. From the **Protocol Configuration list** box, select **WinCollect**.

7. Use the tuning value specified by the WinCollect Event Log Report tool to tune your log sources appropriately.

8. Select all of the **Standard Log Types** check boxes. The WinCollect agent reads and forwards these remote logs to JSA.

   NOTE: Do not select **Forwarded Events** the check box. Forwarded events is a special use case. Selecting this option will not add multiple log sources correctly.

9. Select all of the **Event Types** check boxes.

10. Select the **Enable Active Directory Lookups** check box. This option identifies user names in Windows events that appear as a hexadecimal and resolves them to human readable user names.

11. From the **WinCollect Agent** list, select the Windows host that manages the log source.

12. From the **Target Internal Destination** list, select the JSA appliance that receives and processes the Windows events.

13. Add the IP addresses for the Windows operating systems that you want to remotely poll for events.

    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 take time for the WinCollect agent to access and collect all Windows events from the log source list.

14. Click **Save** and then click **Continue**.

Wait for the configurations to be pushed to the remote agents. Verify in the **Log Activity** tab that events are received.

RELATED DOCUMENTATION

Microsoft SQL Server Log Source Configuration Options | 117

NetApp Data ONTAP Configuration Options | 122

7

CHAPTER

Troubleshooting WinCollect Deployment Issues

Troubleshooting WinCollect Deployment Issues

If you experience issues with your WinCollect deployment, the following information might help you identify and resolve the issues.

In a complex WinCollect deployment with many assets, identifying the source and cause of problems can be difficult. Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and explain how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the WinCollect Support representative know where to start to find the cause of the problem. This step includes asking some basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, and that is the best way to start down the path of problem resolution. After you have a clear description, you can investigate the cause of and solution to the problem, or contact WinCollect Support to assist you in the investigation.

Where to get help

Troubleshooting is not the same as problem solving, although during the process of troubleshooting, you can often obtain enough information to solve a problem. However, sometimes you might encounter a problem that you cannot solve by yourself, even after you determine its cause. If you are unable to solve a problem on your own, you can contact WinCollect Support for a solution.

RELATED DOCUMENTATION

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | 137

The Statistics Subsystem | 139

Event ID 1003 Splits the Message in JSA | 139

WinCollect Files are Not Restored During a Configuration Restore | 141

Windows 10 (1803) Cannot Read the Security Bookmark File | 141

Common Problems

The following topics describe some known problems that can occur in a WinCollect deployment, and provide solutions to those problems.

- "Replacing the Default Certificate in JSA Generates Invalid PEM Errors" on page 137
- "The Statistics Subsystem" on page 139
- "Event ID 1003 Splits the Message in JSA" on page 139
- "WinCollect Files are Not Restored During a Configuration Restore" on page 141
- "Windows 10 (1803) Cannot Read the Security Bookmark File" on page 141
- "Resolving Log Source Error After WinCollect Update" on page 142

If your problem is described here, you can try these solutions before you need to contact Juniper Customer Support.

RELATED DOCUMENTATION

Replacing the Default Certificate in JSA Generates Invalid PEM Errors

Replacing the default certificate in JSA causes the `ConfigurationServer.PEM` file to change, affecting all WinCollect agents in the deployment. To fix this issue, you must replace the `ConfigurationServer.PEM` file on the Windows host.

WinCollect agents receive rejection messages because the incorrect certificate is passed when the agents attempt to communicate with the updated JSA appliance. The following error message appears in the logs:

```
May 17 17:06:31 ::ffff:IP ADDRESS [ecs-ec] [WinCollectConfigHandler_4]
com.q1labs.sem.semsources. wincollectconfigserver.WinCollectConfigHandler:
[ERROR]
[NOT:0000003000] [192.0.2.0/- -] [-/- -]Agent with ip: IP ADDRESS tried to
connect
with an invalid PEM
```

The IP address of the agent that is attempting to communicate is displayed. The WinCollect agent also sends LEEF Syslog messages to inform the administrator of the communication issue due to the invalid certificate. To fix this issue, you must replace the `ConfigurationServer.PEM` file on the Windows host.

NOTE: This action must be completed by a Windows administrator or a user that has privileges to delete files from the remote Windows host.

1. Open a remote desktop connection to the WinCollect Agent that is unable to communicate.
2. Click **Start** > **Run**.
3. Type `services.msc`, then click **OK.**
4. Stop the WinCollect service.
5. On the Windows host, navigate to the WinCollect configuration folder.

   By default, the folder path is: **C:\ProgramFiles\IBM\WinCollect\config**
6. Delete `ConfigurationServer.PEM`.
7. From the **Services** window, start the WinCollect service.

RELATED DOCUMENTATION

The Statistics Subsystem | **139**

Event ID 1003 Splits the Message in JSA | **139**

WinCollect Files are Not Restored During a Configuration Restore | **141**

Windows 10 (1803) Cannot Read the Security Bookmark File | **141**

Resolving Log Source Error After WinCollect Update | **142**

The Statistics Subsystem

The Statistics Subsystem collects events per second (EPS) data from all log sources and destinations in a single text file.

