Micro Focus Interset 5.9.2 Release Notes

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be 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.

Except as specifically indicated otherwise, this document contains confidential information and a valid license is required for possession, use or copying. If this work is provided to the U.S. Government, 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.

Contents

Introduction 4

Interset 5.9.2 Supported Environments 5

Interset Analytics System 5

Supported Data Sources 6

New Features 8

Interset 5.9.2 8

Interset 5.9.0 8

Deprecated Features 10

Known Issues 11

Interset 5.9.2 11

Index 14

Introduction

This Guide provides the Interset 5.9.2 release notes, which include:

- the supported software environments,
- the new features introduced in Interset 5.9.2,
- the features discontinued in the current or a future release, and
- known issues as of January 31, 2020.

Should you have any questions or concerns about the information presented in this or any other Interset Guide, please contact Micro Focus Interset Support at interset.support@microfocus.com.

Interset 5.9.2 Supported Environments

Interset 5.9.2 includes

- the Interset Analytics system, version 5.9.2

Interset Analytics System

Interset Analytics version 5.9.2 supports the following (x86_64) environments:

- CentOS 7.6
- Red Hat Enterprise 7.6

Interset 5.9.2 is supported with the following third-party components:

- Oracle OpenJDK 8u201/211
- Elasticsearch 6.8.1

Interset 5.9.2 is supported with HDP 3.1.0, including the following components:

Ambari	2.7.3.0
AsyncHBase	1.8.2
Avro	1.8.2
Hadoop	3.1.1
HBase	2.0.2
Hortonworks Schema Registry	0.5.3
Kafka	2.0.0
NiFi	1.10.0
Phoenix	5.0.0
Scala	2.11.8
Spark	2.3.2
Storm	1.2.1
ZooKeeper	3.4.6

Interset 5.9.2 is supported with CDH 6.1.1, including the following components:

AsyncHBase	1.8.2
Avro	1.8.2
Hadoop	3.0.0
HBase	2.1.1
Hortonworks Schema Registry	0.5.3
Kafka	2.0
NiFi	1.10.0
Phoenix	5.0.0-HBase-2.0-cdh6.1.1
Scala	2.11.8

Spark	2.4
Storm	1.2.1
ZooKeeper	3.4.5

Interset 5.9.2 supports the following Web browsers:

- Google Chrome 74 and above
- Mozilla Firefox 67 and above

Supported Data Sources

Interset 5.9.2 supports the following data sources. For .csv data sources, the delimiter can be customized.

- Active Directory
    - Active Directory event logs stored in McAfee® Enterprise Security Manager (ESM)
    - Active Directory event logs stored in Splunk®
    - Active Directory event logs stored in Micro Focus ArcSight Logger
    - Active Directory event logs stored in IBM QRadar
    - Windows Security event logs (.csv)
    - Interset-extracted Windows event logs (.csv)
    - Universal Windows event logs (.csv)
    - Windows Event Viewer-extracted event logs (.csv)
    - Active Directory authentication logs
- Universal Alerts stored in third-party DLP systems (.csv)
- NetFlow
    - Version 5
    - Version 9
    - Version 10 (IPFIX)
- Repository
    - Perforce
        - P4AUDIT logs
        - Perforce Structured Server audit logs
    - GitHub Enterprise audit logs
    - Universal repository logs (.csv)
- Pluggable Authentication Module (PAM) AuditD logs (.csv)
- Printer logs
    - Windows printer events stored in Splunk
    - Windows event logs (.csv)
    - Universal logs (.csv)
- Universal Web Proxy (.csv)

- Violations
- Expense Data
- Email Data

Interset 5.9.2 data ingest uses NiFi for data extraction, transformation, and loading. It supports the processing of data set files in the following compression formats:

- tar
- gzip
- tar gzip

To ingest packaged data from other containers such as Arcsight, IBM QRadar, McAfee ESM, and Splunk, please contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/.

New Features

Interset 5.9.2

Interset 5.9.2 is primarily a collection of improvements to the deployment scripting, and related defect fixes. There are no new features.

- **Platform Upgrades**

  The Interset 5.9.2 platform support is unchanged from Interset 5.9.0, with the exception that the version of NiFi has been updated to 1.10.0. The NiFi version upgrade is for an improved data integration experience.

Interset 5.9.0

The new features introduced in Interset 5.9.0 include the following:

- **Analytics: Increased Performance and Reduced Compute Cost**

  Interset 5.9.0 includes optimizations for HBase query operations and entity-risk analytic operations, as well as enhanced analytic operation controls (enable/disable) and environment performance monitoring.

- **Security and Encryption by Default**

  The Interset installer has been updated to perform secure installation on both HDP and CDH by default. The underlying components are configured for default encryption of data-in-motion.

- **Elasticsearch Enhancements**

  It is now possible to prune ES data based on event timestamps.

  The Interset stack now uses the Elasticsearch REST client rather than the Transport client.

- **Enriched User Interface**

  You can now annotate anomalies and add comments to help track your analysis. The history of annotation changes is maintained, so you can see what other analysts have done. Changes performed by different analysts are synchronized in real time.

  The new native event viewer allows you to review event details without leaving the Interset application.

- **Enhanced PDF reporting**

  New custom report templates allow you to change the wording of specific anomalies, including abstracted anomaly parameters. You can also combine annotations and comments in reports.

- **Workflow Enhancements**

  You can now create and import DROOLS Workflows (including timestamp-based rules) independent of the Interset user interface. New Workflow validation lets you test your Workflow logic ahead of deployment. Your Workflows can now include custom API endpoints as data sources.

