Micro Focus Security ArcSight Intelligence

Software Version: 6.2.0

Release Notes

Document Release Date: December 2020
Software Release Date: December 2020

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

Introduction

This release introduces ArcSight Intelligence 6.2.0.

- System Requirements
- Downloading Intelligence
- Installing Intelligence
- Upgrading Intelligence
- Licensing Information
- What's New?
- Known Issues
- Contacting Micro Focus

System Requirements

For information about the software and hardware requirements for your deployment and performance tuning guidelines, see the Technical Requirements for ArcSight Platform.

Downloading Intelligence

Before you begin installing Intelligence, 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 Intelligence

Micro Focus provides several options for deploying your Intelligence environment. For more information, see the Administrator's Guide for ArcSight Platform.

Upgrading Intelligence

You can upgrade only from 6.1.0 to 6.2.0 version of Intelligence. For more information about upgrading Intelligence, see the Administrator's Guide for ArcSight Platform.

Licensing Information

For information about activating a new license, see the Administrator's Guide for ArcSight Platform.

What's New?

The following sections outline the key features and the issues resolved in this release:

- ArcSight Platform Installer
- Support for New Devices
- Support for a New Data Type
- Integration with Enterprise Security Manager
- Integration with Fusion
- URL Compression and Encoding
- Software Fixes

ArcSight Platform Installer

The ArcSight Platform Installer provides an installation process that can automatically take care of all the prerequisites, software installations, and post-installation configurations for a new deployment. This tool provides configuration files applicable for single-node and multi-node setups. For more information about the ArcSight Platform Installer, see the *Using ArcSight Platform Installer to Build Your Environment* section in Administrator's Guide for ArcSight Platform.

Support for New Devices

For the supported data types, Intelligence also provides support for new devices that provide data of relevance to the Intelligence analytics models. For more information, see the *Adding Support for New Devices* section in Administrator's Guide for ArcSight Platform.

Support for a New Data Type

Intelligence now supports the ingestion and analysis of the Repository data type. The following repository systems are supported:

- GitHub Enterprise - 2.21.0
- BitBucket Server - 7.5.0
- Perforce - 2020.1

Integration with Enterprise Security Manager

Enterprise Security Manager (ESM) can now use risky users and alerts information provided by Intelligence to automatically populate Active Lists. This can be achieved by integrating Intelligence with ESM with the help of FlexConnectors. For more information, see the *Integrating Intelligence with Enterprise Security Manager* section in Administrator's Guide for ArcSight Platform.

Integration with Fusion

The Fusion UI now includes a link called **Entities at Risk** which allows direct navigation to the Intelligence UI. The Intelligence UI also includes a new Fusion link that takes the users back to the Fusion UI. In the Fusion UI, you can create widgets that display the count of entities analysed by Intelligence.

URL Compression and Encoding

For enhanced data security, Intelligence provides options to encode the Intelligence URL string. Based on your requirement, you can set the limit for the URL string length and then select a preferred URL encoding option. For more information, see the *Setting an Encoding Option for the URL* section in Administrator's Guide for ArcSight Platform.

Software Fixes

- Cannot Explore Raw Events for the Anomaly Types 282, 286, and 287 of the Active Directory Server Data
- Cannot View the Events for Anomalies Related to Travel
- Events in Recon For Historical Data
- Swagger User Interface Might Display an Alert Icon Even When Properly Authenticated
- Cannot View the Events that Triggered an Anomaly

Cannot Explore Raw Events for the Anomaly Types 282, 286, and 287 of the Active Directory Server Data.

Issue: In the Intelligence UI **> Explore** page, when you filter anomalies with 282, 286, or 287, anomalies are displayed in the **Anomalies & Violation** panel based on the filter you provided. When you click an anomaly, a dialog box provides context about the anomaly or violation. When you click **View Events > Explore Raw Events**, you cannot see any events. [FT-20865]

Fix: You can now view and explore the events.

Cannot View the Events for Anomalies Related to Travel

Issue: In the Intelligence UI **> Explore** page **> Anomalies & Violation** panel, when you click an anomaly related to travel and view the events that triggered it by using any of the following methods, you might not see any events:

- Click **View Events** to view the events that triggered the anomaly.
- Click **View Events**, then click **Explore Raw Events** to explore raw events in the Event Viewer.

This happens if the latitude and longitude data from the SmartConnectors have values that are more than four decimal points.

