IBM Surveillance Insight for Financial Services
Version 2.0.0

IBM Surveillance Insight for Financial Services Installation Guide

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 43.

Product Information

This document applies to Version 2.0.0 and may also apply to subsequent releases.

Contents

Introduction

Use IBM® Surveillance Insight for Financial Services to proactively detect, profile, and prioritize non-compliant behavior in financial organizations. The solution ingests unstructured and structured data, such as trade, electronic communication, and voice data, to flag risky behavior. Surveillance Insights helps you investigate sophisticated misconduct faster by prioritizing alerts and reducing false positives, and reduces the cost of misconduct.

Some of the key problems that financial firms face in terms of compliance misconduct include:

- Fraudsters using sophisticated techniques thereby making it hard to detect misconduct.
- Monitoring and profiling are hard to do proactively and efficiently with constantly changing regulatory compliance norms.
- A high rate of false positives increases the operational costs of alert management and investigations.
- Siloed solutions make fraud identification difficult and delayed.

IBM Surveillance Insight for Financial Services addresses these problems by:

- Leveraging key innovative technologies, such as behavior analysis and machine learning, to proactively identify abnormalities and potential misconduct without pre-defined rules.
- Using evidence-based reasoning that aids streamlined investigations.
- Using risk-based alerting that reduces false positives and negatives and improves the efficiency of investigations.
- Combining structured and unstructured data from different siloed systems into a single platform to perform analytics.

IBM Surveillance Insight for Financial Services takes a holistic approach to risk detection and reporting. It combines structured data such as stock market data (trade data) with unstructured data such as electronic emails and voice data, and it uses this data to perform behavior analysis and anomaly detection by using machine learning and natural language processing.

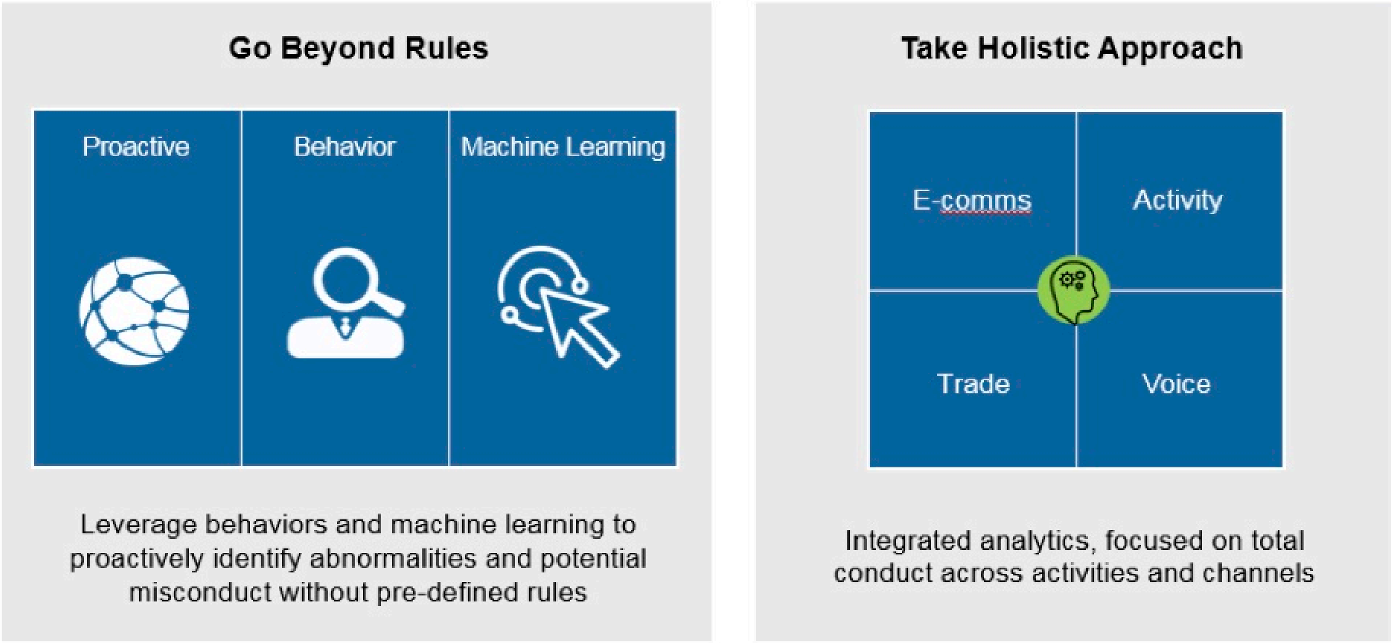

Go Beyond Rules
Proactive
Behavior
Machine Learning
Leverage behaviors and machine learning to proactively identify abnormalities and potential misconduct without pre-defined rules
Take Holistic Approach
E-comms
Activity
Trade
Voice
Integrated analytics, focused on total conduct across activities and channels

Figure 1: Surveillance Insight overview

Audience

This guide is intended for administrators and users of the IBM Surveillance Insight for Financial Services 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 IBM Surveillance Insight for Financial Services have accessibility features. For more information, see Appendix A, “Accessibility features,” on page 41.

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.

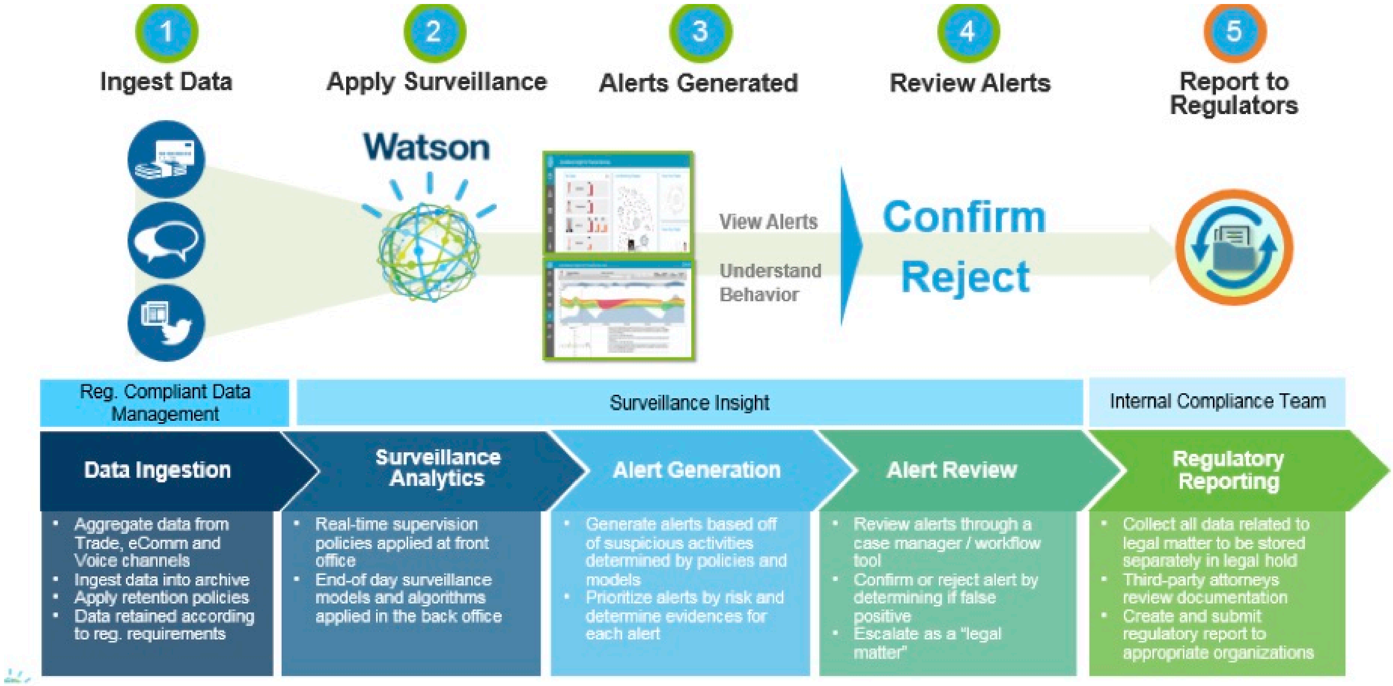
Samples disclaimer

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. IBM Surveillance Insight for Financial Services

IBM Surveillance Insight for Financial Services provides you with the capabilities to meet regulatory obligations by proactively monitoring vast volumes of data for incriminating evidence of rogue trading or other wrong-doing through a cognitive and holistic solution for monitoring all trading-related activities. The solution improves current surveillance process results and delivers greater efficiency and accuracy to bring the power of cognitive analysis to the financial services industry.

The following diagram shows the high-level IBM Surveillance Insight for Financial Services process.



