Micro Focus Security ArcSight Recommendations for Windows Event Log Collection

Technical Note

Document Release Date: September 13, 2019

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Version	Date	Description
1.2	09/13/2019	A typo was corrected on page 4. Typo: Because of the issues with WUC and WiNC as described above, we *only* recommend using the WiNC SmartConnector for production environments. Corrected text: Because of the issues with WUC and WiSC as described above, we *only* recommend using the WiNC SmartConnector for production environments.
1.1	09/12/2019	Document updated to provide an overall recommendatios of WiNC over WUC and WiSC options
1.0	07/24//2019	First edition of this technical note

Contents

Overview

Over the years, Micro Focus 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 below.

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

WUC (Windows Unified Connector)

WUC is a first generation SmartConnector that can be deployed on both Windows and Linux platforms. It can also run on ArcMC Connector Hosting appliance.

Pros:

- It can run on ArcMC Connector Hosting appliance.

Cons:

- It only supports SMB v1 protocol. This is known to be an insecure protocol.

WiNC (Windows Native Connector)

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.

WiSC (Windows SmartConnector running on Linux platforms)

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/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 Technical Note (Recommendations for Windows Event Log Collection 1.2)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!