Micro Focus Security
ArcSight Data Platform Event Broker

Software Version: 2.21

Release Notes

Document Release Date: July 20, 2018
Software Release Date: July 20, 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

What's New in this Release

New Features in Event Broker 2.21

- High availability of Schema Registry
- Support for up to 50 CEB processors
- Allow overriding Kafka and other application properties
- Updated certificate management
- Upgraded version of Kafka Platform
- Upgraded version of Kafka Manager GUI
- CEB handling syslog messages without source data if not available

New Features in ArcSight Installer 1.50

- Pre-check script can be invoked ahead of actual install
- Updated versions of Docker (1.13.1), K8s (1.8.3), and more
- Customizable installation directory
- Built-in support for graceful shutdown/reboot of a node
- Updated certificate management (support for intermediate CAs)
- Support for SELinux in “enforcing” mode
- New support tool: $K8S_HOME/tools/support-tool/support-dump

Supported Platforms and Browsers

For details on Event Broker platform and browser support, refer to the ADP Support Matrix document available from the Micro Focus Community.

Event Broker Documentation

In addition to these Release Notes, the following documents are available in PDF format for download from the ArcSight Software Community.

- *ArcSight Data Platform Support Matrix:* Provides integrated support information such as platform and browser support for ADP ArcMC, Event Broker, and SmartConnectors and Collectors.
- *Event Broker Deployment Guide:* Describes how to deploy and configure Event Broker.
- *Event Broker Administrator's Guide:* Describes how to configure, and manage Event Broker.

Upgrading to Event Broker 2.21

This version of Event Broker supports upgrade from Event Broker 2.20. The procedure includes upgrading the ArcSight Installer from version 1.40 to 1.50, and then using the Upgrade capabilities in ArcSight Installer to upgrade the Event Broker images. See the section titled 'Upgrading to Event Broker 2.21' in the Event Broker Deployment Guide for the complete procedure. See the ADP Support Matrix for upgrade supported versions and path.

Fixed Issues

This release contains the following fixed issues.

Key	Release Note Description
EB-1214	Issue: The number of routing rules that can be created within a single route was limited due to a bug. Fix: The number of routing rules that can be created within a single route is no longer limited.
EB-938	Issue : The Kafka broker node can become unavailable due to KAFKA-3984 : "Broker doesn't retry reconnecting to an expired Zookeeper connection" Fix: The new version of Kafka 1.1.0 used in EB 2.21.0 fixed KAFKA-3984 (as KAFKA-5473)

Known Limitations

Event Broker is known to have the following limitations.

EB-631	In some cases, when Kafka goes down and then recovers, there can be a difference in the event count of CEF and Avro topics. Under failure conditions it is expected that there may be data duplication since messages are re-delivered. The redelivery leads to some duplicate events. This is a known Kafka behavior.

Open Issues

This release contains the following open issues.

Key	Release Note Description
INST-1382	Issue: After a successful upgrade of the Arcsight Installer, the arcsight-installer.properties file is reset to the default value. The configuration file is located here: ${K8S_HOME}/installer/arcsight-installer.properties EB will continue to run with the previous configuration until undeployed and re-deployed. The arcsight-installer.properties file is read only during new deployment. Workaround: Copy the original arcsight-installer.properties file from the temporary backup file used during the upgrade to the $ {K8S_HOME}/installer/arcsight-installer.properties location by running the following cmd: # cp /path/to/upgrade/backup/folder/arcsight-installer-1.50.9/arcsight-installer.properties ${K8S_HOME}/../installer/ Verify and change parameter values as necessary before deploying the eventbroker.
INST-1370	Issue: While running ./downloadimages.sh --suite investigate -r docker -o arcsightsecurity, the following errors are displayed: 1: q: error: Cannot iterate over null 2: mv: cannot stat ?/var/opt/kubernetes/offline/temp_files/suite-metadata/feature?: No such file or directory Workaround: No action is needed, these errors don't affect the download.
INST-1334	Issue: Unable to access the Investigate UI after upgrading to version 2.20. Workaround: Undeploy and Deploy Investigate.
INST-1300	Issue: When uninstalling the Arcsight installer via the script $K8S_HOME/uninstall.sh, the script may hang. Workaorund: Reboot the machine and run uninstall.sh again or remove the /opt/arcsight/kubernetes directory. Interrupt the script and re-invoke it. If it still hangs, reboot the node, and invoke the script once the server has rebooted.
INST-1236	Issue: hercules-rethinkdb-0 is in CrashLoopBack state after deployment. Workaround: Delete rethink-db pod and let it recreate itself, together with install container it will retry to reach the vault again.

