Financial Crimes Insight with Watson
Last updated: 2017-05-30

Financial Crimes Alerts Insight with Watson Solution Guide

Note
Before using this information and the product it supports, read the information in “Notices” on page 19.

Product Information

This document applies to and may also apply to subsequent releases.

Licensed Materials - Property of IBM

Contents

Introduction

IBM® Financial Crimes Alerts Insight with Watson™ is designed to reduce the overall cost and maintenance of monitoring transactions while also complying with anti-money laundering regulations. The solution is designed to save time and money while also protecting financial institutions from fraud.

Financial Crimes Alerts Insight with Watson helps financial and non-financial institutions to reduce exposure to money laundering and terrorism financing activities. It effectively monitors bank customer transactions daily and by using customer historical information and account profiles, it provides a whole picture to the bank management.

Audience

This guide is intended for administrators and users of the solution. It provides information on installation and configuration of the solution, and information about using the solution.

Finding information and getting help

To find product documentation on the web, access IBM Knowledge Center (www.ibm.com/support/knowledgecenter).

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. Some of the components included in the have accessibility features. For more information, see "Accessibility features," on page 17.

The HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no added accessibility features.

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.

Samples disclaimer

Sample files may contain fictional data manually or machine generated, factual data that is compiled from academic or public sources, or data that is used with permission of the copyright holder, for use as sample data to develop sample applications. Product names that are referenced may be the trademarks of their respective owners. Unauthorized duplication is prohibited.

Chapter 1. Solution overview

This section will provide you with a high-level overview of the IBM Financial Crimes Alerts Insight with Watson solution.

The IBM Financial Crimes Insight with Watson solution

The IBM Financial Crimes Insight with Watson solution uses advanced analytics to detect and prevent financial crime before it happens while investigating occurrences to minimize negative financial impact.

Financial crimes are growing in frequency and complexity and technological advances have provided malicious insiders and organized criminals more opportunity to commit crimes. At the same time, business must remain compliant. New regulatory guidelines continue to arise with increased scrutiny and complexity, challenging even the most advanced compliance programs.

Suspicious activity reports (SARs) increasingly cross boundaries between fraud, cyber and anti-money laundering (AML), further increasing the complexity. Regulators are pushing for more detailed reviews of implementations, especially for knowing your customer (KYC) requirements.

Keeping up with compliance risks can be extremely difficult and costly, with high false positive rates.

The solution

- Continuously harnesses a powerful array of advanced analytics that are available to proactively fight the long-term war against financial criminals on multiple fronts.
- Helps you to more effectively resolve identities, relationships and ambiguous patterns with entity and predictive analytics, broader cross channel visibility, and stronger risk scoring.
- Continuously adapts and embeds new operating models through retrospective forensic and big data techniques.
- Helps accelerate investigations and the management of cases through SAR filings with improved triage alerts, automation, and deep mining of data sets.

Chapter 2. Configuring access

Before you can use IBM Financial Crimes Alerts Insight with Watson, you must configure access to your environment.

Overview of security in IBM Financial Crimes Alerts Insight with Watson

IBM Financial Crimes Alerts Insight with Watson does not contain a registry of user IDs and passwords. Instead, it relies on a third-party registry. Secure data access by creating a LDAP registry, or by creating a single user registry.

Financial Crimes Alerts Insight with Watson is not a standalone application and needs to be launched from a case manager application.

If single-sign on (SSO) has been configured for both the case manager and with Financial Crimes Alerts Insight with Watson, you will not see the login screen. Financial Crimes Alerts Insight with Watson will share a session with the case manager, so you will be taken directly to the user interface when launching the Financial Crimes Alerts Insight with Watson.

If SSO has not been configured, LDAP will be used to authenticate. In this case, when launching the Financial Crimes Alerts Insight with Watson user interface, you will first need to log in with your LDAP credentials.

When you log in to Financial Crimes Alerts Insight with Watson, the solution will authenticate you by ensuring that your user ID exists in the third-party user registry and that the provided password of the user ID is correct.

Financial Crimes Alerts Insight with Watson also ensures that you are authorized to access the solution. This is accomplished by verifying the group in which you belong and ensuring that the group is authorized to access Financial Crimes Alerts Insight with Watson.

The groups that are authorized to access Financial Crimes Alerts Insight with Watson can be configured in the `config.js` file located in the `config/ folder`. The `config.security.groupToRoles` object contains two roles: user and admin. Each of these roles is mapped to a group. Modify the name of the group to match groups in your user registry that map to these roles.