The system creates the **logs\Statistics.txt** file and populates it with collected EPS statistics every 5 minutes.

When the Agent starts, it writes the first set of collected statistics to the end of the `Statistics.txt` file, leaving older statistics intact. The system then writes the content at the same location with new statistics every 5 minutes.

You can change the interval at which new statistics are reported in the `logconfig.xml` file. The `ReportEvery` parameter specifies the number of minutes between each report. The default value is 5 minutes

RELATED DOCUMENTATION

Event ID 1003 Splits the Message in JSA | **139**

WinCollect Files are Not Restored During a Configuration Restore | **141**

Windows 10 (1803) Cannot Read the Security Bookmark File | **141**

Resolving Log Source Error After WinCollect Update | **142**

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | **137**

Event ID 1003 Splits the Message in JSA

Windows Event ID 1003 can exceed the default maximum payload size in JSA. It is then split into two separate messages.

The default maximum payload size in JSAis 4096 bytes. If Event ID 1003 messages are being split, you must increase the maximum payload size to keep the messages intact.

Follow these steps to increase the maximum payload size:

1. Log in to the Console as an administrator.

2. Click the **Admin** tab.

3. Click **System Settings** > **Advanced**.

4. On the System Settings pane, update the **Max TCP Syslog Payload Length** value to 8,192.

   NOTE: Extremely large payload values can impact performance of the event pipeline. Do not increase the TCP Payload Length Value above 8,192 bytes without contacting Juniper support.

5. Click **Save**.

6. On the Admin tab, click **Advanced > Deploy Full Configuration**.

   NOTE: Completing a full deployment restarts all services on all JSAappliances. Verify whether reports are running before you run the deployment, as a full deployment stops reports that are in progress. These reports must be manually restarted by a user or the administrator. This procedure also temporarily stops event and flow collection on all appliances while services are restarting. To avoid these issues, make this change during a maintenance window.

7. Click **Continue** to start the full deployment process.

   After the deployment completes, all JSA managed hosts are sent the change to accept larger TCP payload length. The payloads across all managed hosts do not truncate the event message, unless they exceed 8,192 bytes.

RELATED DOCUMENTATION

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | **137**

WinCollect Files are Not Restored During a Configuration Restore | **141**

Windows 10 (1803) Cannot Read the Security Bookmark File | **141**

Resolving Log Source Error After WinCollect Update | **142**

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | **137**

The Statistics Subsystem | **139**

WinCollect Files are Not Restored During a Configuration Restore

When you complete a configuration restore and some WinCollect files are not restored, it might be because the installation ISO contains a previous version of WinCollect.

The JSA ISO contains a built-in version of WinCollect. When you restore by using that ISO, it deploys the WinCollect files that are stored in that ISO, rather than the files from your backup.

To remedy this issue, you must install the WinCollect SFS that matches the version of WinCollect in your backup before you restore the configuration. Perform the following tasks in this order:

1. Perform JSA backup.
2. Bring new hardware online and deploy the ISO.
3. Install the WinCollect SFS that matches the version of WinCollect in your backup on the Console.
4. Restore the configuration backup.

   The appropriate WinCollect files are deployed with the configuration restore.

RELATED DOCUMENTATION

Windows 10 (1803) Cannot Read the Security Bookmark File | **141**

Resolving Log Source Error After WinCollect Update | **142**

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | **137**

The Statistics Subsystem | **139**

Event ID 1003 Splits the Message in JSA | **139**

Windows 10 (1803) Cannot Read the Security Bookmark File

Log sources for Windows 10, build 1803 fail to read the Security Bookmark file after the host is restarted.

This is a known issue with Windows 10, build 1803. After you install WinCollect and restart the computer, the log source can fail to read the Security Bookmark file.

To fix this issue on WinCollect 7.2.5, edit any log sources that are experiencing the issue with an XPATH that includes the Security event log and any other channels that you're monitoring.

To fix this issue on WinCollect 7.2.6 or later, edit the log source to use MSEVEN6.

RELATED DOCUMENTATION

Resolving Log Source Error After WinCollect Update | 142

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | 137

The Statistics Subsystem | 139

Event ID 1003 Splits the Message in JSA | 139

WinCollect Files are Not Restored During a Configuration Restore | 141

Resolving Log Source Error After WinCollect Update

An error message might appear when you attempt to edit a log source after you upgrade WinCollect, JSA, a Device Support Module (DSM), a protocol, or any Vulnerability Information Services (VIS) components. To remove cached files, restart the JSA web service and clear the JSA files from your browser cache.

You must have SSH access and root account credentials.

The following message indicates that the web server didn't restart after JSA was updated:

```
An error has occurred. Refresh your browser (press F5) and attempt the action again.

If the problem persists, please contact Juniper Customer Support for assistance.
```

A file might be cached by JSA web service or your desktop browser. You must restart JSA web service and remove the cached files on your desktop.