1
Ingest Data
2
Apply Surveillance
3
Alerts Generated
4
Review Alerts
5
Report to Regulators
Watson
View Alerts
Understand Behavior
Confirm
Reject
Reg. Compliant Data Management
Surveillance Insight
Internal Compliance Team
Data Ingestion
• Aggregate data from Trade, eComm and Voice channels
• Ingest data into archive
• Apply retention policies
• Data retained according to reg. requirements
Surveillance Analytics
• Real-time supervision policies applied at front office
• End-of day surveillance models and algorithms applied in the back office
Alert Generation
• Generate alerts based off of suspicious activities determined by policies and models
• Prioritize alerts by risk and determine evidences for each alert
Alert Review
• Review alerts through a case manager / workflow tool
• Confirm or reject alert by determining if false positive
• Escalate as a "legal matter"
Regulatory Reporting
• Collect all data related to legal matter to be stored separately in legal hold
• Third-party attorneys review documentation
• Create and submit regulatory report to appropriate organizations

Figure 2: High-level process

1. As a first step in the process, data from electronic communications (such as email and chat), voice data, and structured stock market data are ingested into IBM Surveillance Insight for Financial Services for analysis.
2. The data is analyzed.
3. The results of the analysis are risk indicators with specific scores.
4. The evidences and their scores are used by the inference engine to generate a consolidated score. This score indicates whether an alert needs to be created for the current set of risk evidences. If needed, an alert is generated and associated with the related parties and stock market tickers.
5. The alerts and the related evidences that are collected as part of the analysis can be viewed in the IBM Surveillance Insight for Financial Services Workbench.

After the alerts are created and the evidences are collected, the remaining steps in the process are completed outside of IBM Surveillance Insight for Financial Services. For example, case investigators must work on the alerts and confirm or reject them, and then investigation reports must be sent out to the regulatory bodies as is required by compliance norms.

The solution architecture

IBM Surveillance Insight for Financial Services is a layered architecture made up of several components.

The following diagram shows the different layers that make up the product:

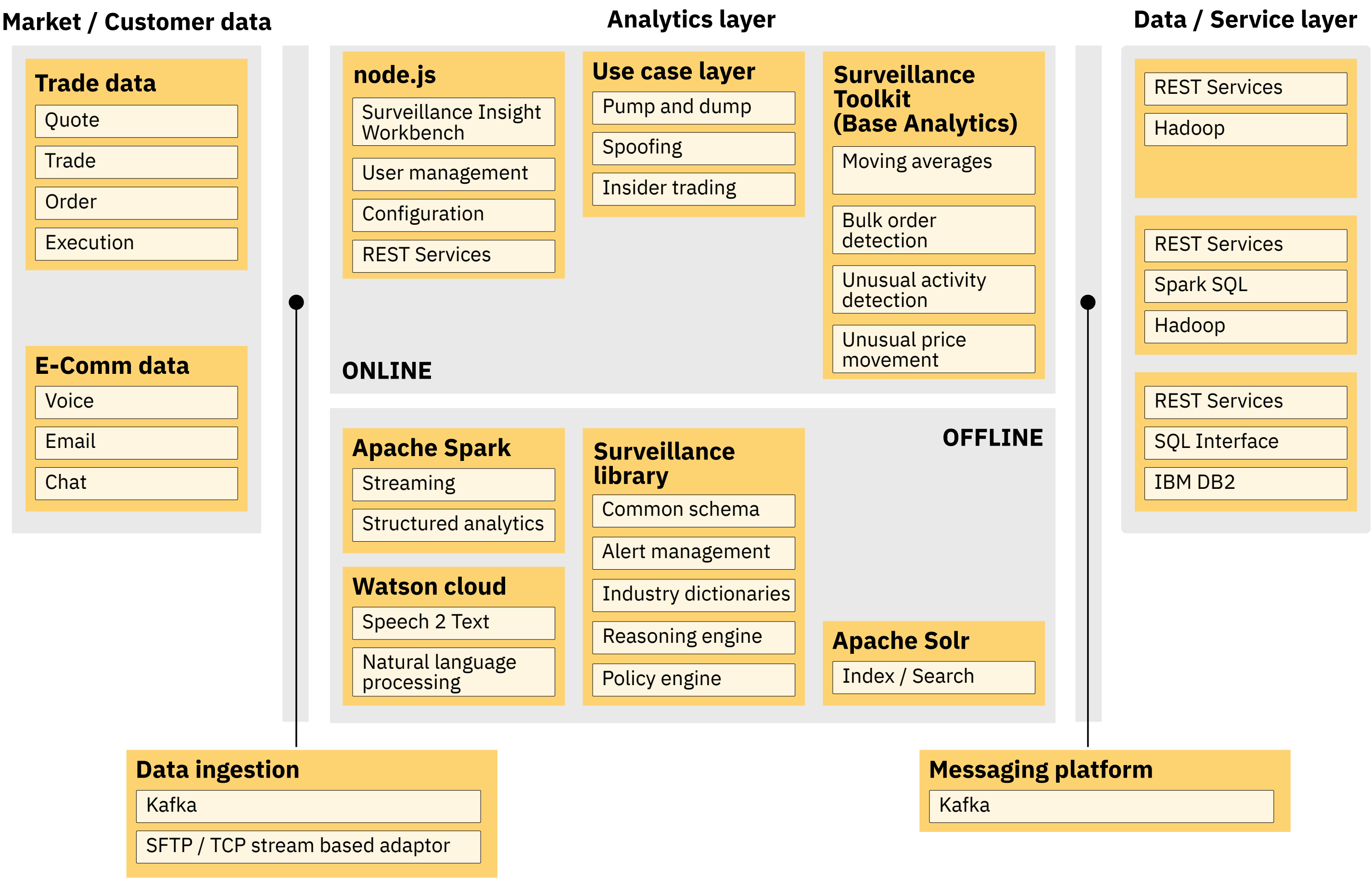


Figure 3: Product layers

- The data layer shows the various types of structured and unstructured data that is consumed by the product.
- The data ingestion layer contains the FTP/TCP-based adaptor that is used to load data into Hadoop. The Kafka messaging system is used for loading e-communications into the system.

  Note: IBM Surveillance Insight for Financial Services does not provide the adaptors with the product.
- The analytics layer contains the following components:
  - The Workbench components and the supporting REST services for the user interfaces.
  - Specific use case implementations that leverage the base toolkit operators.
  - The surveillance library that contains the common components that provide core platform capabilities such as alert management, reasoning, and the policy engine.
  - The Spark Streaming API is used by Spark jobs as part of the use case implementations.
  - Speech 2 Text and the NLP APIs are used in voice surveillance and eComms surveillance.
  - Solr is used to index content to enable search capabilities in the Workbench.
- Kafka is used as an integration component in the use case implementations and to enable asynchronous communication between the Streams jobs and the Spark jobs.
- The data layer primarily consists of data in Hadoop and IBM DB2®. The day-to-day market data is stored in Hadoop. It is accessed by using the spark-sql or spark-graphx APIs. Data in DB2 is accessed by using traditional relational SQL. REST Services are provided for data that needs to be accessed by the user interfaces and for certain operations such as alert management.

The following diagram shows the end-to-end component interactions in IBM Surveillance Insight for Financial Services.