For example, longitude value = 100.992541

This does not have an impact on Intelligence Analytics and hence, anomalies are generated. However, the events contributing to the anomalies are not displayed. [FT-20867]

Fix: Intelligence now displays events for anomalies related to travel having latitude and longitude values more than four decimal points.

Events in Recon For Historical Data

Issue: When you ingest historical data in the database and Analytics is run for it, the anomalies are displayed in the Intelligence dashboard. In Recon, you cannot view or explore the events that triggered the anomalies when the database receives historical events that were generated more than 7 days ago.

For example, if the database receives historical events on 9th July and the events were generated on 1st July, the events are not visible in Recon. [FT-20973]

Fix: You can now view or explore the events in Recon.

Swagger User Interface Might Display an Alert Icon Even When Properly Authenticated

Issue: When Intelligence Administrators log into the Swagger user interface, they might see an alert icon on certain functions. [FT-10243]

Fix: After logging in to the Swagger user interface, the alert icon is not displayed.

Cannot View the Events That Triggered an Anomaly

Issue: In the Intelligence UI **> Explore** page **> Anomalies & Violation** panel, when you click an anomaly or violation, a dialog box provides context about the anomaly or violation. When you click **View Events** to view the events that triggered the anomaly or violation, you might not see any events. This is a sporadic issue. [FT-20305]

Fix: You can now view the events.

Known Issues

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs.The following issues are currently being researched. If you need further assistance with any issue, contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/.

- Special Characters for Database Credentials
- Search Query Is Not Populated in Recon for the Anomaly Types 605 and 606 of the Web Proxy Data
- Links in the PDF Reports Do Not Work
- Intelligence Installation Using the ArcSight Installer Results in Intelligence Analytics Failure when the Analytics Pods Start for the First Time
- Multi-node Installation of Intelligence Using the ArcSight Installer Results in Analytics Failure because of HDGS NameNode Mismatch
- Cannot Log in to the Intelligence UI if the URL Encoding Option for a Multi-node Setup is Set as Hash
- When Custom SSL Chain Certificates are Used, Logstash Pods Fail to Communicate with Transformation Hub
- Analytics Might Fail or ENTITYID Might Truncate if the Ingested Data has Entities More Than 255 Characters
- Unable to View Events for Anomalies after Upgrading Intelligence from 6.1.0 to 6.2.0 when Event Sorting is Disabled before the Retention Period
- Recon Search Fails to Work for Fileshare and Resource Data if the Values of the File Name and File Path Fields Contain “\”
- Filtering Does Not Work for the '-' Character in Intelligence UI
- Filtering Using the Hand Icon in the Matrix of Anomalies &amp; Violations Does Not Update the Top Risky Users Accordingly
- Mismatch Between the Anomaly Expected Highest Value and the Visualization Expected Highest Value
- CSV Reports Do Not Have Timestamps in the Date and Time Format
- Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects
- Bad Message 413 reason: Request Entity Too Large
- Daylight Savings Time
- Repartition Percentage Threshold
- Prefix Filtering Does Not Work in CDF for Event Viewer
- Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container
- Certificate Warnings in Logstash Logs

Special Characters for the Database Credentials

Issue: Intelligence Analytics does not support the following characters when you specify the database credentials:

- Whitespace
- Single quotes

Workaround: There is no workaround at this time.

[FT-21600]

Search Query Is Not Populated in Recon for the Anomaly Types 605 and 606 of the Web Proxy Data

Issue: In the Intelligence UI **> Explore** page, when you filter anomalies with 605 or 606, anomalies are displayed in the **Anomalies & Violation** panel based on the filter you provided. When you click an anomaly, a dialog box provides context about the anomaly or violation. When you click **View Events > Search in Recon**, the search query is not populated in Recon.

Workaround: There is no workaround at this time.

[FT-21921]

Links in the PDF Reports Do Not Work

Issue: When you click a link in a PDF report downloaded from the Intelligence UI, you must be directed to the Intelligence UI. Instead, you are directed to the **https://interset-api-svc:9090/interset/0/** URL and you get a site cannot be reached error.

For example, for a PDF Report which gives the top risky users' information, when you click a top risky user listed in the PDF, instead of being directed to the Intelligence UI, you are directed to **https://interset-api-svc:9090/interset/0/**.

Workaround: In the address bar of the web browser, replace the **https://interset-api-svc:9090/interset/0/** URL with the **https://<IP address or hostname of Intelligence>/interset/0/** URL and press enter. You are directed to the Intelligence UI.