1. Use SSH to log in JSA.

2. Stop the JSA web service by typing the following command:

   service tomcat stop

3. Keep one web browser window open.

4. To clear your browser cache, go to your web browser's preference settings.
5. Restart the browser.
6. Restart the JSA web service by typing the following command:

   service tomcat stop

RELATED DOCUMENTATION

Replacing the Default Certificate in JSA Generates Invalid PEM Errors | 137

The Statistics Subsystem | 139

Event ID 1003 Splits the Message in JSA | 139

WinCollect Files are Not Restored During a Configuration Restore | 141

Windows 10 (1803) Cannot Read the Security Bookmark File | 141

WinCollect Log File

IN THIS SECTION

The WinCollect log file provides information about your deployment. Logs provide valuable information for troubleshooting issues.

WinCollect Log Overview

WinCollect generates log event extended format (LEEF) messages during installation and configuration and writes them to a single log file. The server in the **Status Server** field receives the LEEF messages through the syslog. These messages report on the status of the WinCollect service, authorization token, configuration, and more.

Example:

The following example displays a LEEF message that alerts administrators that the WinCollect agent is generating more events than the log source is tuned for.

```
<13>Sep 22
09:07:56 IPADDRESS LEEF:1.0|IBM|WinCollect|7.2|3|src=MyHost.example.com
dst=10.10.10.10
sev=4 log=Device.WindowsLog.EventLog.MyHost.example.com.System.Read
msg=Reopening event log
due to falling too far behind (approx 165 logs skipped). Incoming
EPS r.avg/max =
150.50/200.00. Approx EPS possible with current tuning = 40.00
```

You search for syslog messages by using the IP address of the WinCollect agent. JSA tracks information from the audit log to determine when log sources are created, when searches are run, and so on.

WinCollect Log Types

WinCollect Log Types

The default log directory is **C:\Program Files\IBM\WinCollect\logs\**. The log file is named `WinCollect.log`.

Each log entry is tagged with an identifier that indicates the entry type:

- System
- Code
- Device

The following table describes the types of log entries in the WinCollect log file.

Table 41: WinCollect Log Types

Subfolder	Description
System	Indicates system information, such as the operating system that the agent is installed on, RAM and CPU information from the operating system, service start-up information, and WinCollect version information.

Table 41: WinCollect Log Types *(Continued)*

Subfolder	Description
Code	Indicates information about for spillover and cache messages, file reader messages, authorization token messages, IP address or host name information for the local host, issues with destinations, log source auto-creation, stand-alone mode messages, and thread or process start-up and shutdown messages. Use these entries to investigate the WinCollect configuration. This log does not provide information about event collection.
Device	Created when WinCollect collects events, the protocols that run event log collection. The following issues are logged as device entries:: Loading Plug-in Connection issues Permission or Authentication Windows error codes (hex value codes provided by the operating system, such as 0x000005 access denied) File path or location Event log is overdue to be polled Event log transactions RPC is unavailable (unable to find the location that you specified) Reopening due to falling too far behind (tuning messages)

Disk Space Management for Log Files

WinCollect manages disk space for logs by generating a ".1" version when the log size exceeds 20 MB. After a ".5" version is created, WinCollect deletes the oldest version of the log.

WinCollect also manages disk space by archiving checkpoint folders. When JSA updates WinCollect with new code, the checkpoint folders store a backup of the replaced code. WinCollect archives the oldest patch checkpoint folder after 10 are created. WinCollect creates an archive folder that contains a list of files in the patch checkpoint folder, and a compressed file of the AgentConfig.xml file. WinCollect then deletes the patch checkpoint folder that it archived.

InfoX Debug Logs

InfoX debug logs make debugging WinCollect easier, without interfering with performance.

By default, InfoX is enabled and logs events for the first five minutes that the agent runs, for a maximum of 5,000 log entries. After that, InfoX logs events for one minute every 15 minutes, for a maximum of 200 log entries. InfoX generates debug logs even if your log level is set to info.

You can edit the InfoX configuration by adding any of these parameters to the **install_config.txt file**.

Table 42: InfoX Configuration Options

Parameter	Description
InfoX.enabled	Used to enable or disable InfoX. Example: InfoX.enabled=true
InfoX.startLen	The number of seconds to run the agent at startup. To disable this feature, set this value to 0. Example: InfoX.startLen=300
InfoX.startMax	The maximum number of events that can be logged at startup. Example: InfoX.startMax=5000
InfoX.nextWait	The number of seconds to wait for the next logging period. Example: InfoX.nextWait=900
InfoX.nextLen	The number of seconds to run the agent at each interval. To disable this feature, set this value to 0. Example: InfoX.nextLen=60
InfoX.nextMax	The maximum number of events that can be logged at each interval. Example: InfoX.nextMax=200

RELATED DOCUMENTATION

Adding Custom Entries to WinCollect Status Messages | **62**

WinCollect Destinations | **58**

Configuration Options for Systems with Restricted Policies for Domain Controller Credentials | **76**