LDAP integration

In order to integrate with a LDAP server, you must configure IBM Financial Crimes Alerts Insight with Watson to connect to the LDAP server. You must also map certain user properties in the LDAP system to Financial Crimes Alerts Insight with Watson properties of the user.

About this task

All configuration is done in the Financial Crimes Alerts Insight with Watson `config.js` file located in the `config/ folder`.

To configure Financial Crimes Alerts Insight with Watson to connect to the LDAP server, edit the `config.security.ldap.passportOptions.server` object:

url The LDAP server in which to connect. For instance, `ldap://localhost:389`.

bindDn
The LDAP user in which to perform authentication. For instance, `cn='root'`.

bindCredentials
Password for bindDn.

searchBase
A LDAP expression that points to the object containing the users. For instance, `o=users`, `o=example.com`.

searchFilter
A LDAP search filter used to search for users who are logging in. For instance, `(uid={{username}})`.

To configure how Financial Crimes Alerts Insight with Watson maps certain user properties in the LDAP repository, edit the `config.security.ldap.profile` object:

id The LDAP property that contains the user's ID.

email The LDAP property that contains the user's email address.

displayName
The LDAP property that contains the user's display name.

groups
The LDAP property that contains the groups in which the user belongs.

SSO integration

IBM Financial Crimes Alerts Insight with Watson can use an existing SSO infrastructure to authenticate and authorize users. Financial Crimes Alerts Insight with Watson supports the SAML standard for this integration. In this configuration, you must register Financial Crimes Alerts Insight with Watson as a service provider with your existing identity provider.

About this task

In order to integrate with a SSO infrastructure, you must configure Financial Crimes Alerts Insight with Watson to connect to the identity provider. You will also need to map certain user properties in the identity provider to Financial Crimes Alerts Insight with Watson properties of the user.

All configuration is done in the Financial Crimes Alerts Insight with Watson `config.js` file located in the `config/ folder`. To configure Financial Crimes Alerts Insight with Watson to connect to the identity provider, edit the following properties in the `config.security.saml` object:

entryPoint
The URL to the identity provider entry point.

issuer The issuer string to supply to the identity provider.

To configure how Financial Crimes Alerts Insight with Watson maps certain user properties from the identity provider, edit the following properties in the `config.security.saml` object:

profileNameIdProp
The LDAP property that contains the user's ID.

profileEmailProp
The LDAP property that contains the user's email address.

profileDisplayNameProp
The LDAP property that contains the user's display name.

Integration with a case manager application

IBM Financial Crimes Alerts Insight with Watson can be launched via an alert produced by a case manager application.

The following configurations must be made in the case manager application to support integration with Financial Crimes Alerts Insight with Watson:

- In the case manager application, configure the hostname and port on which Financial Crimes Alerts Insight with Watson is running.
- In the case manager application, provide a link to Financial Crimes Alerts Insight with Watson when displaying alert information.
- In Financial Crimes Alerts Insight with Watson, the link to the alert will be in the following form: `https://<aml_hostname>:<aml_port>?external_alert_id=<xxxx>` where `<xxxx>` is the ID of the alert in the case manager application.

After successful configuration, users can follow the alert link in the case manager application to view additional details of the alert, including how the alert was scored, in Financial Crimes Alerts Insight with Watson.

Note: If SSO is not enabled and you do not have an existing Financial Crimes Alerts Insight with Watson session open, then you must log in to Financial Crimes Alerts Insight with Watson to view the alert details.

Chapter 3. Configuration tasks

There are some aspects of IBM Financial Crimes Alerts Insight with Watson that can be configured to suit your business needs.

Set analytic thresholds

Some analytic rules in IBM Financial Crimes Alerts Insight with Watson have configurable thresholds that you can adjust to control when a rule violation is triggered. The thresholds are contained in JSON files. When you edit the threshold values, the new values are applied the next time that the analytics are run.

Rounding rule

The rounding rule identifies the originator-beneficiary pairs that are receiving or sending funds in large round-dollar amounts. The round-dollar amounts are amounts greater than $1,000 where the values end in "000.00." The rule generates an alert for any pairs that violate the threshold within a month.

```
{
 "TenderType": ["ATM","Wire"],
 "MinSingleTxAmt": 1000,
 "MinTotalTxCount": 1,
 "MinPercentRDTx": 0.05
}
```

- `TenderType` is the tender types that are evaluated in this rule.
- `MinSingleTxAmt` is the minimum transaction amount that triggers this rule.
- `MinTotalTxCount` is the minimum number of round-dollar transactions that exceed the `MinSingleTxAmt` amount that triggers this rule.
- `MinPercentRDTx` is the minimum percent of round-dollar transactions to the total number of transactions that triggers this rule.