[FT-21863]

Intelligence Installation Using the ArcSight Installer Results in Intelligence Analytics Failure when the Analytics Pods Start for the First Time

Issue: If you install Intelligence by using the ArcSight Platform Installer and execute the install script, the analytics pods move to the Running state even before the postinstall is complete. Intelligence Analytics runs for the first time but it fails and you get an error that "Investigation Schema does not exist". This happens because when the analytics pods come up after the install command is complete, they look for the Investigation schema. However, the Investigation schema is created in the database only after you execute the postinstall script and the postinstall is complete.

Workaround: After the postinstall is complete, perform the following steps:

1. Launch a terminal session and log in to the NFS node.
2. Navigate to the following directory:

   ```
   cd <NFSVolume>/interset/analytics
   ```

3. (Conditional) Delete the blackhawk_down file, if present. This is an error file and it is generated if the previous Analytics execution fails.

   ```
   rm blackhawk_down
   ```

4. When prompted whether you want to delete the file, enter yes.
5. Execute the following command to delete the latest AnalyticsStarted.mk and AnalyticsCompleted files:

   ```
   rm -rf AnalyticsStarted-0-<Today's_date>.mk AnalyticsCompleted-0-<Today's_date>.mk
   ```

6. When prompted whether you want to delete the files, enter yes.
   After 30 seconds of deletion of the files, Analytics is triggered automatically.

[FT-21922]

Multi-node Installation of Intelligence Using the ArcSight Installer Results in Analytics Failure Because of HDFS NameNode Mismatch

Issue: When you perform a multi-node installation of Intelligence by using the ArcSight Platform Installer, the postinstall script creates the HDFS configuration files on all the database nodes. By default, it adds the corresponding database hostname or IP address instead of the HDFS NameNode hostname or IP address in the **core-site.xml** HDFS configuration file. This leads to Intelligence Analytics failure when it is run for the first time and you get an error that could not connect to the HDFS URL: hdfs://<HDFS NameNode hostname or IP address>:30820.

Workaround: After the postinstall is complete, perform the following steps:

1. Log in to a database node as a root user.
2. Navigate to the the **/etc/hadoop/conf/** directory.
3. For the **core-site.xml** file, update the NAMENODE_HOST value for the **fs.defaultFS** and **dfs.namenode.http-address** properties with the hostname or IP address of the node where the **interset-namenode:yes** label has been applied.
4. Repeat Steps 1 to 3 on all database nodes.
5. Change to the following directory:

   ```
   cd /opt/vertica/bin/
   ```

6. Log in as a dbadmin:

   ```
   su dbadmin
   ```

7. Log in to vsql and specify the password when prompted:

   ```
   vsql
   ```

   ```
   [password prompt]
   ```

8. (Optional) Clear the cache:

   ```
   SELECT CLEAR_HDFS_CACHES();
   ```

9. Execute the following command:

   ```
   SELECT VERIFY_HADOOP_CONF_DIR();
   ```

10. Do the following to restart the HDFS DataNodes:
    a. Launch a terminal session and log in to a worker node where an HDFS DataNode is deployed.

    b. Execute the following commands:

    ```
    NAMESPACE=$(kubectl get namespaces | grep arcsight-installer | awk '{ print $1}')
    ```

    ```

    kubectl get pods -n $NAMESPACE | grep -e 'hdfs\|interset-analytics' | awk '{print $1}' | xargs
    kubectl delete pod -n $NAMESPACE --force --grace-period=0
    ```

11. Launch a terminal session and log in to the NFS node.
12. Navigate to the following directory:

    ```
    cd <NFSVolume>/interset/analytics
    ```

13. (Conditional) Delete the blackhawk_down file, if present. This is an error file and it is generated if the previous Analytics execution fails.

    ```
    rm blackhawk_down
    ```

14. When prompted whether you want to delete the file, enter yes.
15. Execute the following command to delete the latest AnalyticsStarted.mk and AnalyticsCompleted files:

    ```
    rm -rf AnalyticsStarted-0-<Today's_date>.mk AnalyticsCompleted-0-<Today's_date>.mk
    ```

16. When prompted whether you want to delete the files, enter yes.
    After 30 seconds of deletion of the files, Analytics is triggered automatically.