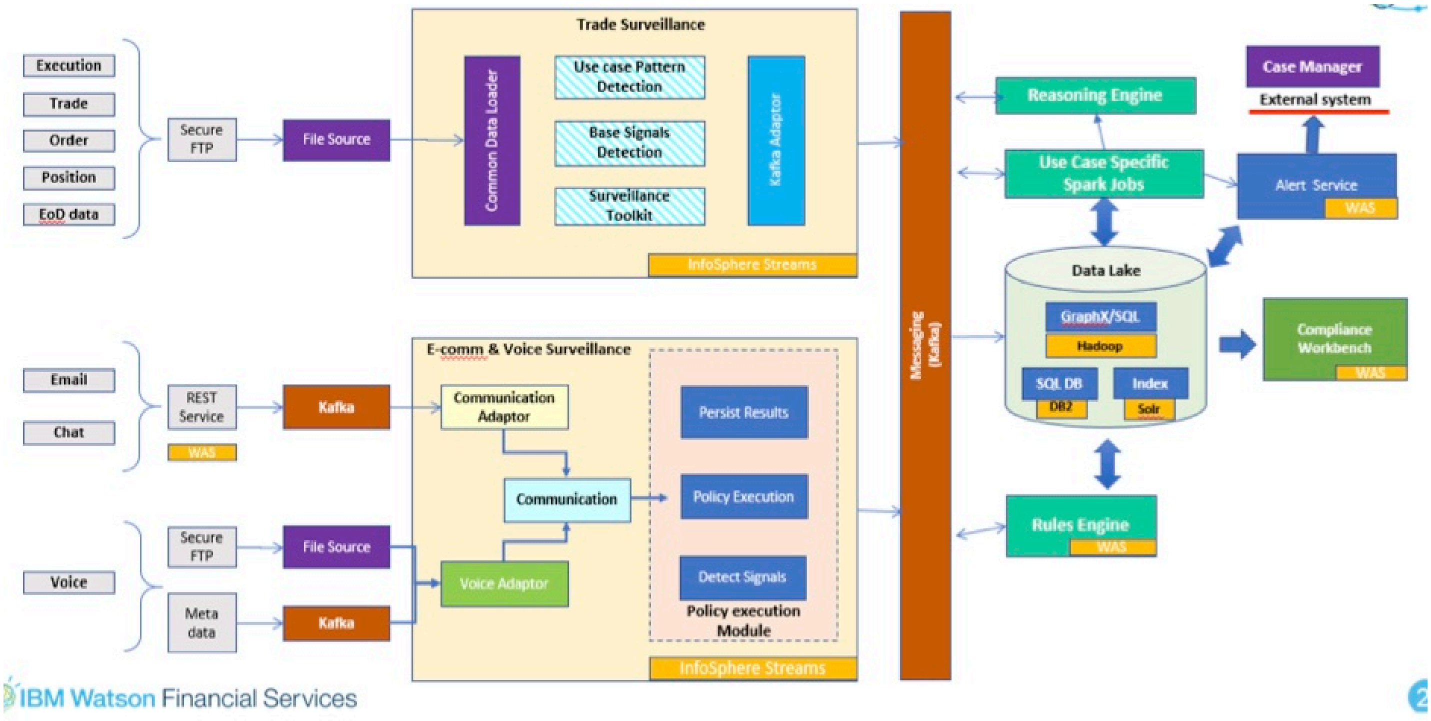


Figure 4: End-to-end component interaction

- Trade data is loaded into Hadoop through secure FTP. The Data Loader Streams job monitors specific folders in Hadoop and provides the data to the use cases that need market data.
- The trade use case implementations analyze the data and creates relevant risk evidences.
- Email and chat data is brought into the system through a REST service that drops the data from third-party sources into the Kafka topic.
- The unstructured data is analyzed by the Streams jobs and the results are persisted to Kafka.
- Voice data is obtained through secure FTP. The trigger for processing the data is then passed on through the Kafka message that contains the metadata about the voice data that needs to be processed.
- After the voice data is converted to text, the rest of the analysis is performed in the same way as the email and chat data is processed.
- The output, or the risk evidences from the use case implementations (trade, ecomm, and voice), are dropped into the Kafka messaging topics for the use case-specific Spark jobs. The Spark jobs perform the post processing after the evidences are received from the Streams jobs.

Chapter 2. Installation tasks

Before you install IBM Surveillance Insight for Financial Services, ensure that the computers that you use meet the minimum requirements for operating systems, prerequisite software, processing, and disk space.

You must deploy the IBM Surveillance Insight for Financial Services to access some of the prerequisite software that you will need.

After the prerequisite software is installed and configured, you can deploy the IBM Surveillance Insight for Financial Services content to complete the installation.

Supported operating systems and hardware requirements

Review the minimum hardware and operating system requirements before you install IBM Surveillance Insight for Financial Services.

For an up-to-date list of environments that are supported by IBM Surveillance Insight for Financial Services, see the IBM Software Product Compatibility Reports (www.ibm.com/support/docview.wss?uid=swg27047153).

The computer on which you run the solution installer and the computer on which you install IBM Surveillance Insight for Financial Services must be running a 64-bit Red Hat Enterprise Linux Server Edition 7.1 operating system.

Hardware requirements

The computer on which you install IBM Surveillance Insight for Financial Services must have the following hardware requirements:

Processors
2 sockets with 6 cores per socket

RAM
32 GB

Disk space
500 GB

User requirements

You must have root or sudo access to install IBM Surveillance Insight for Financial Services.

Setting ulimit values

Before you install IBM Surveillance Insight for Financial Services, ensure that you have appropriate ulimit values. You set the ulimit values in two files: `90-nproc.conf` and `91-nproc.conf`.

Procedure

1. Log in to the computer as the root user or as a user with sudo permissions.
2. Go to the `/etc/security/limits.d` directory.
3. Open the `90-nproc.conf` file for editing. If the file does not exist, you must create it.
4. Add the following lines to the file:

```
*     soft  nproc  100000
root  soft  nproc  unlimited
```

5. Save and close the file.
6. Open the `91-nproc.conf` file for editing. If the file does not exist, you must create it.
7. Add the following lines to the file:

```
* - nofile 100000
```

8. Save and close the file.

9. Restart the computer for the changes to take effect.

Deploy the IBM Surveillance Insight for Financial Services software

IBM Surveillance Insight for Financial Services is deployed on different node computers that host different parts of the solution. Some prerequsite components are required on each of the nodes.

The following diagram provides a high-level overview of the solution architecture.

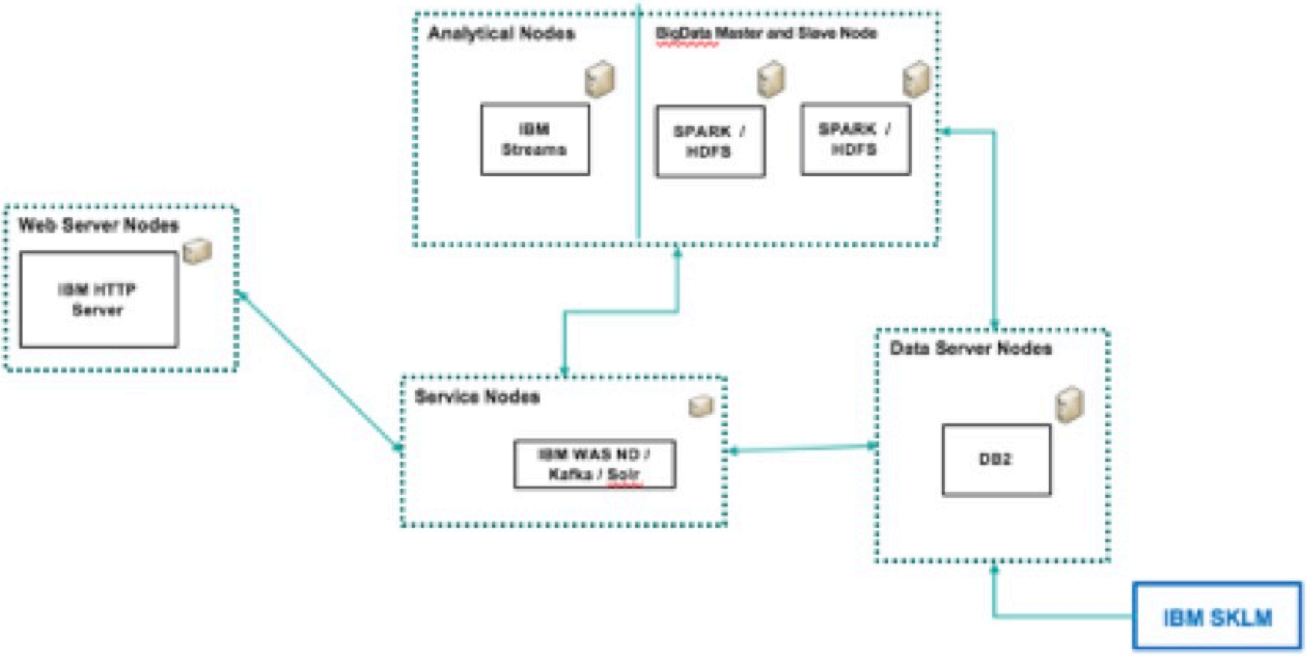


Figure 5: Six node topology

There is a separate installer for each of the four components that comprise IBM Surveillance Insight for Financial Services.

- IBM Surveillance Insight for Financial Services
- IBM Trade Surveillance Analytics
- IBM Electronic Communication Surveillance Analytics
- IBM Voice Surveillance Analytics

The IBM Surveillance Insight for Financial Services base component also deploys some of the prerequisite software that you will need, such as IBM Solr.

Creating directories for the solution installer

You must create a directory on each computer on which you deploy an IBM Surveillance Insight for Financial Services component.

The solution installer uses the /opt/IBM directory to copy license files and other files. This directory must exist on each node computer and on the computer on which you run the solution installer before you run the installation.

Procedure

1. Create an /opt/IBM directory on each computer on which you are going to deploy an IBM Surveillance Insight for Financial Services component.
2. Create an /opt/IBM directory on the computer on which you are going to run the solution installer.

Adding each node computer to the hosts file on all computers

You must add all computers on which you deploy an IBM Surveillance Insight for Financial Services component to the `hosts` file on each other computer.

Procedure

1. On each computer, open the `/etc/hosts` file.
2. Ensure that each node computer is listed in the file.
   For example, ensure that your `hosts` files contain entries in the following pattern:

   ```
   127.0.0.1 localhost.localdomain localhost
   IP_Address computer1.domain.com computer1
   IP_Address computer2.domain.com computer2
   ```
3. Save and close the file.

Modifying the sudoers file for the user who runs the installation

To deploy IBM Surveillance Insight for Financial Services components as a non-root user, you must add that user to the `sudoers` file on each computer.

