Micro Focus Security

ArcSight Interset Standard Edition

Software Version: 6.0.0

Release Notes

Document Release Date: April 2020

Software Release Date: April 2020

Contents

Introduction 4

System Requirements 5

Software Requirements 5

Hardware Guidelines 5

Supported SmartConnectors 5

Supported Data Sources 5

Ports Used 7

New Features 8

Interset 6.0.0 8

Unsupported Features 9

Known Issues 10

ArcSight Interset 6.0.0 10

Introduction

This Guide provides the ArcSight Interset 6.0.0 release notes, which include:

- the supported software environments,
- the new features introduced in ArcSight Interset 6.0.0,
- the unsupported Features
- known issues as of April, 2020.

Should you have any questions or concerns about the information presented in this or any other ArcSight Interset 6.0.0 Guide, please contact Micro Focus Interset Support at interset.support@microfocus.com.

System Requirements

This section provides information about system requirements and tuning guidelines for ArcSight Interset.

> **Important**: For information about system requirements for CDF, Transformation Hub, Vertica, and SmartConnectors, see the specific product documentation.

Software Requirements

Software	Version
CDF	2020.02
Transformation Hub	3.2.0
Analytics	3.1.0
Vertica	9.2.1
SmartConnectors	7.14.0

Hardware Guidelines

Hardware specifications for ArcSight Interset are heavily dependent on your deployment environment and requirements. As a result, the hardware requirements listed below represent minimum hardware specifications needed for demonstration purposes only. Please contact your local Sales Engineer for sizing requirements for your specific needs.

CPU: 16 Cores

RAM: 64 GB

HDD: 300 GB

Supported SmartConnectors

Interset supports the following SmartConnectors:

- SmartConnector for Microsoft Active Directory Windows Event Log Native
- SmartConnector for Squid Web Proxy Server File
- SmartConnector for Blue Coat Proxy SG Multiple Server File

Supported Data Sources

Interset supports the following data sources:

- Active Directory
- Web Proxy

Ports Used

In addition to the ports used by CDF, Transformation Hub, and Vertica, Interset uses the following ports when firewall is enabled. Therefore, ensure that the following ports are available:

Ports	Direction	Description
TCP 30820	Inbound	Used for Vertica to connect to HDFS during Analytics processing
TCP 30070	Inbound	Used for Hadoop Monitoring Dashboard (Optional)

New Features

Interset 6.0.0

ArcSight Interset 6.0.0 is primarily a containerized application that is based on Container Deployment Foundation (CDF). Within Micro Focus there is a **Container Deployment Foundation**(CDF), which is an abstraction on top of Kubernetes. ArcSight Interset 6.0.0 works with CDF by integrating with other Micro Focus technologies that are also deployed via CDF.

- **Platform Upgrades**

  ArcSight Interset 6.0.0 ships with the following upgraded components for improved performance, security, and stability :

  - HDP 3.2.1
  - Vertica 9.2.1
  - Spark 2.4.2
  - CDF 2020.02
  - SmartConnectors 7.14.0

- **Integration with Micro Focus Container Deployment Foundation**

  ArcSight Interset works within CDF, Kubernetes. It uses the ArcSight SmartConnector to collection and refine data, which then streams into Kafka. Kafka passes the data into Vertica Analytics database. The Analytics results are read by the Interset API and can be viewed on the Interset UI.

- **Risk V2 Implementation**

  ArcSight Interset 6.0.0 Risk engine version 2.0 is a standalone risk engine that computes entity risks on any given set of anomalies. There are several benefits for this change such as more traceability of change in entity risk to individual anomalies.

- **Vertica Support Enhancements**

  Micro Focus supports the Vertica Analytic Database 9.2.x running on the following 64-bit operating systems and versions on x86_x64 architecture. In general, Micro Focus provides support for the Vertica Analytic Database, not its host operating system, hardware, or other environmental elements.

- **User Experience Improvements**

  The primary ArcSight Interset 6.0.0 UI remains the same as the previous versions. The improvement with the UX is the new grid based search capability with the Event Viewer. With Event Viewer you can customize search queries and filter results.

Unsupported Features

The following features are currently not being supported in ArcSight Interset 6.0.0. These are currently projected for future release versions.

- **Multi Tenancy** is unsupported for ArcSight Interset Standard Edition 6.0.
- Interset “**Workflow**” is unsupported in ArcSight Interset Standard Edition 6.0.

⚠ **Important:** One Node Cluster has specific configuration parameters required in CDF. For further details regarding a single node setup contact Micro Focus Customer Support at interset.support@microfocus.com.

Known Issues

The known issues include issues as of April, 2020 for ArcSight Interset 6.0.0.

ArcSight Interset 6.0.0

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]

Bad Message 413 reason: Request Entity Too Large

While logging to the Interset UI, a bad message **413** is encountered. To resolve this issue, clear the cookies for the site and login again.

[FT-20164]

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 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]

Repartition Percentage Threshold

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

To avoid this situation, ensure that you set a value between 0.7 and 1.0.

[FT-20011]

Prefix filtering does not work in CDF for Event Viewer

When searching for a prefix string in Event Viewer within a CDF environment, the result of the query is of all the occurrences of the string. This is a known issue and will be addressed in a later version.

[FT-20239]

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

In the **CDF Management Portal > Configure/Deploy** page **> Interset**, 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.

As a workaround, you need to 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 Vertica with HDFS. For more information, see the "Configure Vertica with HDFS" section in *Interset 6.0.0 Deployment Guide for CDF.*
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

When you view the Logstash logs, you may 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

Though these warnings are displayed, there is no impact in the functionality. Hence, you can ignore these warnings.

[FT-20038]

Swagger UI session expires after 120 seconds of inactivity

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 when re-tried, results in returning an error code of **401**.

To get the correct result, the workaround for this issues is to go back to the Interset UI. Refresh the Interset UI and then use the Swagger UI. The reason for the issue is due to token expiry after 120 seconds. This will be addressed in a later version.

[FT-20234]

Cannot save searches in Event Viewer

When exploring events in the Event Viewer, you can not 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.

There is a workaround to the issue which involves modification of the **investigator.yml**. Please contact Micro Focus Customer Support at **interset.support@microfocus.com** to resolve the issue. This will be addressed in a later version.

[FT-20299]