
Micro Focus Security ArcSight Kafka FlexConnector

FlexConnector Configuration Guide

Document Release Date: July 24, 2019

Software Release Date: July 24, 2019



Legal Notices

Copyright Notice

© Copyright 2019 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

US. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are US 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://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to [ArcSight Product Documentation Community on the Micro Focus Security Community](#).

Document Changes

Date	Product Version	Description
07/24/2019	1.0	First edition of this guide

Contents

Overview	5
Understanding Kafka	5
SSL encryption and authentication	6
To enable SSL encryption and authentication:	6
To SSL for inter-broker communication:	7
Creating Flex Parsers	7
Advanced Parameters	7
Send Documentation Feedback	9

Overview

The Arcsight Kafka FlexConnector helps you subscribe and collect events from a topic of Kafka server and the topic only contains a specific event type.

This version supports 5 event types:

- JSON
- CEF
- REGEX
- SYSLOG
- KEY-VALUE.

This is a FlexConnector so you need create your personal parsers before setup connector.

Understanding Kafka

Apache Kafka is a distributed publish-subscribe messaging system and a robust queue that handles a high volume of data and enables you to pass messages from one end-point to another.

Kafka is suitable for both offline and online message consumption.

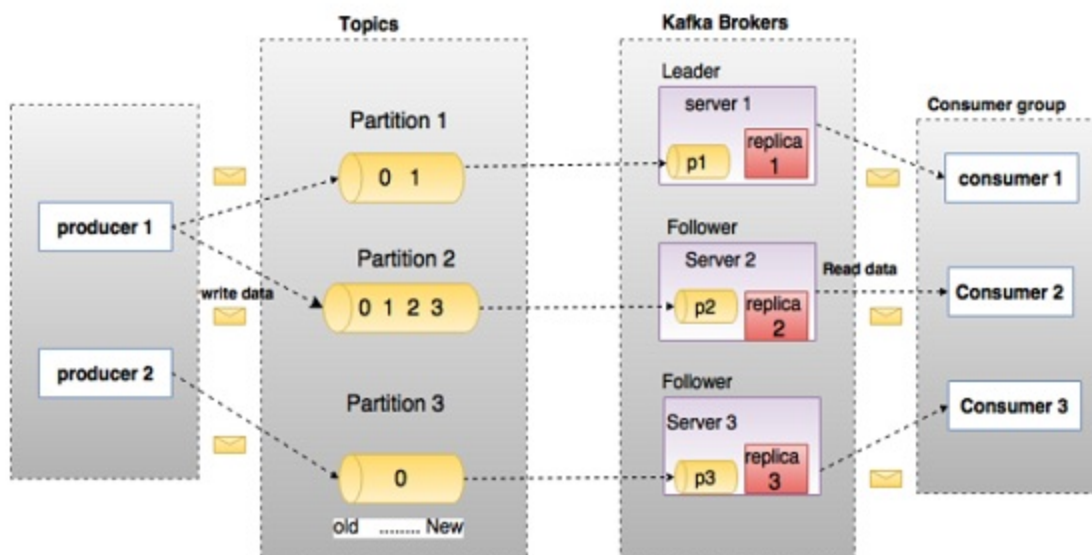
Kafka messages are persisted on the disk and replicated within the cluster to prevent data loss. it is built on top of the ZooKeeper synchronization service and it integrates very well with Apache \Storm and Spark for real-time streaming data analysis.

The following diagram illustrates the main terminologies and the table describes the diagram components in detail. A topic is configured into three partitions.

- Partition 1 has two offset factors 0 and 1.
- Partition 2 has four offset factors 0, 1, 2, and 3.
- Partition 3 has one offset factor 0.

The Id of the replica is same as the Id of the server that hosts it.

Assume, you want to install 3 Kafka Flex Connectors to parse data of a topic, you need to increase the partitions of your Kafka server.



For more information about Apache Kafka, see [Apache Kafka Tutorials](#)

SSL encryption and authentication

About

The Arcsight Kafka FlexConnector provides secure connection to Kafka servers.