Procedure

1. Log in as root user.
2. Go to the `etc` directory, and open the `sudoers` file in a text editor.
3. Add the following line for your user:

   ```
   username ALL=(ALL) ALL
   ```
4. Save and close the file.
5. Repeat these steps on each computer on which you deploy an IBM Surveillance Insight for Financial Services component.

Downloading and decompressing the installation files

You download the IBM Surveillance Insight for Financial Services solution from IBM Passport Advantage®, and then decompress the files to run the solution installer.

For more information about the files that you must download, see Downloading IBM Surveillance Insights for Financial Services (www.ibm.com/support/docview.wss?uid=swg24042930).

Procedure

1. Access the IBM Passport Advantage web site.

   Tip: If you receive an error, use a different web browser to access Passport Advantage.
2. Sign in and navigate to the software downloads page.
3. Find the eImages for IBM Surveillance Insight for Financial Services.
4. Download an eImage by selecting the check box beside the name.

   After the download is complete, a **Download Complete** message is displayed. The location of the downloaded files is displayed in the message window.
5. Decompress the installation files.

Opening firewall ports for the solution installer

You can run the `firewall.sh` script to open the ports that are required on the computer on which you are running the IBM Surveillance Insight for Financial Services solution installer.

You must also open ports on the target, or client, computer on which you are installing the IBM Surveillance Insight for Financial Services components. You can use the `client_firewall.sh` script to open the required ports.

The `firewall.sh` script opens the following ports on the solution installer computer:

- 8080 incoming
- 445 incoming
- 9683 incoming
- 22 outgoing

On the target, or client computers, the `client_firewall.sh` script opens the following ports:

- 8080 outgoing
- 445 incoming
- 9683 outgoing
- 22 incoming

Procedure

1. Log on to the computer that contains the solution installer node as the root user or as a user with sudo permissions.
2. Back up your existing firewall settings by typing the following command: `/etc/init.d/iptables save`.
3. Go to the `SolutionInstaller` directory where you decompressed the solution installer files, and run the firewall script by typing the following command: `sh firewall.sh`.
4. Copy the `client_firewall.sh` file onto the computer on which you are going to install IBM Surveillance Insight for Financial Services.
5. On the client computer, back up your existing firewall settings by typing the following command: `/etc/init.d/iptables save`.
6. Go to the directory where you copied the `client_firewall.sh` file, and run the script by typing the following command: `sh client_firewall.sh`.

Starting the solution installer

You use the solution installer to deploy the components. After the solution installer is running, you can access the installer interface from a web browser.

Note: Ensure that you copy the solution installer files to a directory in which you have permissions to execute files.

Procedure

1. Log on to the computer where you decompressed the installation files as the root user or as a user with sudo permissions.
2. Go to the `CNJM9EN/SolutionInstaller` directory where you decompressed the solution installer files.
3. Enter the following command: `sh setup.sh` *`username first_name last_name email password`*.

   You must enter each of the values after `setup.sh`. If you do not enter a password, you will be prompted to enter one. The password must have at least 6 characters.

   After the solution installer starts, open a web browser, and go to the solution installer URL: `https://`*`servername`*`:8080/UI/index.html`.

   The computer on which you are using the browser to access the solution installer must have a screen resolution that is greater than 1024 by 760.

   The solution installer interface can be accessed from a Google Chrome 44, or later, or Mozilla Firefox 38 or later, web browser. It does not run in an Internet Explorer web browser.

Using the solution installer to deploy the base component installation files

Use the solution installer to copy the IBM Surveillance Insight for Financial Services base component files to the computer or computers on which you want to install the solution components.

Procedure

1. Open the solution installer in a web browser.

After the solution installer is running, you can access the URL from any computer from a Firefox or Chrome web browser.

The URL is `https://`*`servername`*`:8080/UI/index.html`, where *`servername`* is the name of the computer where you ran the solution installer.

2. Click **New Configuration**

   If you have a configuration that was previously saved, you can start from that saved configuration.

3. From the **Mandatory Content List** pane, select **Node** and drag it to the **Configuration Editor** pane.

   The **Node** represents the computer where the IBM Surveillance Insight for Financial Services files are to be placed.

   For example, you define a node for the computer where IBM Streams is installed. The **Streams Content** component must be deployed to that computer.

   You can deploy the content on the same computer or on different computers.

4. Select a node object, and enter the following information in the **Property Editor** pane:

   a) Enter a name for the node in **Name**, and press Enter.
   b) Enter the server name in **Host Name**, and press Enter.
   c) Enter the user who has access to install the components in **User Name**, and press Enter.
      For example, enter `root` or a user with sudo permissions.
   d) Enter the user's password in **User Password**, and press Enter.

5. Repeat steps 3 - 4 for each node that you want to install content on.
6. From the **Mandatory Content List** pane, drag the components to the appropriate node that you defined.

   Analytics Content
   Contains the Streams Jobs and Configuration files.
   You must deploy this component to a computer where you installed the IBM Streams.

   BigData Master Content
   Contains the deployment files for the Surveillance BigData component.
   You must deploy this component to a computer where you installed the IBM Open Hadoop Master.

   BigData Slave Content
   Contains the deployment files for the Surveillance BigData component.
   You must deploy this component to a computer where you installed the IBM Open Hadoop Slave.

   Database Content
   Contains the data model files and the sample data content.
   You must deploy this component to a computer where you installed the IBM DB2.

   Services Content
   Contains the deployment files (WAR files) and configuration files content.

   The files content files are copied to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_2.0` directory. You can change that value in the **Property Editor**.

   Tip: If you do not want the components to be decompressed automatically, select each of the content components, and in the **Property Editor**, clear **Uncompress File**.

7. Click **Validate** to ensure that the configuration is complete.

   Any errors or missing information is displayed. You must correct the error or provide the information before you can run the deployment.

8. Click **Run** to start the deployment.
9. When the deployment is complete, click **Close**, and then exit the solution installer.

Using the solution installer to deploy the remaining solution components

There are four components that you must install for IBM Surveillance Insight for Financial Services.

Before you can install the remaining IBM Surveillance Insight for Financial Services components, you must uninstall the solution installer and then install the solution installer for the next component. You must repeat this task for each component installer.

When you uninstall the solution installer, the processes that are used by the solution installer are stopped and removed from your computer.

Important: You must run a script on each node computer where you installed an IBM Surveillance Insight for Financial Services component to remove the solution installer processes on the node computer. Ensure that you copy the `cleanupClient.sh` file from the `SolutionInstaller` directory before you uninstall the server solution installer.

Procedure

1. To remove the solution installer processes on the client node computers, do the following steps on each client node computer:
   a) From the installation computer, copy the `SolutionInstaller/cleanupClient.sh` file onto each computer on which you installed an IBM Surveillance Insight for Financial Services component.
   b) On the client node computer, go to the directory where you copied the `cleanupClient.sh` file.
   c) Enter the following command: `sh cleanupClient.sh`.
2. To remove the solution installer from the installation computer, do the following steps:
   a) Go to the `SolutionInstaller` directory.
   b) Enter the following command: `sh cleanup.sh`.
   c) Restart the installation computer.
3. Install the IBM Electronic Communication Surveillance Analytics component:
   a) Decompress the `ecomm_surv_anlytics_2.0_l86-64_en.tar.gz` file.
   b) Go to the `CNJN0EN/SolutionInstaller` directory where you decompressed the solution installer files.
   c) Enter the following command: `./setup.sh` *`username first_name last_name email password`*.
   d) After the solution installer starts, open a web browser, and go to the solution installer URL: `https://`*`servername`*`:8080/UI/index.html`.
   e) Use the solution installer to deploy the Services Content component.

      The files content files are copied to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_EComm_2.0` directory. You can change that value in the **Property Editor**.
   f) Run the `cleanupClient.sh` script on the client node computers.
   g) Run the `cleanup.sh` script on the installer computes.
   h) Restart the installation computer.
4. Install the IBM Trade Surveillance Analytics component:
   a) Decompress the `trade_surv_analytics_2.0_l86-64_en.tar.gz` file.
   b) Go to the `CNJN1EN/SolutionInstaller` directory where you decompressed the solution installer files.
   c) Enter the following command: `./setup.sh` *`username first_name last_name email password`*.
   d) After the solution installer starts, open a web browser, and go to the solution installer URL: `https://`*`servername`*`:8080/UI/index.html`.
   e) Use the solution installer to deploy the components.

      The files content files are copied to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_Trade_2.0` directory. You can change that value in the **Property Editor**.
   f) Run the `cleanupClient.sh` script on the client node computers.
   g) Run the `cleanup.sh` script on the installer computes.
5. Install the IBM Voice Surveillance Analytics component:
   a) Decompress the `voice_surv_anlytics_2.0_l86-64_en.tar.gz` file.
   b) Go to the `CNJN2EN/SolutionInstaller` directory where you decompressed the solution installer files.
   c) Enter the following command: `./setup.sh` *`username first_name last_name email password`*.
   d) After the solution installer starts, open a web browser, and go to the solution installer URL: `https://`*`servername`*`:8080/UI/index.html`.
   e) Use the solution installer to deploy the components.

