Micro Focus Security ArcSight SmartConnector for Microsoft Windows Event Log (WiSC)

Technical Note on WinRM-related Issues

Document Release Date: July 24, 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
1.0	07/24//2019	First edition of this technical note

Contents

Overview

The infrastructure provided with the SmartConnector for Microsoft Windows Event Log has been improved to deliver critical features such as Operational Windows Event Logs and event collection and event filtering from IPv6 hosts. It leverages the native technology on the Microsoft platform and provides the best support for Windows event features and capabilities (including collection for all log types).

Even though, WiSC can be deployed on supported Linux operating systems, we have been experiencing some performance 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.

Workaround: To mitigate these issues, we recommend using the Windows Native Connector (WiNC) SmartConnector

Recommended Mitigation Steps

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.

Workaround 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.

Workaround 2: Use WiNC in a WEC/WEF 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, and for every WEF aggregation point (WEC Server), you may consider deploying a WiNC SmartConnector on it directly, or remotely connect and collect forwarded events from it. In this way, you can minimize the footprint of the ArcSight WiNC footprint, 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 on WinRM-related Issues (SmartConnector for Microsoft Windows Event Log (WiSC) 1.0)

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!