Key	Release Note Description
INST-1230	Issue: A long running cluster with Investigate deployed may experience an out of memory condition requiring a reboot of a cluster node. Workaround: Monitor the cpu / memory usage of pods / cluster nodes, for example using the commands 'kubectl top node' and 'kubectl top pod <pod name> -n <pod namespace>'
INST-1186	Issue: Installer doesn't properly handle interface names when VLAN tagging is configured. Workaround: Please Contact Support to help address this issue.
INST-1143	Issue: The Zookeeper cluster is out of sync at times and Kafka fails to select a leader after losing multiple brokers, causing Kafka to fail. This occurs on Zookeeper startup, due to a timing problem. It may also occur on a Zookeeper cluster. Workaround: Undeploy and then redeploy Event Broker.
INST-1118	Issue: The User is never logged out of the Arcsight Installer Deployment page. Workaround: Move to a different page.

EB-1330	Issue: A pod that is restarted after running successfully for a period of time may appear in ImagePullBackOff or ErrImagePull state.
	
	Workaround: The container image needs to be reloaded. First, identify the missing image by looking at the events for the pod:
	
	$ kubectl describe <pod name> -n <pod namespace>
	
	The events section should show the name of the image that Docker can't find. Given the image name, look for the tarball which contains that image, e.g. under $K8S_ HOME/images.
	
	Next, load the image into Docker via:
	$ docker load -i /path/to/image/file.tgz
	e.g.:
	$ docker load -i/opt/arcsight/kubernetes/images/kubernetes-vault-init-0.2.1.tgz
	
	Upon a successful load, docker will report that the image is loaded <image name>
	e.g.:
	"Loaded image: localhost:5000/kubernetes-vault-init:0.2.1"
	
	Push that image to the private Docker registry:
	$ docker push <image name>
	e.g.:
	$ docker push localhost:5000/kubernetes-vault-init:0.2.1
	
	Verify that the image can now be pulled:
	$ docker pull <image name>
	e.g.:
	$ docker pull localhost:5000/kubernetes-vault-init:0.2.1

EB-1132	Issue: The recovered kafka/zookeeper is not added to the cluster. Workaround: Please contact customer support if you encounter this issue.

Key	Release Note Description
EB-1124	Issue: eb-web-service pods status shows “running” but displays the following error message: "JMX client heartbeatjava.lang.OutOfMemoryError" Workaround: If you see this issue, please restart web service by executing the kubectl delete command on the web service pod. After the web service pod restarts, ArcMC will connect with the proper status.
EB-909	Issue: If the stream processor stops processing events and you see “ConcurrentModificationException” with the exception stack trace pointing to “org.apache.kafka.common.internals.PartitionStates.partitionSet” then this is the known Kafka defect KAFKA-4950. Workaround: Restart the affected stream processor using the 'kubectl delete' command. Example if c2av stream processor is affected : # kubectl delete eb-c2av-processor-927505239-xc1ol -n arcsighteventbroker1 Example if routing stream processor is affected : # kubectl delete eb-routing-processor-0 -n arcsighteventbroker1
EB-631	In some cases, when Kafka goes down and then recovers, there can be a difference in the event count of CEF and Avro topics. Under failure conditions it is expected that there may be data duplication since messages are re-delivered. The redelivery leads to some duplicate events. This is a known Kafka behavior.
EB-630	Issue: The Kafka version displayed on Event Broker Manager is not the correct version used by Event Broker. Workaround: None at this moment.

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 (Event Broker 2.21)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!