[FT-21924]

Cannot Log in to the Intelligence UI if the URL Encoding Option for a Multi-node Setup is Set as Hash

Issue: In the Kubernetes Dashboard of CDF Management Portal, for the **investigator-default-yaml** file in the arcsight-installer namespace, when you specify the URL encoding option as Hash, you cannot log in to the Intelligence UI when you try to log in again.

Workaround: There is no workaround at this time.

[FT-21920]

When Custom SSL Chain Certificates are Used, Logstash Pods Fail to Communicate with Transformation Hub

Issue: When configured with custom SSL chain certificates, the Logstash pods fail to communicate with Transformation Hub and enter into the CrashLoopBackOff stage. This issue occurs when you use the intermediate CA certificates. The issue does not occur when you use the default CA certificates.

Workaround: Perform the following steps:

1. Launch the CDF Management Portal on port 5443.
2. Log in with the following credentials:
   User name: admin
   Password: *<the password you provided during CDF installation>*
3. Click **Cluster>Dashboard**. The Kubernetes Dashboard is displayed.
4. Under the **Namespace**, search and select the arcsight-installer-xxxx namespace.

5. Under **Config and Storage**, click **Config Maps**.
6. Click the filter icon and search for logstash-config-pipeline.
7. Click ⋮ and then click **Edit**.
8. In the **YAML** file, in the **codec => avro_schema_registry**, update the **ca_certificate =>** field with **'/vault-crt/trustedCAs/RE_ca.crt'**.
9. Click **Update**.
10. Do the following to restart the Logstash pods:
    a. Launch a terminal session and log in to the master node or a worker node.

    b. Execute the following commands:

    ```
    export NS=$(kubectl get namespaces | grep arcsight|cut -d ' ' -f1)
    ```

    ```
    kubectl -n $NS scale statefulset interset-logstash --replicas=0
    kubectl -n $NS scale statefulset interset-logstash --replicas=3
    ```

[FT-21957]

Analytics Might Fail or ENTITYID Might Truncate if the Ingested Data has Entities More Than 255 Characters

Issue: If the ingested data has entities more than 255 characters, either of the following may occur:

- The value of ENTITYID in the analytics schema might truncate after running analytics.
- Analytics might fail with the following error messages:
    - Unable to create/insert into target table: UEBA.ENTITIES_RISK with SaveMode: Append. ERROR MESSAGE: ERROR: java.sql.SQLIntegrityConstraintViolationException: [Vertica][VJDBC](6745) ERROR: Duplicate key values: 'TID=0,ENTITYTYPE=usr,ENTITYID=<entity_id_displayed>,SCORETYPE=vul,"TIMESTAMP"=2020-09-21 22:00:00,TIME_BUCKET=hourly' – violates constraint 'UEBA.ENTITIES_RISK.C_PRIMARY'
    - Exception in thread "main" java.sql.SQLIntegrityConstraintViolationException: [Vertica]VJDBC ERROR: Duplicate MERGE key detected in join [(UEBA.PREVIOUS_ENTITIES_RISK x UEBA.PREVIOUS_ENTITIES_RISK_STAGING) using PREVIOUS_ENTITIES_RISK_super and subquery (PATH ID: 1)]; value

Workaround: Execute the following queries:

Note: Consider the following:

- <schema_name> - Replace with the actual analytics schema name. For example: UEBA
- VARCHAR(1024) - 1024 must be same as the OBSERVED_ENTITY_RELATION_MINUTELY_COUNTS.entityid column length. Change accordingly in the following queries:

```
ALTER TABLE <schema_name>.ENTITIES_RISK DROP CONSTRAINT C_PRIMARY;

ALTER TABLE <schema_name>.ENTITIES_RISK alter column ENTITYID SET DATA TYPE VARCHAR(1024);

ALTER TABLE <schema_name>.ENTITIES_RISK ADD CONSTRAINT C_PRIMARY PRIMARY KEY (TID, ENTITYTYPE, ENTITYID, SCORETYPE, TIMESTAMP, TIME_BUCKET) ENABLED;

ALTER TABLE <schema_name>.PREVIOUS_ENTITIES_RISK DROP CONSTRAINT C_PRIMARY;

ALTER TABLE <schema_name>.PREVIOUS_ENTITIES_RISK alter column ENTITYID SET DATA TYPE VARCHAR(1024);

ALTER TABLE <schema_name>.PREVIOUS_ENTITIES_RISK ADD CONSTRAINT C_PRIMARY PRIMARY KEY (TID, ENTITYTYPE, ENTITYID, SCORETYPE, TIMESTAMP, TIME_BUCKET) ENABLED;

ALTER TABLE <schema_name>.PREVIOUS_ENTITIES_RISK_STAGING alter column ENTITYID SET DATA TYPE VARCHAR (1024);
```

