Micro Focus Security ArcSight Investigate

Software Version: 2.10

Release Notes

Document Release Date: March 30, 2017
Software Release Date: March, 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

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

Introduction

ArcSight Investigate enables you to search, analyze, and visualize machine-generated data gathered from such entities as websites, applications, sensors, and devices that comprise your IT infrastructure or business.

After Investigate ingests the data stream of individual events from Event Broker, you can view and search.

You can use the English-like search language to create searches.

Features and benefits

The following are the main features and benefits of Investigate.

- **Search**

  Search is the primary way to navigate data in ArcSight Investigate. The search is contextual and has auto-suggest capability to help you specify the query input. Therefore, there is no need to learn a complex query language or schema. This can boost the productivity of analysts. Using Vertica, information retrieval is extremely rapid, making a search up to 10x faster than competing products. You can write a search to retrieve events from an index, use statistical commands to calculate metrics and generate charts, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. Data visualization charts can be added to a search in order to better understand search-results data. With Investigate supporting up to 100 concurrent queries, there can be 10 active searches and 40 saved searches per user. You can export a search either as a CSV or PDF file.

- **Indexing**

  ArcSight Investigate indexes machine data. This includes data streaming from packaged and custom applications, application servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors, and so on, that make up your IT infrastructure. The maximum indexing volume depends on the ArcSight Investigate license.

- **Data Analysis**

  ArcSight Investigate enables you to conduct a security investigation by filtering, comparing, visualizing, and analyzing event data dynamically. You are able to expedite the investigation process with quick and easy data analysis, deriving insights without any complexity. ArcSight Investigate provides precise investigation outcomes through pre-defined queries (and fieldsets) for security use cases; therefore, improving SOC efficiency and reducing threat posture.

- **Charting**

You can graphically represent search-results data using the chart editor. This editor enables you to map attributes defined by data-model objects to a chart data visualization without having to write the searches to generate them.

ArcSight Investigate offers two ways to build visualizations: (1) built-in security analytics provides pre-defined visualizations that are configured for specific security use cases, and (2) user-defined visualizations where you can define all of the elements of the visualization, including the type, fields, and functions used.

A chart is saved with a search and can be added to dashboards.

- **Dashboard**

  The dashboard can be comprised of search-results charts or text panels, or a combination of these.

  A chart can either have a fixed start and end date, where data cannot be refreshed, or a chart can have a "canned" date range. For example, for a last-30-minutes "canned" date range, data is updated upon refresh based on the most recent 30 minutes.

- **Host Profiler**

  Host Profiler is a predefined dashboard where you can monitor event traffic for a specified host using visualization widgets. The traffic displayed is for the five most active host ports and communication paths related to other systems. This information can enable you to better analyze events.

Available documentation

In addition to the release notes, the following ArcSight Investigate documentation is available on Protect 724.

Document	Description
MicroFocus Security ArcSight Investigate Deployment Guide	Specifies requirements for Investigate. Describes the technology used in Investigate and how the product works. Also, describes the deployment architect and scenarios. How to deploy and implement Event Broker as part of the solution is also described. "Support Matrix" section provides details on the ArcSight Investigate 2.10 platform, browser support, and supported product compatibility.

MicroFocus Security ArcSight Investigate User's Guide	Addresses the needs of both analysts and administrators. Describes the technology and features used in Investigate and how the product works. Also describes product functions based on workflow.
MicroFocus Security ArcSight Event Broker Administrator's Guide	Describes the technology and features used in ADP Event Broker. Also describes how the product works. Finally, describes how to set up ADP Event Broker in your environment.
ArcSight Investigate 1.0 HDFS Feature Tech Note (beta)	Describes how to automatically archive old data (for example, data older than 90 days) to HDFS and query this data using Investigate. This feature will enable you to periodically archive data based on a predetermined retention period. If you use any HDFS storage locations, the HDFS data must be available at the time you start Vertica. Your HDFS cluster must be operational, and the ROS files must be present. If you have moved data files, or if they have become corrupted, or if your HDFS cluster is not responsive, Vertica cannot start. This feature is for testing only in ArcSight Investigate 1.0. It is not recommended to deploy in production.

Upgrading to ArcSight Investigate 2.10

ArcSight supports an upgrade from ArcSight Investigate 2.01 to version 2.10. Upgrading involves updating the Vertica database, Investigate containers, Event Broker, and ArcSight Installer. Ensure to update the last three of these from the ArcSight Installer (see the MicroFocus Security*ArcSight Event Broker Deployment Guide*).

For upgrade details, see the MicroFocus Security *ArcSight Investigate Deployment Guide*.

ArcSight Investigate issues

Open issues are ones of which we are aware and may be working to resolve.