      The files content files are copied to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_Voice_2.0` directory. You can change that value in the **Property Editor**.

Install prerequisite software

Some prerequisite software is required before you can install IBM Surveillance Insight for Financial Services.

Installing IBM DB2 Workgroup Server

You must install IBM DB2 Workgroup Server Edition version 11.1.

Note: On Linux operating systems, the setup wizard is a graphical installer that requires an X Windows System (X11) to display the graphical user interface.

Procedure

1. Go to the directory where you decompressed the installation files.
2. Decompress the IBM DB2 installation file (`DB2_AESE_PVU_11.1_Svr_Linux_x86-64.tar.gz`), and go to the `server_r` directory.
3. Start the installer by using the following command: `./db2setup`.
4. In the **DB2 Setup Launchpad**, click **Install a Product**.
5. Under **DB2 Version 11.1 IBM DB2 Advanced Workgroup Server Edition**, click **Install New**.
6. Select **Typical** for the installation type.
7. On the **Select the installation, response file creation, or both** page, accept the default or select **Install DB2 Server Edition on this computer**.
8. Follow the steps in the wizard to install and configure your database server. For more information about any of the settings, see the IBM DB2 documentation on IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.swg.im.dbclient.install.doc/doc/c0023452.html).
9. Install fix pack 11.1.1.1. For more information, see the support documentation (https://www.ibm.com/support/docview.wss?uid=swg24043113).

Adding the IBM DB2 license

You must add the DB2 license after you install IBM DB2 server for IBM Surveillance Insight for Financial Services.

Procedure

1. Go to the folder where you decompressed the installation files.
2. Decompress the file that is named `DB2_AWSE_AUSI_Activation_11.1.zip`.
3. Change to the database administrator user.
   For example, `su db2inst1`.
4. Type the following command and press Enter:

   ```
   db2licm -a ese_u/db2/license/db2ese_u.lic
   ```
5. Type the following command to validate that the license was added:

   ```
   db2licm -l
   ```

Securing data at rest for IBM DB2

You must configure data at rest security for IBM DB2 and then create three databases for IBM Surveillance Insight for Financial Services.

Procedure

1. Log in to the database server computer as the root user.
2. Add the IBM Global Security Kit (GSKit) path to the LD_LIBRARY_PATH environment variable.
   For example, enter the following command: `export LD_LIBRARY_PATH=/home/db2inst1/sqllib/gskit/bin:$LD_LIBRARY_PATH`
3. Change to the database instance owner user.
   For example, enter `su db2inst1`.

4. Go to the `/home/db2inst1/sqllib/gskit/bin` directory.
5. Create a PKCS#12-compliant keystore by entering the following command:

   ```
   ./gsk8capicmd_64 -keydb -create -db /home/db2inst1/SIdb2keys.p12 -pw YourPassword -
   strong -type pkcs12 -stash
   ```

   For more information, see the GSKCapiCmd User's Guide (ftp://public.dhe.ibm.com/software/webserver/appserv/library/v61/ihs/GSK7c_CapiCmd_UserGuide.pdf).
6. Update the DB2 configuration with the new keystore by entering the following command:

   ```
   db2 update dbm cfg using keystore_type pkcs12 keystore_location /home/db2inst1/
   SIdb2keys.p12
   ```
7. Restart the database instance.
   a) Stop the database. Enter `db2stop`
   b) Start the database. Enter `db2start`
8. Create a 256 bit (32 bytes) master key. You can use the Linux operating system pseudorandom number generator or another utility.

   If you use the pseudorandom number generator, you can use the following command: `dd if=/dev/random of=/home/db2inst1/SIKey bs=1 count=32`
9. Import the generated key into the keystore that you created. You use the `-label` value in the following step.

   ```
   gsk8capicmd_64 -secretkey -add -db /home/db2inst1/SIdb2keys.p12 -file /home/db2inst1/
   SIKey -label SIlabel.SIdb.SIinstance.SIserver -pw YourPassword
   ```

Securing data in motion for IBM DB2
You must configure data in motion security for IBM DB2 for IBM Surveillance Insight for Financial Services.

Procedure

1. Log in to the database server computer as the database instance owner.
2. Go to the `/home/db2inst1/sqllib/gskit/bin` directory.
3. Add a certificate for your server to your key database.

   The server sends this certificate to clients during the SSL handshake to provide authentication for the server. You can use the IBM Global Security Kit (GSKit) command to create a new certificate request and send it to a certificate authority to be signed. You can use a self-signed certificate for testing or demonstration purposes. For production, you cannot use a self-signed certificate.

   ```
   ./gsk8capicmd_64 -cert -create -db /home/db2inst1/SIdb2keys.p12 -pw YourPassword -
   label "db2-selfsigned" -dn "CN=si.ibm.com,O=IBM,OU=IBMAnalytics,L=IN,ST=ON,C=CA"
   ```

   For more information about using this application, see the GSKCapiCmd User's Guide (ftp://public.dhe.ibm.com/software/webserver/appserv/library/v61/ihs/GSK7c_CapiCmd_UserGuide.pdf).
4. Extract the certificate that you created to a file. The file can be distributed to computers that run clients that use SSL communications with the DB2 server.

   For example, you can use `gsk8capicmd` to extract the certificate to a file that is named `SIDB2.arm`:

   ```
   ./gsk8capicmd_64 -cert -extract -db /home/db2inst1/SIdb2keys.p12 -pw YourPassword -
   label "db2-selfsigned" -target "/home/db2inst1/SIDB2.arm" -format ascii -fips
   ```
5. Update your IBM DB2 configuration:

   ```
   db2 update dbm cfg using SSL_SVR_KEYDB /home/db2inst1/SIdb2keys.p12
   db2 update dbm cfg using SSL_SVR_STASH /home/db2inst1/SIdb2keys.sth
   db2 update dbm cfg using SSL_SVR_LABEL db2-selfsigned
   db2 update dbm cfg using ssl_svcename 50001
   db2set -i db2inst1 DB2COMM=SSL
   ```
6. Restart the database instance.
   a) Stop the database. Enter `db2stop`

b) Start the database. Enter `db2start`

Installing IBM Installation Manager on the Services node

You must install IBM Installation Manager so that you can install WebSphere Application Server. IBM Installation Manager and WebSphere Application Server must be installed on the services node computer.

Procedure

1. Go to the `InstallationMgr` directory where you decompressed the installation files.
2. Decompress the Installation Manager installation file.
3. Enter the following command to start the installer:

   ```
   ./install
   ```
4. Follow the steps to install IBM Installation Manager.

Installing WebSphere Application Server on the Services node

IBM Surveillance Insight for Financial Services services are deployed to a WebSphere® Application Server instance on the services node computer.

You install WebSphere Application Server by using IBM Installation Manager.

For more information about WebSphere Application Server, see the product documentation (www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0).

Procedure

1. Go to the directory where you downloaded the installation files.
2. Decompress the WebSphere Application Server installation file: `WAS_ND_V9.0_MP_ML.zip`.
3. Decompress the WebSphere SDK installation file: `sdk.repo.8030.java8.linux.zip`.
4. Start IBM Installation Manager from the **Application Browser** or go to the `/opt/IBM/InstallationManager/eclipse` directory, and run `./IBMIM`.
5. Click **File** > **Preferences**.
6. Click **Add Repository**.
7. Browse to the location where you decompressed the WebSphere Application Server installation files.
8. In the directory where you decompressed the installation files, select `repository.config`, click **OK** to close the dialog.
9. Click **Add Repository**.
10. Browse to the location where you decompressed the WebSphere SDK installation files.
11. In the directory where you decompressed the installation files, select `repository.config`, click **OK** to close the dialog.
12. In IBM Installation Manager, click **Install**.
13. Select **IBM WebSphere Application Server Network Deployment**, and ensure that the underlying components are selected as well.
14. Click **Next**, and follow the steps in IBM Installation Manager to install the product.
15. When prompted for **Which program do you want to start?**, select **None**, and click **Finish**.

Creating a WebSphere Application Server deployment manager profile

After you install WebSphere Application Server, you must create a deployment manager profile.

Procedure

1. Log in to the services node computer as the root user or as a user with sudo permissions.
2. Go to the `/opt/IBM/WebSphere/AppServer/bin` directory.