Scoring function

The overall risk score is a function of multiple subscores from different analytical models. The contribution of each subscore to the overall risk score can be adjusted through a `subscore_weight` file.

Chapter 4. Using IBM Financial Crimes Alerts Insight with Watson

This section will introduce you to key concepts of the IBM Financial Crimes Alerts Insight with Watson user interface.

IBM Financial Crimes Alerts Insight with Watson interface overview

The IBM Financial Crimes Alerts Insight with Watson user interface provides an at-a-glance view into suspicious activity in the form of alerts.

This section provides a high-level overview of the basic concepts you will need in order to make a decision about an alert and to summarize your findings.

Watson Insight Score
This score represents the secondary score that is generated by the analytics. This provides an indication of the risk of the alert and is not meant to be a confidence score.

Entity Summary
This panel is a summary of the entity that triggered the alert. This entity can be an individual, a group, or a corporation. The summary includes information about any related parties, any known name variances, including aliases for the current entity, and any identifying properties known about the current entity (for instance, DOB, gender, telephone number, address, country of residence, SSN, tax ID).

Key Insights
This section provides a summary of all insights found for the alert.

True/False Positive Indicator
This is a summary that indicates whether the alert is likely to require further investigation (possibly a true positive) or not likely to require further investigation (a possible false positive).

Insight Summary
This is a widget that shows how the insights fall on a scale of riskiness. There are tiles for each insight that also serve as anchors for the insights.

Insights
The user interface consists of insights generated by the analytics. Together, these make up the components of the **Watson Insight Score**. Each insight is displayed as a separate section which contains a brief explanation about the insight, along with a display in the form of a map, or bar or line graph, and a table of transaction data.

Types of Insights
Each insight is generated based on the available data and thresholds that are set for various analytics. The combination of all the insights make up the Watson Insight Score. Types of insights that you may see include:

- **Jurisdictions**. This is displayed when there are transactions made in special jurisdictions (for instance, transactions made with a crime ring). Tender types include Wire or IATS.
- **Structuring**. This insight is displayed when there are an unusual sequence of transactions or patterns between two parties:

Wire High percentage of transactions during a certain time between two parties.

Cash A certain number of cash deposits that fall within a certain range where the total sum is greater than a specific threshold (for example, 5 or more cash deposits between $3,000 and $10,000 totaling more than $30,000).

Check At least a certain number of checks for a particular range in a certain time frame (for example, at least two checks between $9,250 and $10,000 in a one day period).

- **Manipulated Amount**. This insight is displayed when there is at least one transaction of a high value.

  IATS For example, at least one individual transaction is a minimum of $10,000.

  Check For example, at least one check is over $10,000.
- **Profile Change**. This insight is displayed when there is an unusual change in the total count and total amount of transactions for a specific amount.

  Wire For instance, the total amount or count in the current month is greater than a specific threshold.
- **Funds Turnover**. This insight is displayed when there is an unusual frequency of transactions. An example is seeing a large amount of debit and credit within a short period of time.
- **Location**. This insight is displayed when there are transactions made in high risk countries. For example, a high amount of transactions in high risk countries.
- **Flipping**. This insight is displayed when there is an unusual frequency of transactions. For example, a large amount of trade within a short period of time.

Narrative Generation

In order for an analyst to summarize their findings from Financial Crimes Alerts Insight with Watson, the solution provides the ability to generate a narrative. The analyst can select which insights they would like to include in the narrative by selecting the option to **Add Insight to narrative** from each insight, and the narrative can be generated by clicking on the **Generate Narrative** button. Then the analyst can select any additional insights they would also like to include. The summaries for each insight are consolidated in a text area on the narrative generation dialog, into which the analyst can add any extra details. From there, the analyst can download the narrative as a text file that they can then edit in another program, or attach in the case manager.

Generating a narrative

IBM Financial Crimes Alerts Insight with Watson provides an analyst with the ability to summarize their findings by generating a narrative about a particular entity.

About this task

You can either generate a narrative for every insight about a specific entity, or you can select which insight to include in the narrative.

Procedure

1. To generate a narrative for every insight about an entity, click the **Generate Narrative** button. A dialog box is displayed with the name of the entity, and details about the insights for that entity.

   Note: The dialog text box is editable. You can add or delete text.
2. To download the narrative, click the **Download** button in the narrative dialog box. The narrative is downloaded as a text file.
3. To select specific insights to include in your narrative, click the **Add Insight to narrative** button for each insight you want to add. Once it has been added successfully, an **Added to narrative** message is displayed.
4. Click the **Generate Narrative** button. All of the insights you have selected will be checked in the dialog box. If you want to add another insight, select the check box for that insight. The text area is populated with the summaries of all the insights you have selected.

