opentext™

ArcSight SmartConnectors

Software Version: 8.4.3

Recommendations for Windows Event Log Collection

Document Release Date: October 2023
Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Recommendations for Windows Event Log Collection 4

Overview 5

Microsoft Windows Event Log - Native (WiNC) 5

Windows Event Log SmartConnector (WiSC) 5

Windows Event Log Collection Best Practices 6

Option 1: Use WiNC SmartConnector as a Log Aggregator 6

Option 2: Use WiNC in a WEC or WEF Environment 6

Useful References 7

Send Documentation Feedback 8

Recommendations for Windows Event Log Collection

Over the years, OpenText has released multiple SmartConnectors to collect event logs from Microsoft Windows OS and Microsoft Active Directory environments.

A short summary and deployment considerations are provided in this document.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors 8.4.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

Overview

At this time, we *only* recommend using the WiNC SmartConnector for production environments, because of the limitations with WiSC options that are listed below.

Microsoft Windows Event Log - Native (WiNC)

WiNC is a next-generation SmartConnector that supports native event log collection, using the .NET framework.

Pros:

- It is scalable.
- It provides high performance event log collection.

Cons:

- It can only be deployed on Windows Server operating systems.

Windows Event Log SmartConnector (WiSC)

WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. We have experienced the following issues.

- **High CPU utilization on the monitored Windows host (log endpoint)**

  High CPU utilization has been detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average).

- **WinRM inherent EPS limitations**

  Given the circumstances with WinRM, the event rate has a limit of around 140 EPS (sustained). Therefore, we do not recommend the use of the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates.

Windows Event Log Collection Best Practices

Use the Windows Native Connector (WiNC) SmartConnector, as detailed below.

Windows Native Connector is our recommended deployment option, while we are investigating a long-term solution to have a SmartConnector running on Linux operating systems.

Option 1: Use WiNC SmartConnector as a Log Aggregator

WiNC SmartConnector is a high-performance SmartConnector that can handle large EPS volumes. See the *"SmartConnector for Microsoft Windows Event Log – Native 'Configuration Guide'"* for detailed implementation steps.

Option 2: Use WiNC in a WEC or WEF Environment

Windows Event Collection (WEC) and Windows Event Forwarding (WEF) are native Microsoft technologies that support Windows event log collection in a Windows environment.

WiNC SmartConnector is capable of collecting "Forwarded Events or Other WEC Logs from Local Or Remote Hosts". As such, you may consider deploying a suitable Windows Event Forwarding architecture for your organization.

WiNC can be deployed in the following ways:

- Directly on WEF aggregation point (WEC Server)
- Remotely on another Windows Server, to connect and collect forwarded events from one or many WEC Server(s).

As a result, the footprint of the ArcSight WiNC SmartConnector can be optimized depending on your architectural goals.

Useful References

For more information on using WiNC in a WEF environment, please check the following document:

Collecting Windows Event Logs Using Windows Event Forwarding

For more information on Windows Event Forwarding, please check the following documents:

Windows Event Collector

Use Windows Event Forwarding to help with intrusion detection

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Recommendations for Windows Event Log Collection (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!