MICRO FOCUS

Release Notes

ArcSight Recon 1.4 Release Notes

February 2022

ArcSight Recon includes new features, improves usability, and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input.

We hope that you continue to help us ensure that our products meet all your needs. We want to hear your comments and suggestions about the documentation available with this product. If you have suggestions for documentation improvements, click Send Us Feedback at the bottom of the page in the HTML version of the documentation posted at the Recon Documentation page.

This release also includes Recon capabilities. Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database. Recon deploys within the **ArcSight Platform**. For more information about the other products available within the suite, see the *Release Notes for ArcSight Platform 22.1*.

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website, well as context-sensitive user guides within the product. If you have suggestions for documentation improvements, click Send Us Feedback at the bottom of the page in the HTML version of the documentation posted at the Recon Documentation page.

What's New

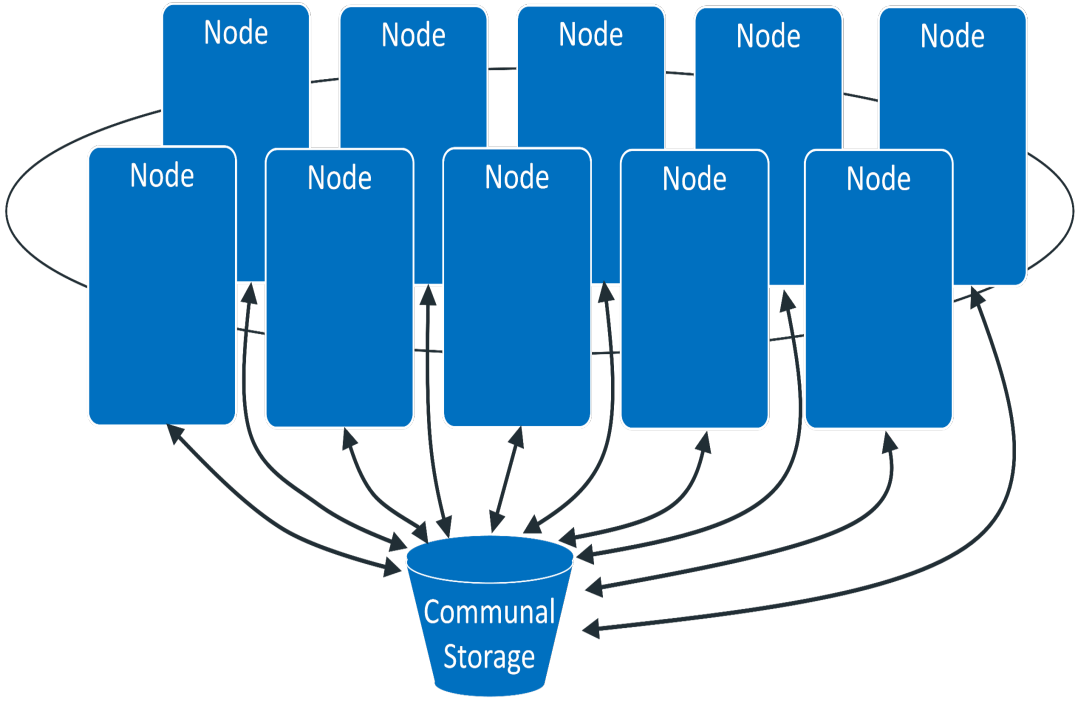
Monday, February 14, 2022

This release includes the following features, enhancements, and software fixes:

Enhancement to the ArcSight Database

This version of the ArcSight Database separates computing from storage to provide an intelligent and cost-effective way of storing security event data for the long term. Basically, instead of storing data locally, the database will use a single communal storage location for all data and metadata. **Communal storage** is the database's centralized storage location, shared among the database nodes. Communal storage is based on an object store, such as Amazon's S3 bucket in the cloud or a storage device for an on-premises deployment. The database relies on the object store to maintain the durable copy of the data.

