Micro Focus Security ArcSight Investigate

Software Version: 3.0

Release Notes

Document Release Date: December, 2019
Software Release Date: December, 2019

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

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:

ArcSight Product Documentation on the Micro Focus Security Community

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 (EPS) ingestion rates in a multi-node Vertica cluster.
  - Vertica ROS pushback issues that were causing pauses during ingestion have been addressed. These issues were caused by DeviceReceiptTime (DRT) being invalid (e.g. weeks in the future or years in the past). A new column called NormalizedEventTime (NET) has been introduced which contains either the valid DRT or the current timestamp when the record was added to Vertica if DRT is considered invalid.
- Significant search speed performance improvements
  - 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, and schema changes.
  - More efficient INTEGER column casting results in far less disk storage required for NULL INTEGER values.
- Deployment, configuration and manageability using the Container Deployment Foundation (CDF).
  - Greatly improved product stability and manageability over Investigate 2.30 and prior releases.
  - Wizard-based Installer - A far-simpler and more intuitive, wizard-based Installer. Fewer initial configuration properties, with appropriate defaults and allows post-deployment reconfigurations.

    - Customers can now choose infrastructure size from a single, shared Worker Node to 10 or more nodes.
    - Upgrades to Version 3.0.0 and future releases from Version 2.40 and patches/hotfixes are now supported in the CDF Installer, using rolling upgrades through the Master and Worker Nodes in the cluster.
    - Non-root USER Installation.
    - Changing execution parameters results in a rolling stop/restart of cluster pods to enable the new settings.
    - Supports FIPS at the OS level.
- 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.
- Platform component version updates
    - Support for RHEL 7.7 and CentOS 7.7, and current releases of Apache Kafka Server and Client libraries, Schema Registry, ZooKeeper, Azul Zulu Java runtime, other component libraries and compliance with up-to-date vulnerabilities.
- Supports Brazilian time zone changes.
- Support for Vertica 9.2.1.6.
- Licensing metrics based on Events per Second (EPS) rates are now supported through Micro Focus AutoPass licensing using a Moving Median EPS over a 45-day period. This helps to smooth EPS processing spikes.
- New online help feature supports context-sensitive help for Investigate web pages.

Fixed Issues

This release addresses the following issues:

Issue	Description
HERC-8290	This release resolves an issue where admin users were unable to create another user with the same admin role
HERC-8230	This release resolves an issue where searches using lookup list would display an error if 'Equal' or '=' keywords were used in the join query.
HERC-8199	This release resolved and issue where the context menu (triggered by right click action) on Grid events rows was not displayed for columns: 'Start Time' & 'End Time'.
HERC-8087	This release resolves an issue where lookup list field remained selected after a failed search.
HERC-7183	This release resolves an issue were the scroll down on Filter By dialog (in Visualization feature) caused the loading icon to remain visible.
HERC-7153	This release resolves an issue where filter values could not be edited in the Outlier Analytics page.
HERC-6415	This release resolves an issue where creating a lookup list, if there was an error in the CSV file, the page continued to show the loading icon without displaying an error message.

Open Issues

This release contains the following open issues:

Issue	Description
HERC-8682	Filtering Source Address from Outliers model may show a warning message "Could not refresh widgets" and data on OUTLIER SCORES HISTORY graph will not be displayed. Workaround: Click Detect a few times.
HERC-8665	The warning message "No Outliers Detected. click "DETECT" button. is displayed after selecting "Search" or Profile an IP on Insight > Outliers page. Workaround: Go to Insights > Host Profiler and then go back to Insights > Outliers to display the expected outliers results.
HERC-8678	Online Help requests login credentials twice when using Edge browser. Workaround: Use Mozilla Firefox or Google Chrome.
HERC-8645	Modifying the fieldset and then restoring it creates a new search after clicking play. Workaround: Search time range and query can be restored by navigating to another section as Dashboard and coming back to the search.
HERC-8553	Search cannot be resumed after changing the time range and then setting it back to the original time. Workaround: Navigate to another section such as Dashboard and come back to the search, this will restore Search time range and query
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: Unselect the lookup fields from the fieldset or use the lookup list in the search query.
HERC-8130	UI for ANALYTIC, Vertica Configuration, and Vertica host name are not accepting the FQDN input. Workaround: Use the IP address.
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-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.
HERC-3241	The error "Fix query first" is displayed when using complex special characters in an ESM search. Workaround: When invoking Investigate from ESM with values that contain both single and double quotes, truncate the value in Investigate Search Input after the second quote symbol, e.g. if your ESM value of the Name field is: `my_esm_value'with"single'and"double_quotes` and it got inserted into Investigate as: `Name = 'my_esm_value'with"single'and"double_quotes` truncate it after the single quote: `Name= 'my_esm_value'` and replace = with 'starts with': `Name starts with 'my_esm_value'` After invoking Investigate, remove text starting from the first quote inside the value (the text starting from the second red highlighting in the control). e.g. for the following example: 19@\Aaction@=accept@\Aorig@=167798303@\Ai/f_dir@=outbound@\Ahas_accounting@=0@\Aproduct@=FWM@\AObjectName@=firewall_properties@\AObjectType@=firewall_properties@\AObjectTable@=properties@\AOperation@=Modify Object@\AUid@= Unknown macro: {97AEB653-9AEA-11D5-BD16-0090272CCB30}@\AAdministrator@=Security Management Server@\AMachine@=localhost@\AFieldsChanges@=cluster_id_counter: changed from '0' to '4239' ;@\ASubject@=Object Manipulation@\AOperation Number@=1,-9223372036854775808,-2147483648,-2147483648,"","","","","","" 1) leave: Name = '19@\Aaction@=accept@\Aorig@=167798303@\Ai/f_dir@=outbound@\Ahas_accounting@=0@\Aproduct@=FWM@\AObjectName@=firewall_properties@\AObjectType@=firewall_properties@\AObjectTable@=properties@\AOperation@=Modify Object@\AUid@= Unknown macro: {97AEB653-9AEA-11D5-BD16-0090272CCB30}@\AAdministrator@=Security Management Server@\AMachine@=localhost@\AFieldsChanges@=cluster_id_counter: changed from ' 2) replace '=' with starts with: Name starts with '19@\Aaction@=accept@\Aorig@=167798303@\Ai/f_dir@=outbound@\Ahas_accounting@=0@\Aproduct@=FWM@\AObjectName@=firewall_properties@\AObjectType@=firewall_properties@\AObjectTable@=properties@\AOperation@=Modify Object@\AUid@= Unknown macro: {97AEB653-9AEA-11D5-BD16-0090272CCB30}@\AAdministrator@=Security Management Server@\AMachine@=localhost@\AFieldsChanges@=cluster_id_counter: changed from '

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 3.0)

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!