3. Run the following command to create the profile:

```
./manageprofiles.sh -create -profileName SIFS-WAS-Dmgr
-profilePath /opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Dmgr
-templatePath /opt/IBM/WebSphere/AppServer/profileTemplates/management
-serverType DEPLOYMENT_MANAGER -hostName <hostname> -cellName SIFS-WAS-Cell
-nodeName SIFS-WAS-CellMgr -enableAdminSecurity=true -adminUserName=wasadmin
-adminPassword=wasadmin
```

4. Go to the `/opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Dmgr/bin` directory.
5. Run the following command to start the Deployment Manager:

   ```
   ./startManager.sh
   ```

Enabling administrative security for WebSphere Application Server
You must enable administrative security for WebSphere Application Server.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. Expand **Security** and then click **Global Security**.
4. Click **Security Configuration Wizard**.
5. Select **Enable application security**, and then click **Next**.
6. Select **Federated repositories**, and then click **Next**.
7. Enter the administrative credentials, and then click **Next**.
8. Click **Finish**.
9. Click **Save**.
10. Restart WebSphere Application Server.
    a) Go to the `/opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Dmgr/bin` directory.
    b) Run the following command: `./stopManager.sh`.
    c) Run the following command: `./startManager.sh`.

Creating a custom WebSphere Application Server profile
You must also create a custom profile in WebSphere Application Server.

Procedure

1. Log in to the services node computer as the root user or as a user with sudo permissions.
2. Go to the `/opt/IBM/WebSphere/AppServer/bin` directory.
3. Run the following command to create the profile:

```
./manageprofiles.sh -create -profileName SIFS-WAS-Custom
-profilePath /opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Custom
-templatePath /opt/IBM/WebSphere/AppServer/profileTemplates/managed
-hostName <hostname> -nodeName SIFS-WAS-Node -federatedLater true
```

Adding the custom node to the Deployment Manager
After you create the custom profile, you must add it to the WebSphere Application Server Deployment Manager instance.

Procedure

1. Log in to the computer where you created the custom WebSphere Application Server profile as the root user or as a user with sudo permissions.

2. Go to the /opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Custom/bin directory.
3. Run the following command to create the profile:

   ```
   ./addNode.sh <deployment-manager-hostname> 8879 -username admin-user -password
   admin-password
   ```

   Port 8879 is the default SOAP port that is used by the Deployment Manager. If you are using a different port, ensure that you set it for your environment.

Creating a WebSphere Application Server cluster
You must create a WebSphere Application Server cluster, and add the nodes as members of the cluster.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console for the Deployment Manager.

   The Admin console address is `http://`*`deployment-manager-servername`*`:9060/ibm/console` where *`deployment-manager-servername`* is the name or IP address for the computer where you installed WebSphere Application Server and created the Deployment Manager profile.
3. Expand **Servers** > **Clusters**, and then click **WebSphere application server clusters**.
4. Click **New**.
5. Enter SIFS-WAS-Cluster in the **Custom name** box, and click **Next**.
6. Do the following steps:
   a) Enter SIFSAppSrv01 in the **Member name** box.
   b) Select SIFS-WAS-Node in the **Select node** box.
   c) Enter 49 in the **Weight** box.
   d) Click **Next**.
7. Click **Finish**.
8. Expand **System administration** and click **Nodes**.
9. Select all of the nodes, and click **Full Resynchronization**.
10. Expand **Servers** > **Clusters** and then click **WebSphere application server clusters**.
11. Select the cluster that you added, and click **Start**.

Applying fix pack 2 to WebSphere Application Server version 9.0.0
You must apply fix pack 2 to your installation of WebSphere Application Server version 9.0 installation. You can apply the fix pack by using IBM Installation Manager.

For more information about the fix pack, see the 9.0.0.2: WebSphere Application Server traditional V9.0 Fix Pack 2 page (www.ibm.com/support/docview.wss?uid=swg24042989).

Procedure

1. Stop WebSphere Application Server Deployment Manager.
   a) Go to the /opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Dmgr/bin directory.
   b) Enter the following command: ./stopManager.sh
2. Start IBM Installation Manager from the **Application Browser** or go to the /opt/IBM/InstallationManager/eclipse directory, and run ./IBMIM.
3. Click **Update**.
4. On the **Update Packages** page, select **IBM WebSphere Application Server V9.0**, and click **Next**.
5. Enter your IBM ID and password, and click **OK**.
6. In the list of updates, select **Version 9.0.0.2**, and the recommended IBM SDK update, and click **Next**.
7. Select the 9.0.0.2 fixes from the list of fixes, and click **Next**.
8. Follow the remaining steps to apply the fix pack, click **Update**, and click **Finish**.

9. Start WebSphere Application Server Deployment Manager.
    a) Go to the `/opt/IBM/WebSphere/AppServer/profiles/SIFS-WAS-Dmgr/bin` directory.
    b) Enter the following command: `./startManager.sh`

    Starting the Deployment Manager will also start the node and custom profile.

Installing HTTP Server and the WebSphere Customization Tool

You must install the HTTP Server and Web Server Plug-ins component and the WebSphere Customization Tool for WebSphere Application Server.

You can download the **IBM HTTP Server and Web Server Plugins** and **WebSphere Customization Tool** from 9.0.0.2: WebSphere Application Server traditional V9.0 Fix Pack 2 page (www.ibm.com/support/docview.wss?uid=swg24042989).

Procedure

1. Download and decompress the IBM HTTP Server and Web Server Plug-ins installation file: `9.0.0-WS-IHSPLG-FP002.zip`.
2. Download and decompress the WebSphere Customization Tool installation file: `9.0.0-WS-WCT-FP002.zip`.
3. Start IBM Installation Manager from the **Application Browser** or go to the `/opt/IBM/InstallationManager/eclipse` directory, and run `./IBMIM`.
4. Click **File** > **Preferences**.
5. Click **Add Repository**.
6. Browse to the location where you decompressed the IBM HTTP Server and Web Server Plug-ins installation files.
7. In the directory where you decompressed the installation files, select `repository.config`, click **OK** to close the dialog.
8. Click **Add Repository**.
9. Browse to the location where you decompressed the WebSphere Customization Tool installation files.
10. In the directory where you decompressed the installation files, select `repository.config`, click **OK** to close the dialog.
11. In IBM Installation Manager, click **Install**.
12. Select **Web Server Plug-ins for IBM WebSphere Application Server** and **WebSphere Customization Toolbox**, and ensure that the underlying components are selected as well.
13. Click **Next**, and follow the steps in IBM Installation Manager to install the product.
14. When prompted for **Which program do you want to start?**, select **None**, and click **Finish**.

Configuring the web server plug-ins

You must create and configure IBM HTTP Server by using the WebSphere Application Server Web Server Plug-in Configuration Tool.

The Web Server Plug-in Configuration Tool is part of the WebSphere Customization Toolbox. For more information about installing the WebSphere Customization Toolbox, see WebSphere Customization Toolbox installation information (https://www.ibm.com/support/knowledgecenter/en/SSEQTP_9.0.0/com.ibm.websphere.installation.base.doc/ae/rins_wct_info.html).

Procedure

1. Log in to the services node computer as the root user or as a user with sudo permissions.
2. Start the Web Server Plug-in Configuration Tool. From the RedHat Kickoff Application Launcher, click **Applications** > **IBM WebSphere** > **WebSphere Customization Toolbox V9.0** > **Tools** > **Web Server Plug-in Configuration Tool**.
3. Click **Add**.
    a) Enter `http` in **Name**.
    b) Enter `/opt/IBM/WebSphere/Plugins` in **Location**.
    c) Click **Finish**.
4. In the **Web Server Plug-in Configuration** box, click **Create**.

  a) Select **IBM HTTP Server**, and click **Next**.
  b) Select **64 bit**, and click **Next**.
  c) Select the location of the `httpd.conf` file, enter 443 as the port, and click **Next**.
  d) Select **Setup IBM HTTP Server Administration**, enter `8008` as the HTTP port number, and enter the user credentials.
  e) Enter the user ID and group ID information, and click **Next**.
  f) Enter a name for the web server. For example, enter `SIFSIHServer01`.
  g) Enter the host name of the computer where Deployment Manager is running, and click **Next**.
  h) Click **Configure**.
  i) Clear the check box, and click **Finish**.

5. Start IBM HTTP Server by running the following commands.

```
/opt/IBM/HTTPServer/bin/apachectl start
/opt/IBM/HTTPServer/bin/adminctl start
```

Configuring SSL for IBM HTTP Server

IBM Surveillance Insight for Financial Services requires that you use SSL for your web server configuration.