- **New Analytics Models**

  Interset 5.9.0 now includes geo-velocity models based on latitude and longitude (for AD, Authentication, WebProxy, and VPN data), and new user agent models on WebProxy logs.

- **Platform Upgrades**

  Interset 5.9.0 ships with the following upgraded components for improved performance, security, and stability:

  - HDP 3.1
  - CDH 6.1.1
  - Elasticsearch 6.8.1

Deprecated Features

The following features are deprecated in Interset 5.9.0:

- **Apache Flume**

  Apache Flume was removed from HDP 3.0. As a result, support for Apache Flume in Interset 5.9.0 is deprecated and will be removed in the next release. If you require assistance with replacing Apache Flume, contact Interset Customer Support.

- **HDP/Ambari**

  HDP/Ambari is deprecated in Interset 5.9.0, but will be supported in this version of the product.

Known Issues

The known issues include issues as of January 31, 2020 for Interset 5.9.2.

Interset 5.9.2

The Interset Installer May Unexpectedly Exit after Installing OpenJDK

After installing OpenJDK in **Step 1** (Initial server config), the Interset Installer may unexpectedly exit. This does not cause any problems, and OpenJDK will have installed correctly.

Continue the installation by running **Step 1** again, but this time select the option to keep the Java version that is already installed.

[FT-19209]

After Adding New Index Patterns in Kibana, You Must Refresh the Interset Explore Page

When you add a new index pattern in Kibana, you must refresh the Interset **Explore** page in your Web browser before searching the data. If you do not refresh the Explore page, your search will not be successful.

After you refresh the **Explore** page, the searches with that index pattern will be successful.

[FT-16758]

5.9.2 Schema Registry User Interface Appears Differently than the Defined Schema

When you view a schema in the Interset 5.9.2 schema registry user interface, and you advance to the next schema, the name of the next schema will appear but the actual schema shown will be the first schema you viewed.

To avoid this situation, when viewing a schema, use the search function on the schema page to look up the schema of interest.

[FT-16677]

Blank Lines in Workflow List Files Can Prevent Rules from Triggering

When you use a list file as input to Workflows and the list contains a blank line, the blank line will cause Workflow to fail to trigger on events.

To avoid this situation, ensure that Workflow list files do not contain blank lines.

[FT-16105]

Inconsistent Time Zone Conversion for Daily Anomalies in Expense Data

When you ingest expense data that captures only the date in the timestamp field, and not a time, the timestamp conversions within the different Interset components results in inconsistent interpretations in daily anomalies.

For example,

- Expense data without a specified time in the timestamp field that is ingested on June 1, 2018 will have the timestamp converted by Interset to June 1, 2018, 00:00:00.000 UTC.
- Because daily anomalies are triggered 24 hours later, the anomalies identified in this data would appear in HBase with a timestamp of June 2, 2018, 23:00:00.000 UTC.
- In the Interset user interface, however, due to the manner in which anomalies and raw data are converted to the local time zone, in the Eastern Time Zone for example, these anomalies would appear with a timestamp of June 2, 2018, 20:00:00.000 EST.
- In the raw data, the timestamp for these anomalies would appear as June 1, 2018, 20:00:00.000 EST, or June 1, 2018, 00:00:00.000 UTC.

This issue will be addressed in a future release.

[FT-14631]

Raw Data Downloaded to .csv is Capped at 10,000 Events

When you view anomalies in the Interset user interface and you click **Explore Raw Events** to view the underlying raw events in Kibana, if you choose to download the raw events to a .csv file, a maximum of 10,000 events will appear in the resulting .csv file. This is regardless of the total number of underlying raw events.

This issue will be fixed in a future release.

[FT-14030]

Top Risky List May Include Entities with No Anomalies

Following upgrade, when you log in to Interset and view results, as you scroll through the Top Risky entities, you may see fewer entities than you did in earlier versions. In version 5.7.0, entities that have anomalies but whose risk on the latest timestamp in the data is exactly zero (0) are now excluded from the list. You may still see some entities that are showing a risk score of zero (0), but these are entities that have some small amount of risk that rounds to 0. For example, a risk score of 0.00001 would still be shown in the list, but the score rounds to 0.

[FT-13703]

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

When anomalies are identified because so 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.

This issue has no workaround.

[FT-8934]

Daylight Savings Time

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.

[FT-8601]

Swagger User Interface Displays "Error"

When you launch Swagger, you may receive the following error message: "Message": "Can't read from file http://<*server_name*>.yourcompany.com/api/swagger.json"

This error message is the result of Swagger attempting to reach a Cloud service to perform schema validation, and will not prevent you from performing any actions using the API.

[FT-9448]

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

When an Interset Administrator logs into the Swagger user interface, they may see an alert icon on certain functions. This alert does not impact the API, and can be ignored.

[FT-10243]

While reinstalling Workflow, the existing topology does not get deleted automatically.

When reinstalling Workflow, it is a known issue that the existing topology does not get deleted. This causes an error while reinstalling the topology later. The only workaround to the issue is to remove the topology manually before running the step to re-install Workflow. Use the following command to delete the current topology:

```
/opt/interest/rules/bin/workflow.sh --kill /opt/interset/rules/conf/rules.conf
```

This issue will be fixed in a future release.

[FT-19686]

Index

environments

supported 5

features

new 8

Interset system

supported environments 5

issues

known 11

known

issues 11

new

features 8

supported

environments 5