Micro Focus Security ArcSight Investigate

Software Version: 2.40

Release Notes

Document Release Date: July, 2019
Software Release Date: July, 2019

Legal Notices

Copyright Notice

© Copyright 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.

U.S. 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 U.S. 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 U.S. 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 U.S. 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 U.S. 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

Contents

Supported Platforms and Browsers

For details on browser support, refer to the Investigate Deployment Guide.

What's New in this Release

- Data ingestion performance improvements to the Vertica Kafka Scheduler now support hundreds of thousands of Events-per-Second ingestion rates in a multi-node Vertica cluster.
- Significant search speed performance improvements have been achieved
  - Database locale now defaults to case sensitive searching, greatly improving search speeds. While your speed increases may vary, testing has shown improvements between 17 times faster on a 3-node Vertica cluster to 164 times faster on a 14-node Vertica cluster.
  - Hybrid text indexing improvements, including removal of unnecessary columns.
  - More efficient INTEGER column casting results in far less disk storage required for NULL INTEGER values.
- Support for the latest Container Deployment Foundation (CDF) code-base.
  - The 'Arcsight Installer' process is replaced by the native CDF Installer process.
  - Installation uses the latest CDF release, improving stability and manageability from prior CDF releases.
  - Customers can now choose infrastructure size from a single, shared Worker Node to 10 or more nodes.
  - Upgrades to future releases from version 2.40 and patches/hotfixes are now supported in the native CDF Installer, using rolling upgrades through the nodes in the cluster.
  - Installation can use a non-root USER.

    - Changing execution parameters results in a rolling stop/restart of cluster pods to enable the new settings.
    - Supports FIPS at the OS level
- Wizard-based Container Installer - A far-simpler and more intuitive, wizard-based Installer. Fewer initial configuration properties, with appropriate defaults and allows post-deployment reconfigurations.
- Completely rewritten documentation. A new CDF Planning Guide used to set up the infrastructure OS, network and storage, and a reorganized and rewritten Deployment Guide now contain explicit instructions and more samples and diagrams.
- Due to the adoption of the native CDF Installer and significant Vertica improvements, a fresh Investigate install is required

Fixed Issues

This release addresses the following issues:

Issue	Description
CPEA-1067	Investigate UI search speed has been improved.
CPEA-927	Vertica and the scheduler are now able to handle multiple simultaneous COPYs from Kafka at great scale.
HERC-7989	This release resolves an issue where in some cases, when in Firefox, dragging a field will not be shown in the Chart Parameters box.
HERC-7690	This release resolves an issue where the incoming ports were displaying the data while overlaying the Distinct Port count.
HERC-7181	This release resolves an issue where Id was displayed as one of the Outlier features.
HERC-7153	This release resolves an issue where Investigate generated exceptions when attempting to edit filter criteria on the Outlier Configuration page.
HERC-6988	This release resolves an issue where the right side of the Outlier Analytics page was not displayed correctly when using Firefox.
HERC-5821	This release resolves an issue where deleting the search name resulted in the error, "Failed to update".

Open Issues

This release contains the following open issues:

Issue	Description
HERC-8283	When a lookup list has the word "user" it will cause search join to fail. Workaround: None available at this time.
HERC-8220	A search with selected lookup list fields needs the lookup list to be part of a join in the search query. Workaround: None available at this time.
HERC-8184	In Scatter Plot visualization the y axis labels are not readable. Workaround: Hover over each label to read the text.
HERC-8130	UI for ANALYTIC, Vertica Configuration, and Vertica host name are not accepting the FQDN input. Workaround: Use the IP address.
HERC-8047	Empty/null IP/MAC address fields show "double colons" instead of "Null"
HERC-7963	No data is returned when using the "Search For" option to search for "Float" in Investigate. Workaround: When searching on float columns use a range that includes the value you are looking for.The "in between" operator must be used in this case instead of "is equal"
HERC-7827	Deleted saved search remains displayed in 'Saved Results' UI. Workaround: Refresh the browser page.
HERC-7597	The datatype for IP and MAC addresses has changed to byte array. This datatype is larger than the previous string datatype. This may impact the upper limit of the CSV file size and number of records when loading a lookup list. Workaround: Limit the CSV file size to approximately 50MB or limit the number of total IP/MAC addresses in the file to 1 million.

Issue	Description
HERC-7580	Exporting large amounts of data to CSV, makes the application run out of memory and slows download. Workaround: Filter search results and reduce the amount of rows being exported.
HERC-7129	If you create a lookup list using a CSV file with invalid data, Investigate ignores the invalid data and creates the lookup list, but does not notify the user that the CSV file contains invalid data. Workaround None available at this time.
HERC-5844	If you are using Investigate with the Microsoft Edge browser, you cannot export search results to a PDF file. Workaround: Use Mozilla Firefox or Google Chrome.

Known Issues

HERC-7125	For horizontal visualizations that include a category (for example, Login by Destination Address Over Time), Investigate only displays the year on the Y axis and does not include the minute, hour, day, and month details. Workaround To view detailed time information, hover over a value in a bar or zoom in to the cluster.
HERC-5737	Issue: When screen resolution is below 1920x1080, visual elements may not render as expected. Workaround: Set the resolution to 1920x1080 or greater.
HERC-2631	Issue: When pasting a query from an Excel document in Firefox, the new lines are not visible in Search input. Workaround: When pasting a URL that contains special characters from another application, place quotes around the URL. When pasting into Search input, new line symbols are be retained in the pasted text if they do not stand between query language constructs. New lines characters are rendered invisible in Search Input. Thus, you will not be able to see them but they will be taken into account when matching column names and column values, and recognizing other query language constructs.
HERC-8318	Some customers may observe that ingestion of events from the Transformation Hub into Investigate/Vertica occasionally pauses. Such a situation can occur where source devices run with incorrect system clocks or when they produce timestamps (device receipt times) that cannot be parsed correctly and which may have gone unnoticed before the deployment of Investigate. The duration and frequency of the ingestion pauses is dependent upon the extent to which such timestamps deviate more than +/- 2 days from real-time. Extreme cases (event timestamps spanning many days before or after the actual date) could result in a backlog of events beyond the available/configured retention of the TH Avro Topic that feeds Investigate. In such a case, there is a risk that some events may be purged from TH before Investigate/Vertica automatically resumes its ingestion; any events purged from TH will never be consumed in to Investigate. Should such behavior be observed, please contact Micro Focus Support to first validate the cause. While the most effective remediation is to correct such timestamp anomalies at source (this is also needed for effective security event-monitoring), Micro Focus is researching methods to mitigate the effect on Investigate ingestion for a future release.

For information regarding Transformation Hub known issues, refer to the Transformation Hub Release Notes available from the Micro Focus Community.

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 Release Notes (Investigate 2.40)

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!