[FT-21970]

Unable to View Events for Anomalies after Upgrading Intelligence from 6.1.0 to 6.2.0 when Event Sorting is Disabled before the Retention Period

Issue: After upgrading Intelligence from 6.1.0 to 6.2.0, if you disable **CDF Management Portal > Event Sorting** before the configured retention period, you cannot view the events for anomalies.

Workaround: After upgrading Intelligence from 6.1.0 to 6.2.0, do not disable **Event Sorting** before the configured retention period.

Perform the following steps after the completion of your configured retention period, and then disable **Event Sorting**:

1. Launch the CDF Management Portal on port 5443.
2. Log in with the following credentials:
   User name: admin

   Password: <*the password you provided during CDF installation*>
3. Click ⋮ , then click **Reconfigure**.
4. Click **Intelligence** and enable **Enable Search Manager**.
5. Click **Save**.

6. Log in to Intelligence as a System Admin user.
7. Click **Settings**⚙ and select **Search Manager**.
8. Select **Submit a Job** from the drop-down list.
9. Select **Purge** from **Select Your Job Type**.
10. Specify the information for the fields present under **Set Your Job Parameters**.
11. Click **Submit Job**. Verify whether the job was completed successfully.
12. Navigate back to the CDF Management Portal and disable **Enable Search Manager** and **Event Sorting**.
13. Click **Save**.
14. Do the following to restart the interset-api pods:
    a. Launch a terminal session and log in to the master node or a worker node.
    b. Execute the following commands:

```
export NS=$(kubectl get namespaces | grep arcsight|cut -d ' ' -f1)
```

```
kubectl -n $NS scale deployment interset-api --replicas=0
kubectl -n $NS scale deployment interset-api --replicas=2
```

[FT-21937]

Recon Search Fails to Work for Fileshare and Resource Data if the Values of the File Name and File Path Fields Contain “\”

Issue: In the Intelligence UI **> Explore** page **> Anomalies & Violation** panel based on the filter you provided. When you click an anomaly related to FileShare or Resource, a dialog box provides context about the anomaly or violation. When you click **View Events>Search in Recon**, the Recon search fails to work for Fileshare and Resource data if the values of the **File Name** and **File Path** fields contain “\”.

Workaround: There is no workaround at this time.

[FT-21997]

Filtering Does Not Work for the '-' Character in Intelligence UI

Issue: When filtering using the search filter in the Intelligence UI, if the search includes the '-' character, no results are displayed.

Workaround: There is no workaround at this time.

[FT-20825]

Filtering Using the Hand Icon in the Matrix of Anomalies & Violations Does Not Update the Top Risky Users Accordingly

Issue: In the Intelligence UI **> Explore** page **> Matrix of Anomalies & Violations**, when you click the hand icon, then click and drag the cursor across the matrix to see the risky users and anomalies or violations for a specific time interval, the users in the **Top Risky Users** panel are not updated accordingly.

For example, if there are no risky users and the associated anomalies or violations in the selected time interval (for example, between 4:30 pm and 4:35 pm on a day), the **Top Risky Users** panel still displays users.

Workaround: There is no workaround at this time.

[FT-20451]

Mismatch Between the Anomaly Expected Highest Value and the Visualization Expected Highest Value

Issue: In the Intelligence UI **> Explore** page **> Anomalies & Violation** panel, when you click an anomaly or violation, a dialog box provides context about the anomaly or violation. The **Expected highest for <user_name>** value in the visualization does not match the value in the anomaly or violation.

For example, an anomaly is " It was slightly unusual that <user_name> logged in to Intelligence 12 times in an hour; <user_name> typically logs in at most 6 times in an hour." and the **Expected highest for <user_name>** value in the visualization is 4. In this example, the expected highest value for the user is 6 and the value in the visualization is 4. There is a mismatch between the values.

Workaround: There is no workaround at this time.

[FT-20947]

CSV Reports Do Not Have Timestamps in the Date and Time Format

Issue: The CSV Reports have timestamps in the Unix Epoch format instead of the date and time format.

Workaround: There is no workaround at this time.