The following are the type of issues tracked:

- Known — Issues of which we are aware and currently working to resolve.
- Open — Issues of which we are aware and may be working to resolve.
- Fixed — Issues that were resolved in the last product release, which may include Beta.

Known issues

The following known issues apply to this release.

Fixed issues

The following issues are fixed in this release.

General

Issue	Description
HERC-4717	Export to a CSV file was not downloading all events, only a maximum of 500. All events are now downloaded.
HERC-4711	Previously, if you added fields to the fieldset after executing a search, but before creating a chart, the Visual Configurator displayed the new fields. You would encounter an error when using a new field to build a chart. Data for the new field did not exist in the temp table because the search had not been re-executed. This no longer occurs. Now, you will not be presented with the new fields as an option until you re-execute the search.
HERC-4611	Charts now consistently delete after selecting the ellipses (...) > Delete.
HERC-4605	The Timeline now displays the time stamp using a user's local timezone. This is the same behavior as grid and charts as well.
HERC-4571	The Bar Chart Category Parameter is now saved when clicking Save. Likewise, a chart containing the Bar Chart Category Parameter is now auto-saved after navigating away from a search.
HERC-4187	The Configuration > Lookup Lists no longer disappear from the left navigation when you open the Admin page.

Open Issues

This release contains the following open issues.

General

Issue	Description
HERC-5905	Issue: 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. This will be addressed in a future release.
HERC-5902	Issue: Using the right-click menu option, "Get Authenticated Users" from Events table returns an error: "Failed to Execute Search". The cause is that the time is not being passed correctly from the Events table while constructing a search. Workaround: Make a slight modification to the end time and run the search. The search will proceed normally.
HERC-5901	Issue: After deployment or upgrade, browsing to 'https://master-ip' fails in single-master deployments. You may get error such as a 502 or 504 type. Workaround: Delete arcsightinvestigate1 nginx-ingress-controller-* pod and wait for a new pod to be created. If deployment or upgrade still fails, repeat the operation.
HERC-5900	Issue: When you upgrade to Investigate 2.10, if you have not configured a retention policy then the retention policy will be broken due to a missing db_retention_ days=90 in vertica_user.properties. Workaround: After performing the Vertica upgrade, copy the following line from the original vertica.properties file to the config/vertica_user.properties file: db_retention_days=<value> Then, follow the deployment guide instructions to enable and configure the data retention policy.

Issue	Description
HERC-5893	Issue: The "Only show selection" and "Show all" options in the Events table causes the table to be in a bad state. Workaround: None. This option has been temporarily disabled and will be re-enabled in a future release.
HERC-5886	Issue: The drag and drop for IP, MAC, and IPv6 fields from the Events table to filters does not work. Workaround: Instead of using drag and drop, use the right-click option, "Use as a filter" on the desired value. Another option is to type the value in the search field or select it from the field drop down.
HERC-5865	Issue: If you multi-select the saved results from the Saved Results page and then click Delete, an error message appears. Workaround: These errors are benign and do not impact functionality. To prevent the error message from appearing, delete one search result at a time.
HERC-5860	Issue: When selecting any row from the Events table, "Only show selection" appears. When deselecting this row, "Show All" appears. This is a wrong functionality because no rows are selected. The expected behavior is neither label appear. Workaround: Click on "Show All" to make the label disappears.
HERC-5844	Issue: Export search to PDF does not work with Microsoft Edge browser. Workaround: Load the search in a supported browser, then export the search to PDF. This will be fixed in a future release.
HERC-5821	Issue: Deleting the search name results in the error, "Failed to update". Workaround: All searches must be named. Provide a valid text string for the search name.

Issue	Description
HERC-5789	Issue: There is a delay from the time you save a search and when it appears in Saved Results of the left navigation area. Workaround: Refresh the browser to update the Saved Results list.
HERC-5747	Issue: When you export Events table data to a CSV file, the sorting and column positions that you specified in the table is not maintained in the CSV. The data, however, is correct. Workaround: Use a third-party tool on the CSV file to re-apply the event sorting and column order.
HERC-5746	Issue: When you export Event table data to a CSV file, field names for fields that store IP and MAC addresses have the suffix "Bin". Workaround: This affects the header row only. Use a third-party tool to remove the "Bin" string.
HERC-5737	Issue: When screen resolution is below 1920x1080, visual elements may not render as expected. Workaround: Set the monit resolution to to 1920x1080 or greater.
HERC-5706	Issue: A long query for a saved search does not appear cleanly in the Saved Result page. Workaround: To view the full search query, open the search and read the values in the search field.
HERC-5671	Issue: You cannot delete a saved search (left navigation > Saved Results) when there are saved results. Workaround: In the Saved Results page, deleted the saved searches and then delete the session searches.