Why is this new solution better? When using traditional database storage, the database nodes in your cluster store all the data for the retention period. Traditionally, as the ingestion rate and retention period increases, you must increase the number of database nodes. However, with this new solution, you don't need to add more database nodes as the retention period grows. Instead, you can increase the size of the communal storage, which is significantly less expensive to expand than adding database nodes. To expand communal storage, you purchase additional storage devices without purchasing additional CPU and memory.



The database keeps the primary copy of your data in the communal storage, and the local cache serves as the secondary copy. This means that adding and removing nodes does not redistribute the primary copy. This shared storage model enables elasticity, meaning it is both time and cost effective to adapt the cluster resources to fit the usage pattern of the cluster. If a node goes down, other nodes are not impacted because of shared storage. Node restarts are fast and no recovery is needed. Thus, you do not need to keep track of and load/unload long- term retention event data explicitly. The ArcSight Database can bring them to the cache on demand automatically then move data out when not in use.

Within communal storage, data is divided into portions called **shards**. Shards are how the database divides the data among the nodes. Nodes subscribe to particular shards, with subscriptions balanced among the nodes. When loading or querying data, each node is responsible for the data in the shards it subscribes to.

To take advantage of this capability, you must install a new version of the database. You cannot upgrade from a previous version.

Event Integrity Check Feature Now Reviews More than 20 Event Fields

This release expands the usefulness of the **Data Reviewed by the Event Integrity Check**, which helps you identify whether event data might be compromised. Previously, you could check the raw event data received from SmartConnectors. Now you can enable Transformation Hub to generate more than 20 fields within an event, such as *deviceProduct* and *sourceHostName*. In addition to the raw event data for each event, the Event Integrity Check will validate these **parsed fields** generated by Transformation Hub.

Reporting Enhancements

This release provides

Save Search Queries and Criteria

This release provides

Enhancements to the Data Quality Dashboard

The Data Quality Dashboard provides detailed information about the gap between Device Receipt Time (DRT) from the raw event itself versus the Normalized Event Time (NET) and Database Receipt Time (dBRT). Based on the information analyzed through the Data Quality Dashboard, you can accurately mitigate the problem. This release expands the range of categories for the results to help you identify the sources that cause issues with the data:

- **Active Events** that have a timestamp within the database's active time frame where NET - DRT = 0. This category organizes results into sub-categories such as *Hour Behind* and *Day Ahead*.
- **Future Events** that indicate your events have a future timestamp where NET - DRT < 0. This category organizes results into the sub-categories *Week Ahead* and *Far Future*. The *Far Future* category helps you identify events that fall well outside the most accepted variance range.
- **Past Events** that have a past timestamp where NET - DRT > 0.

The *Past Events* category and *Far Future* sub-category help you identify events that fall well outside the most accepted variance range.

Known Issues

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support, and then select the appropriate product category.

Refer to the Release Notes for ArcSight Platform 22.1 Known Issues for additional information that might affect the Recon 1.4 software.

PCI Reports Not Included in this Release

Issue: The Help and Recon User Guide lists the following Firewall Configuration reports, but they are not included in the currently released PCI Compliance Pack:

- Cardholder Data Within the DMZ
- Inbound Traffic to the Cardholder Data Environment
- Outbound Traffic From Card Holder Data Environment to Internet
- Outbound Traffic from the Cardholder Data Environment
- Unauthorized Outbound Traffic From Cardholder Data Environment

Workaround: We will include these reports in the future. (`OCTCR33I186008`)

Issues Related to Migrating and Searching Logger Data

This release enables you to import data from Logger to the ArcSight Database for use in the Search feature. The following issues affect your use of the Logger Data feature:

Migration Returned Zero Events Because Migration Started Right after Metadata was Imported

Issue: If you import Logger data immediately after its metadata import completes, you will see a completed migration with zero events. Recon will not allow you to search Logger data for those time ranges. (`OCTCR33I386144`)

Workaround: Wait up to 4 minutes after a metadata import before importing its associated Logger data. The wait time is proportional to the quantity and size of the metadata imported.