[FT-20978]

Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects

Issue: When anomalies are identified because few users access a specific project, and one or more of the users are flagged as bots, changing the BOT users to NOTBOT users — and therefore increasing the number of non-bot users accessing the project — will not impact the project's identification as 'inactive'. Anomalies will therefore continue to be identified when the project is accessed, even though more non-bot users are now regularly accessing the project.

Workaround: There is no workaround at this time.

[FT-8934]

Bad Message 413 reason: Request Entity Too Large

Issue: While logging to the Intelligence UI, a bad message **413** is encountered.

Workaround: Clear the cookies for the site and log in again.

[FT-20164]

Daylight Savings Time

Issue: During the weeks immediately following Daylight Savings Time (DST) clock changes, you may observe an increase in reported Normal Working Hours anomalies. These anomalies, which are due to automatic software clock changes, will usually have risk scores of zero (0), and are reflective of the perceived Normal Working Hours pattern shift.

Workaround: There is no workaround needed.

[FT-8601]

Repartition Percentage Threshold

Issue: In the **CDF Management Portal > Configure/Deploy** page **> Intelligence**, when you specify a value for the **Repartition Percentage Threshold** field, the installer does not validate the value. However, Intelligence Analytics fails if the value is not set between 0.7 and 1.0 as stated in the tooltip.

Workaround: Ensure that you set a value between 0.7 and 1.0.

[FT-20011]

Prefix Filtering Does Not Work for Event Viewer

Issue: When searching for a prefix string in Event Viewer, the result of the query is of all the occurrences of the string.

Workaround: There is no workaround at this time.

[FT-20239]

Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container

Issue: In the **CDF Management Portal > Configure/Deploy** page **> Intelligence**, when you change the value of the **HDFS NameNode** field to deploy the HDFS NameNode container on another worker node, the older instance of the HDFS NameNode container goes into a pending state instead of being terminated.

Workaround: Perform the following steps after changing the value in the field:

1. In the CDF Management Portal, click **Cluster > Nodes**.
2. Click the [-] icon for the **interset-namenode:yes** label present on the worker node.
3. From **Predefined Labels**, drag and drop the **interset-namenode:yes** label to the worker node to which you want to add it. Ensure the worker node matches the new value you specified in the **HDFS NameNode** field.
4. Configure the database with HDFS. For more information, see the "Configuring the Database with HDFS for Intelligence" section in Administrator's Guide for ArcSight Platform.
5. Restart the HDFS DataNodes. Do the following:
   a. Launch a terminal session and log in to a worker node where an HDFS DataNode is deployed.
   b. Execute the following commands:

```
NAMESPACE=$(kubectl get namespaces | grep arcsight-installer | awk '{ print $1}')
```

```
kubectl get pods -n $NAMESPACE | grep -e 'hdfs\|interset-analytics' | awk '{print $1}' | xargs
kubectl delete pod -n $NAMESPACE --force --grace-period=0
```

[FT-20019]

Certificate Warnings in Logstash Logs

Issue: When you view the Logstash logs, you might come across the following warnings:

- ** WARNING ** Detected UNSAFE options in elasticsearch output configuration!
- ** WARNING ** You have enabled encryption but disabled certificate verification.
- ** WARNING **To make sure your data is secure change :ssl_certificate_vertification to true

Workaround: There is no workaround needed. You can ignore these warnings as there is no impact in the functionality.

[FT-20038]

Swagger UI Session Expires After 120 seconds of Inactivity

Issue: When using the Swagger UI and trying an API request for a particular operation, a successful result returns a code of 200. If the Swagger UI is not used for 120 seconds or more (inactive screen), and the same API request is re-tried, it results in returning an error code of **401**.

Workaround: The reason for the issue is due to token expiry after 120 seconds. To get the correct result, go back to the Intelligence UI. Refresh the Intelligence UI and then use the Swagger UI.

[FT-20234]

Cannot Save Searches in Event Viewer

Issue: When exploring events in the Event Viewer, you cannot save the search query that you build. Ideally, when you **Type to filter raw events**, a custom built query can be saved using the **Save** option at the bottom left. This functionality is not working currently.

Workaround: The workaround for this issue involves modification of the **investigator.yml**. Contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/ to resolve the issue.

[FT-20299]

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://softwaresupport.softwaregrp.com/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://softwaresupport.softwaregrp.com/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

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 (Intelligence 6.2.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!