

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

© Copyright 2019 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

US Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the US Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the US Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This US Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 4
- High CPU utilization on the monitored Windows host (log endpoint) 5
- WinRM inherent EPS limitations 5
- Recommended Mitigation Steps 6
 - Workaround 1: Use WiNC SmartConnector as a Log Aggregator 6
 - Workaround 2: Use WiNC in a WEC/WEF Environment 6
- Useful References 7

- Send Documentation Feedback 8

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@microsoft.com.

We appreciate your feedback!