Unable to Execute Migrations for Dates in the Future

Issue: When importing data from future dates, Recon displays `import 0 events` and will cause issues when trying to import new data again. (`OCTCR33I386145`)

Workaround: Only import data from previous days.

Data Migration Fails If a Chunk of Data Is Both Within and Outside the Specified Time Range

Issue: The data migration process is designed to migrate chunks of event data for the specified days. It's possible that some chunks can contain events with a wide time range. For example, an event within a particular chunk might start late in the evening on May 29 and end the next day.

If your data migration includes a chunk of data that crosses the boundaries of the specified start or end days, the system will migrate the chunks of data with events that cross the time boundary. However, any subsequent migration with a specified time range that includes those same chunks of data will fail because the system cannot migrate data that has already been migrated. When this migration fails, you will see the following error in the logs:

```
[<date>][ERROR] To migrate this time range again, delete the migrated data using script
'loggerToReconDeletion.sh'.
```

(OCTCR33I387021)

Workaround: When migrating events, ensure that you specify a date range that incorporates consecutive days. If you have errors, you can skip the migration of data for that day.

For example, if you have events on Day1, Day2, and Day3, set the date range to include all three days instead of migrating each day separately. Alternatively, if you migrate Day1 and Day2 and have an issue with migrating Day3 and Day4, try skipping Day3. To migrate Day3, please contact Support.

Resolved Issues

The following known issues have been resolved in this release.

Search

Search Fails to Display No Fieldsets

This release resolves an issue where if you searched with a custom fieldset that was deleted, the Create Schedule Searches pop-up did not display the No Fieldset option. (OCTCR33I174132)

Start Date is Empty on the Completed Search Tab

Issue: From the **Completed** tab, when you update the date from All Time > Last Week > All Time, the **Start Time** is empty visually. However, Search uses the Start Date of 12/31/1969. (OCTCR33I181058)

Workaround: You can ignore the empty date because Search will use a Start Date of 12/31/1969 for the All Time setting.

Validation Message Fails to Display

Issue: When you run a Scheduled Search where the start and end dates are in a mixed mode (Dynamic + non-Dynamic), Search fails to display the validation message. However, the search will run. (OCTCR33I174139)

Workaround: Search result will display correctly.

Search Does not Run when Lookup Lists are Included

Issue: Search fails to run when the fieldset includes lookup lists fields and the query does not include *in list*. (OCTCR33I174057)

Workaround: Remove the lookup field from the fieldset and run the search again.

Scheduled Search Might Fail to Run with Certain Query Operators

Issue: Normally, when you create a search query, Search warns you if the specified fieldset does not contain any of the fields in the query. However, Scheduled Search does not warn you. (OCTCR33I174141)

Workaround: If you use the listed operators for a Scheduled Search, ensure that the specified fieldset includes all fields that are in the query.

Schedule Tasks Options are Visible Yet Unavailable

Issue: When you schedule a task, like reports and dashboards, there are two options, Burst and User Defined, that display; however, these two options are not available at this time. (OCTCR33I142914)

Workaround: Do not use these two options.

Issues with Scoring Data

Issue: When you apply a timestamp format to an outlier model, and then change the timestamp format, the scoring goes more quickly. (OCTCR33I115030)

Workaround: After setting a different timestamp, restart your analytics pod.

Lookup List

Lookup List Field in a Fieldset Must be Joined to a Query

Issue: When you add a Lookup List field to a fieldset without also adding the field to the query, Search fails to load. This issue occurs because Search expects the Lookup List field to be part of a join in the search query. (HERC-8220)

Workaround: Remove the lookup field(s) from the fieldset or use the Lookup List in the search query.

CSV File with Invalid Data Creates Empty Lookup Table

Issue: If the CSV file for your Lookup List contains invalid data, Recon will successfully create the lookup table. However, because Recon ignores the invalid data, the new lookup table will not have any data. Also, you will not receive a notification about the empty Lookup List. (HERC-7129)

Workaround: Contact support for help with this issue.