Issue	Description
HERC-4687	Issue: In the Firefox browser, if you log out of ArcSight Investigate from the Search page, you are not redirected to the login page and an error message appears. Workaround: Navigate from the Search page to Dashboard Page. Then logout from Investigate and the system will display the login page without showing any errors.
HERC-4570	Issue: In some cases, the Category parameter for a bar chart is not auto-saved when navigating to the Dashboard and then back. Workaround: None. This will be fixed in a future release.
HERC-4274	Issue: If you create a bar chart with multiple categories and select a category attribute that contains long text strings, the labels for categories in the chart may become misaligned. Workaround: None. This will be fixed in a future release.
HERC-3836	Issue: For an ESM - ArcSight Investigate integration search, launching Investigate from ESM to search for Empty Device Custom Floating Point values will show the following query in the search query field: deviceCustomFloatingPoint1 = '' , Null The single quotes in this query will not allow the search to run and will display an error. Workaround: Remove the single quote from the query and run the search using the following query: deviceCustomFloatingPoint1 = Null
HERC-3820	Issue: When you search on a value in the Filter By dialog, Investigate may not find the desired value in the initial group of values in the dialog. (This group of values is a subset of the whole data set.) Workaround: If the value is not found, click Search again and Investigate searches on the whole data set. If the desired field is still not found, then the field does not exist in the values available in Filter By dialog.

Issue	Description
HERC-3351	Issue: When field values are empty (zero or NULL), charts are generated empty. This is the expected behavior, but no message appears stating such. Workaround: Though this is the expected behavior, in a future release you will be notified that there is no data to display.
HERC-3338	Issue: In some cases, ESM does an internal calculation on the Severity field which will not be in sync with what shows in ArcSight Investigate. This will cause a search to fail . Workaround: None. The issue will be fixed in a future release.

Issue	Description
HERC-3241	Issue: For an ESM search, you cannot search for the Name field using complex special characters without receiving the error, "Fix query first" 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 you 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 '

Issue	Description
	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 '
HERC-2631	Issue: Error 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-2132	Issue: If the user make a column sticky and then drags that column to use all the grid space. Then user cannot resize the sticky column back and it continues to occupy the entire grid space. Workaround: Unstick the stick column and it will resize this column and will show all the other grid columns

Issue	Description
INST-1163	Issue: You may not be able to login with the correct username and password and receive the error message "Failed to handle token". Workaround: Delete the idm-postgresql pod.
INST-1143	Issue: The Zookeeper cluster is out of sync at times and Kafka failed to select a leader after losing multiple brokers, which causes Kafka to fail. The problem occurs on Zookeeper startup, due to a timing problem. It also occurs on a Zookeeper cluster, due to an unknown reason. Workaround: Undeploy and redeploy the Event Broker.
INST-1118	Issue: User is never logged out when browser is on deployment page Workaround: Move to a different page

Installation

Issue	Description
INST-1071	Issue: When adding a node to the cluster, you get the error: `Cluster status check failed, [MngPortal] URL: https://172.16.29.8:9090 Inactive` Workaround: Re-run ./arcsight-installer-add-node.sh 15.214.137.1
INST-797	Issue: The pod statuses displayed on the UI do not always correspond to the ones you can see running 'kubceclt get pods'. The pod statuses displayed in the UI (at the moment) could be - Running, Pending, Failed. The statuses you see in kubectl are the container statues which are in most of the cases will be transformed to Pending or Running in the UI. Workaround: None.

Search

Issue	Description
HERC-5888	Issue: For all charts with Bytes in and Bytes out fields having null values, the charts are not rendering after refreshing in the Dashboard page. Workaround: Change the time range and/or query again to try to get no null data.
HERC-5863	Issue: The pie chart does not draw due to an NaN error with plotly on correlated null values with Filter By. Steps to reproduce: 1. Add Pie chart. 2. Measure: Bytes Out. 3. Label: Device Vendor. 4. Filter By: Device Vendor. 5. Open Filter By and select a value that shows as 0% in the preview, such as "Arcsight". The pie chart does not render, or shows as blank. The console log shows an NaN error thrown by Plotly.js. Workaround: If you search for the field in the Measure parameter *(*Bytes Ou*t), not including null values, this error does not occur.
HERC-5026	Issue: Getting authenticated users using null or empty values results in a bad query. For instance, if you select an empty IP or host field to get authenticated users, then the query generates with 0. Wrong query: Agent Address = (Null) and Category Behavior = /Authentication/Verify and Category Outcome = /Success Correct query: Agent Address = Null and Category Behavior = /Authentication/Verify and Category Outcome = /Success Workaround: Manually remove brackets and rerun the query.

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 2.10)

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 arc-doc@hpe.com.

We appreciate your feedback!