Chapter 5. Troubleshooting

If you encounter an issue, you can use a few different third party applications to view log files generated by IBM Financial Crimes Alerts Insight with Watson.

Log messages

IBM Financial Crimes Alerts Insight with Watson uses Logstash to collect and normalize log files.

Logstash

Logstash is a data processing pipeline that collects, parses, and stores logs for future use.

For more information about Logstash, see the product page (https://www.elastic.co/products/logstash) or the logstash page on Github (https://github.com/elastic/logstash).

Log files are collected from the following services:

- Ambari
- Flume
- HBase
- Hadoop
- Hive
- Mapreduce
- Spark
- YARN
- Zookeeper
- Node.js

Because these services do not have identical logging formats, Logstash is used to parse the log and normalize the data so that it can easily be queried and searched.

Logstash uses filters and codecs to parse the incoming data. Logstash includes several default patterns, but you can also customize the filters by using the grok plugin. You use the plugin to analyze word patterns and to map the entries from the log files to the dedicated fields and key value pairs. The codec plugins are provided by Logstash to encode and decode common formats, such as JSON.

More resources:

- For more information about using Logstash, see the product documentation (https://www.elastic.co/guide/en/logstash/5.2/index.html).
- For more information about the grok plugin, see the product documentation (https://www.elastic.co/guide/en/logstash/5.2/plugins-filters-grok.html).
- For more information about the grok patterns that are used, see the grok-patterns information on Github (https://github.com/elastic/logstash/blob/v1.4.2/patterns/grok-patterns).

- For more information about the codec plugins, see the product documentation (https://www.elastic.co/guide/en/logstash/5.2/codec-plugins.html).

Elasticsearch

IBM Financial Crimes Alerts Insight with Watson uses Elasticsearch to store, search, and analyze large volumes of data.

For more information about Elasticsearch, see the product documentation (https://www.elastic.co/guide/en/elasticsearch/reference/1.4/getting-started.html).

An Elasticsearch document is used for every log file event, rather than every line in a log file, because some log files have multiple lines per logging event. Documents are formatted in JSON.

The documents are collected into an index or into multiple indices. For example, Financial Crimes Alerts Insight with Watson sends all of the Ambari documents into an index that is named `logstash-ambari`. Multiple Ambari log files from multiple servers are parsed and sent into the `logstash-ambari` index so that they can be easily searched. The following list shows the indices that IBM Financial Crimes Alerts Insight with Watson creates and the services that feed into each index:

- Ambari → logstash-ambari
- Flume → logstash-flume
- HBase → logstash-hbase
- Hadoop → logstash-hdfs_audit
- Hive → logstash-hive
- Mapreduce → logstash-mapreduce
- Spark → logstash-spark
- YARN → logstash-yarn
- Zookeeper → logstash-zookeeper
- Node.js → logstash-node

For more information about using Elasticsearch, see the product documentation (https://www.elastic.co/guide/en/elasticsearch/reference/5.2/index.html).

Kibana

You can use Kibana to search, view, and interact with data that is stored in Elasticsearch indices.

If you do use it, Kibana must be installed on the same machine as Elasticsearch.

For more information about using Kibana, see the product documentation (https://www.elastic.co/guide/en/kibana/5.2/index.html).

Filebeat

You can also use Filebeat to monitor log directories and send the log files to Logstash or Elasticsearch for indexing.

IBM Financial Crimes Alerts Insight with Watson provides separate configuration files for each service from which log data is collected.

The following list contains the Filebeat configuration files that are used to harvest log data:

- filebeat_ambari.yml
- filebeat_flume.yml
- filebeat_hbase.yml
- filebeat_hdfs_audit.yml
- filebeat_hive.yml
- filebeat_mapreduce.yml
- filebeat_spark.yml
- filebeat_yarn.yml
- filebeat_zookeeper.yml
- filebeat-node.yml

For more information about Filebeat, see the product documentation (https://www.elastic.co/guide/en/beats/filebeat/5.2/index.html).

Appendix. Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products.

For information about the commitment that IBM has to accessibility, see the IBM Accessibility Center (www.ibm.com/able).

HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no added accessibility features.

Notices

This information was developed for products and services offered worldwide.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Software Group
Attention: Licensing
3755 Riverside Dr.
Ottawa, ON
K1V 1B7
Canada

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Trademarks

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at " Copyright and trademark information " at www.ibm.com/legal/copytrade.shtml.

Index