Size or Contents of a CSV File Can Adversely Affect the Ability to Load a Lookup List

Issue: Some storage groups have queries with a strict Vertica SQL syntax, such as events.sourceHostName ~~* 'n15-214-%'. (OCTCR33I180762)

Workaround: To update the storage groups successfully, when you open the modal you must update it using the new syntax.

User Preferences

Issue Time Zone Setting - Performing a Search

Issue: In **User Preferences**, when you set the Time Zone to Database time zone, your ability to search might not work properly. (OCTCR33I115046)

Workaround: In **User Preferences**, set the Time Zone to Browser time zone, then perform the search again.

Issue with Time Zone Setting - Incorrect End Times

Issue: In **User Preferences**, when you set the Time Zone to Database time zone or Custom Time zone, and then Select Range to Yesterday, Week to Date, Month to Date, and so on, the start time is 6:00 instead of 0:00. Recon also displays the end time incorrectly. (OCTCR33I115040)

Workaround: In User Preferences, set the Time Zone to Browser time zone.

Outlier

Fails to Display after you Change the Timestamp Format

Issue: When you apply a timestamp format to an outlier model, and then change the timestamp format, the model fails to appear in **Available Models**. For example, you create a model in Configuration > Outlier with the **Device Receipt Time** of 12/31/19. You then change the timestamp format in My Profile > Preferences > Date/Time Format to YYYY/MM/DD hh:mm:ss:ms. When you access Configuration > Outlier, Recon no longer displays the model with the modified timestamp. (OCTCR33I113036)

Workaround: In My Profile > User Preferences > Date/Time Format, select the original timestamp format for the model. Recon displays the model in **Available Models**.

Erroneously Implies the Date is an Error

Issue: When you copy a search query to create the filter for an outlier model and the query includes a timestamp, Recon erroneously highlights the specified date as if the date or its format were invalid. For example, you copy a search query that includes the phrase Normalized Event Time = 29/05/20 16:20:39:288. In Configuration > Outlier, you paste the copied query in the filter field for a new model. The query field underlines the timestamp in red, which is the usual indication that the value is invalid. (OCTCR33I112031)

Workaround: Ignore the highlight that indicates that the copied timestamp value is invalid.

Technical Requirements

For more information about the software and hardware requirements required for a successful deployment, see the *Technical Requirements for ArcSight Platform*.

Logger and Recon (including the ArcSight Database) can be installed in the same server. Make sure the **RHEL/CentOS** version used in your Logger is also supported by Recon. For additional details, see Logger Release Notes and *Technical Requirements for ArcSight Platform*.

Downloading Recon

Before you begin installing Recon, you must download necessary product installation packages. The installation package also includes the respective signature file, for validating that the downloaded software is authentic and not tampered by a third party.

To review the list of the files and versions to download for this release, see the *Release Notes for ArcSight Platform*.

Installing or Upgrading Recon

Because this release significantly changes the ArcSight Database, you cannot upgrade the database previously installed in your environment. It must be installed as new. However, this release does allow you to upgrade or deploy Recon for the first time. For more information, see the following sections in the *Release Notes for the ArcSight Platform 22.1*.

- Upgrading from Recon 1.2
- Deploying Recon for the first time in an upgraded ArcSight Platform environment
- Deploying Recon 1.4 in a new ArcSight Platform environment

Licensing Information

For information about activating a new license, see the *Administrator's Guide for ArcSight Platform* provided at the Recon Documentation site.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos.
- The Micro Focus Community pages.

Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- *Release Notes for ArcSight Platform 22.1*, which provides an overview of the products deployed in the containerized environment and their latest features or updates
- *Administrator's Guide for ArcSight Platform*, which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.
- *User's Guide for Fusion 1.5 in the ArcSight Platform*, which is embedded in the product to provide both context-sensitive Help and conceptual information for the common features and services.
- *User's Guide for Recon 1.4*, which is embedded in the product to provide both context-sensitive Help and conceptual information for using Recon.
- Product Support Lifecycle Policy, which provides information on product support policies.

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment** or **support** on this topic at the bottom of any page in the HTML version of the documentation posted at the ArcSight Platform Documentation page or the documentation pages for the included products.

Legal Notices