Procedure

To enable SSL encryption and authentication:

1. Configure the truststore, keystore, and password in the server.properties file of every broker.
2. Passwords are directly stored in the broker configuration file, so restrict the access to these files via file system permissions

```
ssl.truststore.location=/var/private/ssl/kafka.server.truststore.jks
```

```
ssl.truststore.password=test1234
```

```
ssl.keystore.location=/var/private/ssl/kafka.server.keystore.jks
```

```
ssl.keystore.password=test1234
```

```
ssl.key.password=test1234
```

Note `ssl.truststore.password` is optional but highly recommended. If a password is not set, access to the truststore is still available, but integrity checking is disabled.

To SSL for inter-broker communication:

1. Add the following property to the broker properties file (it is **PLAINTEXT** by default).
`security.inter.broker.protocol=SSL`
2. Configure the Apache Kafka® broker ports which listen to client and inter-broker **SSL** connections. Configure the **`listeners`** and the **`advertised.listeners`**, in case the value is different.

`listeners=SSL://kafka1:9093`

`advertised.listeners=SSL://0.0.0.0:9093`

3. Configure both **SSL** ports and **PLAINTEXT** ports if:

- SSL is not enabled for inter-broker communication.
- Some clients connecting to the cluster do not use SSL.

`listeners=PLAINTEXT://kafka1:9092,SSL://kafka1:9093`

`advertised.listeners=PLAINTEXT://0.0.0.0:9092,SSL://0.0.0.0:9093`

Note `advertised.host.name` and `advertised.port` configure a single **PLAINTEXT** port are incompatible with secure protocols. Use **`advertised.listeners`** instead.

4. To enable the broker to authenticate clients (2-way authentication), you need to configure all the brokers for client authentication. We recommend setting this value to **`required`**.

`ssl.client.auth=required`

Note Do not use **`requested`** as it creates a false sense of security.

Important: If any of the SASL authentication mechanisms are enabled on a given listener, the SSL client authentication is disabled, even if **`ssl.client.auth=required`** is previously configured. The broker will only authenticate clients via SASL on that listener.

Creating Flex Parsers

To create a flex Parser, see the [ArcSight FlexConnector Developer's Guide](#)

Advanced Parameters

If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

Parameter	Setting
<code>bootstrap.servers</code>	Host-IP
<code>group.id</code>	Use for multiple connectors in a Kafka topic.
<code>max.poll.records</code>	The maximum number of records returned in a single call to a <code>poll()</code> . Default value is 500 (maximum).
<code>auto.commit.interval.ms</code>	The frequency in milliseconds in which the consumer offsets are auto-committed to Kafka if the <code>enable.auto.commit</code> value is set to True . 5000 milliseconds.
<code>reconnect.backoff.ms</code>	The base waiting time, before attempting to reconnect to a given host. It avoids repeatedly connecting to a host in a tight loop. This backoff applies to all client connection attempts to a broker: 50 times
<code>retry.backoff.ms</code>	The amount of waiting time before attempting to retry a failed request to a given topic partition. It avoids repeatedly sending requests in a tight loop under some failure scenarios: 100 times.
<code>request.timeout.ms</code>	It controls the maximum amount of waiting time for a request response. If the response is not received before the timeout elapses, the client resends or fails the request (if the connection attempts have reached the limit: 30000 milliseconds).
<code>client.id</code>	An id string to pass to the server when making requests. It tracks the request source beyond just ip/port, by allowing a logical application name to be included on the server-side login request. For tracking: arcsight
<code>heartbeat.interval.ms</code>	The expected time between heartbeats to the consumer coordinator when using Kafka's group management facilities. Heartbeats are used to ensure that the consumer's session stays active and facilitates rebalancing when new consumers join or leave the group. The value must be set lower than <code>session.timeout.ms</code> and higher than 1/3 of that value. It can be adjusted even lower to control the expected time for normal rebalances.
<code>connections.max.idle.ms</code> (Idle connections timeout)	The server socket processor threads close the connections that appear idle for more than 600000 ms.
<code>auto.offset.reset</code>	It can be executed when there is not an initial offset in Kafka or if the current offset does not exist in the server anymore.

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 Configuration Guide (Kafka FlexConnector)

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!