Procedure

1. Log in to the services node computer as the root user or as a user with sudo permissions.
2. Go to the `/opt/IBM/HTTPServer/conf` directory.
3. Backup the existing `httpd.conf` file. For example, `cp httpd.conf httpd.conf.original`.
4. Open `httpd.conf` in a text editor.
  a) Comment out the following line, if it exists in the file:

```
Listen 80
```

  b) Search for `ServerName`, and change the port number to 443.
  c) Add the following lines, or uncomment them if they already exist:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
SSLCheckCertificateExpiration 30
<VirtualHost *:443>
 SSLEnable
 Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
</VirtualHost>
KeyFile /opt/IBM/HTTPServer/conf/ihsserverkey.kdb
SSLDisable
```

  Note: Ensure that the file contains only one line that says `Listen 443`.

  d) Save and close the file.

5. For testing or demonstration environments, create a self-signed certificate by using the ikeyman utility that is provided with IBM HTTP Server. The certificate is the `keyfile` value that you added in the previous step.
  a) Go to the `/opt/IBM/HTTPServer/bin` directory.
  b) Run the following command: `./ikeyman`.
  c) Click **Create a new key database file**.
  d) Select CMS for the **Key database type**.
  e) Enter `ihsserver.kdb` in **File Name**.
  f) Enter `/opt/IBM/HTTPServer/conf` in **Location**.
  g) Click **OK**.
  h) Enter a password, and click **OK**.
  i) Click **New Self-Signed**.
  j) Enter a **Key Label**, and enter any of the optional values if you choose.

k) Click **OK**.

Note: For production environments, ensure that you use a certificate from a certificate authority rather than a self-signed certificate.

6. Start IBM HTTP Server by using the following command:

```
/opt/IBM/HTTPServer/bin/apachectl start
```

You can access the web server page by going to `https://localhost:443` in a web browser.

Configuring HTTP Server in WebSphere Application Server

You must configure IBM HTTP Server from WebSphere Application Server.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. Enter the **User ID** and **Password**, and click **Log in**.
4. Expand **System administration**, and click **Nodes**.
   a) Click **Add node**.
   b) Select **Unmanaged node**, and click **Next**.
   c) Enter a name for the node, the name of the server on which the web server is installed, and select the operating system for that server. Click **Next**, and then click **Save**.
5. Expand **Servers** > **Server types**, and click **Web servers**.
   a) Click **New**.
   b) Select the node, enter a name for the web server node, select **IBM HTTP Server**, and click **Next**.
   c) Select **IHS** for the template, and click **Next**.
   d) Enter the information for the server, and click **Next**. Ensure that you use 443 for the port number.
   e) Click **Finish**.
   f) Click **Save**.
   g) Select the server, and click **Generate Plug-in**.
   h) Select the server, and click **Propogate Plug-in**.

Configuring data source connections in WebSphere Application Server

You must create data source connections to the Surveillance Insight databases in your WebSphere Application Server profile. You create the data source connections in the WebSphere administration console.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. Enter the **User ID** and **Password**, and click **Log in**.
4. Add the database instance owner credentials to a user alias for WebSphere Application Server.
   a) Expand **Servers** > **Server Types** > **WebSphere application servers**, and click **server1**.
   b) Under **Security**, click **Security domain**.
   c) Under **Authentication**, expand **Java Authentication and Authorization Service**, and click **J2C authentication data**.
   d) Click **New**.
   e) Enter a name for the user credentials in **Alias**.
   f) Enter the database instance owner in **User ID**.

For example, enter `db2inst1`.

g) Enter the database instance owner's password in **Password**.

h) Click **Apply**, and then click **Save**.

5. Expand **Resources** > **JDBC**, and click **Data sources**.
6. Create a data source connection to the SIFS database.

a) On the **Data source** page, click **New**.

b) Enter `SIFS` in **Data source name** and **JNDI name**, and click **Next**.

c) Select **Select an existing JDBC provider**, choose **DB2 Using IBM JCC Driver**, and click **Next**.

d) Select 4 for the **Driver type**.

e) Enter `SIFS` in **Database name**.

f) Enter the name of the server where IBM DB2 is running in **Server name**.

g) Enter the DB2 server port number in **Port number**. For example, `50001`.

h) Click **Next**.

i) Select the alias that you created for the database instance owner in both **Component-managed authentication alias** and **Container-managed authentication alias**, and click **Next**.

j) Click **Finish**, and then click **Save**.

k) Click the data source connection that you created in the table.

l) Under **Additional Properties**, click **Custom properties**.

m) In the properties table, click currentSchema.

n) Enter `SIFS` in **Value**.

o) Click **Apply**, and then click **Save**.

p) Select the data source connection that you created in the table, and click **Test connection**.

Note: Ensure that the test is successful.

Securing communication to the data sources in WebSphere Application Server

You must configure WebSphere Application Server to allow secure access to the data sources.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. If security is enabled, enter the **User ID** and **Password**, and click **Log in**. Otherwise, click **Log in**.
4. Expand **Security** and then click **SSL Certificates and Key Management**.
5. Under **Related Items**, click **Key stores and certificates**.
6. In the list, click **NodeDefaultTrustStore**.

   In a multi-node environment, click the link for the cell truststore.
7. Under **Additional Properties**, click **Signer certificates**.
8. Click **Retrieve from port**.
9. Enter the information for your IBM DB2 instance:

a) Enter the server name in **Host**.

b) Enter the DB2 port number in **Port**.
For example, enter `50001`.

c) Enter a name for this server in **Alias**. The **Alias** is used only by WebSphere.

10. Click **Retrieve signer information**.
11. Click **OK**, and then click **Save**.
12. Update the datasource connections with the certificates.

a) Expand **Resources** and then click **JDBC** > **Data sources**.

b) Click the datasource name.

c) Under **Additional Properties**, click **Custom properties**.
d) In the **Name** box, enter `sslConnection`.
e) In the **Value** box, enter `true`.
f) Click **OK**.
g) Enter the DB2 port number in the **Common and required data source properties** box.
h) Click **OK**, and then click **Save**.

13. Restart WebSphere Application Server.
14. Open the WebSphere Admin Console again.
15. Change the JPA settings:

a) Expand **Servers** > **Server Types** > **WebSphere Application Servers** and then click the server.
b) Click **Container Services** and then click **Default Java Persistence API settings**.
c) Change the **JPA Specification** setting to `2.0`.

16. Change the JAX RS version settings:

a) Expand **Servers** > **Server Types** > **WebSphere Application Servers** and then click the server.
b) Click **Container Services** and then click **Default JAXRS provider settings**.
c) Change the **JAX RS Provider** setting to `1.1`.

17. Change the JVM custom properties to disable CDI scanning:

a) Expand **Servers** > **Server Types** > **WebSphere Application Servers** and then click the server.
b) Click **Java and Process Management** and then click **Process definition**.
c) Under **Additional Properties** select **Java Virtual Machine**.
d) Under **Additional Properties** select **Custom Properties**, and enter the following text:

```
Name = com.ibm.ws.cdi.enableCDI
Value = false
Name = com.ibm.ws.cdi.enableImplicitBeanArchives
Value = false
```

Securing communication to the datasource for the Analytics Content

Use the following steps to allow standalone programs to connect to a secured DB2 data source over JDBC. For example, The Analytics Content uses this kind of connection.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. If security is enabled, enter the **User ID** and **Password**, and click **Log in**. Otherwise, click **Log in**.
4. Expand **Security** and then click **SSL Certificates and Key Management**.
5. Under **Related Items**, click **Key stores and certificates**.
6. In the list, click **NodeDefaultTrustStore**.

   In a multi-node environment, click the link for the cell truststore.
7. Under **Additional Properties**, click **Signer certificates**.
8. Select the IBM DB2 certificate that you added in "Securing communication to the data sources in WebSphere Application Server" on page 19.
9. Click **Extract**, enter a path to save the file, and click **Apply**.
   For example, in the path, enter `/home/db2inst1/Db2Cert.pem`.
10. Use the following command to import the certificate that you extracted:

```
keytool -importcert -alias db2-selfsigned -file /home/db2inst1/Db2Cert.pem -
keystore /opt/IBM/WebSphere/AppServer/java/8.0/jre/lib/security/cacerts -storepass
cacerts_keystore_password
```

Installing Apache Kafka on the Services node

Apache Kafka is used with IBM Streams. You must download and install Apache Kafka on the services node.

For information about using Apache Kafka, see the Kafka documentation (https://kafka.apache.org/quickstart).

Procedure

1. Go to the Apache Kafka download page (https://www.apache.org/dyn/closer.cgi?path=/kafka/0.10.0.0/kafka_2.10-0.10.0.1.tgz).
2. Click one of the links to download the software.
3. In the download directory, decompress the file to the `/opt` directory.
   For example, enter `tar xvf kafka_2.10-0.10.0.1.tgz -C /opt`
4. Set the JAVA_HOME environment variable to be the Java that is provided with WebSphere Application Server.

   ```
   export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0/
   ```
5. Set the PATH environment variable to include the Java that is provided with WebSphere Application Server.

   ```
   export PATH=/opt/IBM/WebSphere/AppServer/java/8.0/bin:$PATH
   ```
6. Optional: If you are using IBM Java, you must edit the `kafka-run-class.sh` file.
   a) Go to the `/opt/kafka_2.10-0.10.0.1/bin` directory.
   b) Open `kafka-run-class.sh` in a text editor.
   c) Locate the loggc value in the following line:

   ```
   KAFKA_GC_LOG_OPTS="-Xloggc:$LOG_DIR/$GC_LOG_FILE_NAME -verbose:gc -
   XX:+PrintGCDetails -XX:+PrintGCDateStamps -XX:+PrintGCTimeStamps "
   ```
   d) Change loggc to verbosegclog:

   ```
   KAFKA_GC_LOG_OPTS="-Xverbosegclog:$LOG_DIR/$GC_LOG_FILE_NAME -verbose:gc -
   XX:+PrintGCDetails -XX:+PrintGCDateStamps -XX:+PrintGCTimeStamps "
   ```
   e) Save and close the file.

Securing data at rest for Apache Kafka

You must create a secure key and keystore, and configure IBM Streams and WebSphere Application Server to be able to encrypt and decrypt messages with Apache Kafka.

Procedure

1. On the computer where Apache Kafka is installed, log on as the root user.
2. Enter the following command to create a secure key for decrypting data:

   ```
   keytool -genkey -alias SIKafkaSecurityKey -validity 365 -keyalg RSA -keysize 1024 -
   keystore SIKafkaDecrypt.jks -dname
   "CN=si.ibm.com,O=IBM,OU=IBMAnalytics,L=IN,ST=ON,C=CA" -keypass YourKeyPassword
   ```
3. When prompted, enter a password for the key.
4. Extract the certificate that you created to a public certificate file.

   ```
   keytool -export -alias SIKafkaSecurityKey -file SIKafka.arm -keystore
   SIKafkaDecrypt.jks
   ```
5. When prompted, enter the password that you used.

   Note: You must copy the extracted public certificate file to each computer that is running a component that encrypts messages to be sent to the Apache Kafka queue.
6. Create a keystore and import the public certificate file that you extracted in step 4.

   ```
   keytool -import -file SIKafka.arm -keystore SIKafkaEncrypt.jks -alias
   SIKafkaSecurityKey
   ```
7. When prompted, enter the password that you used.
8. Copy `SIKafkaDecrypt.jks` and `SIKafkaEncrypt.jks` files to the `/home/streamsadmin/security` directory.

9. Create a file that is named `encrypt.properties` in the `/home/streamsadmin/config/properties` directory.
10. Enter the following text into the `encrypt.properties` file.

    ```
    algorithm=3DES
    keylength=168
    encryptionkeypath=/home/streamsadmin/security/SIKafkaEncrypt.jks
    keystorepassword=YourPassword
    aliasname=SIKafkaSecurityKey
    ```

11. Save and close the file.

    Note: Ensure that the streamsadmin user has access to this file.
12. Create a file that is named `decrypt.properties` in the `/home/streamsadmin/config/properties` directory.
13. Enter the following text into the `decrypt.properties` file.

    ```
    encryptionkeypath=/home/streamsadmin/security/SIKafkaDecrypt.jks
    keystorepassword=YourPassword
    keypassword=YourKeyPassword
    aliasname=SIKafkaSecurityKey
    ```

14. Save and close the file.

    Note: Ensure that the streamsadmin user has access to this file.
15. On the computer where WebSphere Application Server is installed, create a file that is named `kafka_encryption.properties` in the `/home/`*`SIUser`* directory.
16. Enter the following text into the `kafka_encryption.properties` file.

    ```
    com.ibm.si.encryption.algorithm.name=3DES
    com.ibm.si.encryption.key.length=168
    com.ibm.si.encryption.keystore.location=/home/SIUser/SIKafkaEncrypt.jks
    com.ibm.si.encryption.keystore.password=YourPassword
    com.ibm.si.encryption.certificate.alias=SIKafkaSecurityKey
    ```

17. Save and close the file.

Securing data in motion for Apache Kafka

You must create a key and a certificate for the Apache Kafka broker.

Procedure

1. On the computer where Apache Kafka is installed, log on as the root user.
2. Create a key and a keystore for each Kafka broker.

    ```
    keytool -genkey -alias SIKafkaServerSSL -validity 365 -keystore
    SIKafkaServerSSLKeystore.jks -dname
    "CN=si.ibm.com,O=IBM,OU=IBMAnalytics,L=IN,ST=ON,C=CA" -keypass YourKeyPassword
    ```

3. When prompted, enter a password for the key.
4. Export the certificate from the keystore.

    ```
    keytool -certreq -file SIKafkaCert -alias SIKafkaServerSSL -keystore
    SIKafkaServerSSLKeystore.jks
    ```

5. When prompted, enter the password that you used.

    Note: The certificate must be signed by a certificate authority.
6. Generate the certificate authority key.

    ```
    openssl req -new -x509 -keyout ca-key -out ca-cert -days 365
    ```

    Follow the prompts to generate the key.
7. Add the key to the server truststore.

    ```
    keytool -import -file ca-cert -keystore SIKafkaServerSSLTruststore.jks -alias CARoot
    ```

The truststore is automatically created.

8. Add the key to the server keystore.

   ```
   keytool -import -file ca-cert -keystore SIKafkaServerSSLKeystore.jks -alias CARoot
   ```

9. Sign the certificate:

   ```
   openssl x509 -req -CA ca-cert -CAkey ca-key -in SIKafkaCert -out SIKafkaCertSigned -
   days 365 -CAcreateserial -passin pass:YourPassword
   ```

10. Import the signed certificate into the server keystore:

    ```
    keytool -import -file SIKafkaCertSigned -keystore SIKafkaServerSSLKeystore.jks -alias
    SIKafkaServerSSL
    ```

11. Update the `KafkaInstallLocation/config/server.properties` file to include the following text:

    ```
    listeners=SSL://<IP>:<Port>
    advertised.listeners=SSL://<IP>:<Port>
    ssl.keystore.location=/home/SIUser/SIKafkaServerSSLKeystore.jks
    ssl.keystore.password=YourPassword
    ssl.key.password= YourKeyPassword
    ssl.truststore.location=/home/SIUser/SIKafkaServerSSLTruststore.jks
    ssl.truststore.password=YourPassword
    ssl.client.auth=required
    security.inter.broker.protocol=SSL
    ```

12. Copy the `SIKafkaServerSSLKeystore.jks` and `SIKafkaServerSSLTruststore.jks` files to the `/home/streamsadmin/security` directory.

    Note: Ensure that the streamsadmin user has access to this file.

Configuring SSL for Apache Kafka

Follow these steps to configure SSL for Apache Kafka. These steps must be performed on the computer where IBM Streams and WebSphere Application Server are installed.

Procedure

1. On the computer where Apache Kafka is installed, log on as the root user.
2. Add the signed certificate that you created in "Securing data in motion for Apache Kafka" on page 22 to the truststore.

   ```
   keytool -import -file ca-cert -keystore SIKafkaClientSSLTruststore.jks -alias CARoot
   ```

   The truststore is automatically created.
3. When prompted, enter the password that you used.
4. Create a key and a keystore for each Kafka producer or consumer client.

   ```
   keytool –genkey -alias SIKafkaClientSSL -validity 365 -keystore
   SIKafkaClientSSLKeystore.jks -dname
   "CN=si.ibm.com,O=IBM,OU=IBMAnalytics,L=IN,ST=ON,C=CA" -keypass YourKeyPassword
   ```

5. When prompted, enter a password for the key.
6. Export the client certificate from the keystore. The certificate must be imported into the Apache Kafka server. This certificate can be self-signed.

   ```
   keytool -export -file SIKafkaClientCert.arm -alias SIKafkaClientSSL -keystore
   SIKafkaClientSSLKeystore.jks
   ```

7. When prompted, enter the password that you used.
8. Import the client certificate to the truststore for the Apache Kafka broker (server).

   ```
   keytool –import -keystore SIKafkaServerSSLTruststore.jks -alias SIKafkaClientCert1 -
   file SIKafkaClientCert.arm
   ```

9. Create a file that is named `producer.properties` in the `/home/streamsadmin` directory.

10. Enter the following text into the `producer.properties` file.

```
bootstrap.servers=<IP>:<PORT>

serializer.class=kafka.serializer.StringEncoder
request.required.acks=1
value.serializer=org.apache.kafka.common.serialization.ByteArraySerializer
key.serializer=org.apache.kafka.common.serialization.StringSerializer
security.protocol=SSL
ssl.protocol=TLSv1.1
ssl.enabled.protocols=TLSv1.1
ssl.truststore.type=JKS
ssl.truststore.location=/home/streamsadmin/SIKafkaServerSSLTruststore.jks
ssl.truststore.password=YourPassword
ssl.keystore.location=/home/streamsadmin/SIKafkaServerSSLKeystore.jks
ssl.keystore.password=YourPassword
ssl.key.password=YourKeyPassword
```

11. Save and close the file.
12. Save a copy of the `producer.properties` file to the `/home/streamsadmin/config/properties` directory.

    `producer.properties` should exist in both the `/home/streamsadmin` and `/home/streamsadmin/config/properties` directories.
13. Create a file that is named `consumer.properties` in the `/home/streamsadmin/config/properties` directory.
14. Enter the following text into the `consumer.properties` file.

```
bootstrap.servers=<IP>:<PORT>

serializer.class=kafka.serializer.StringEncoder
request.required.acks=1
value.serializer=org.apache.kafka.common.serialization.ByteArraySerializer
key.serializer=org.apache.kafka.common.serialization.StringSerializer
security.protocol=SSL
ssl.protocol=TLSv1.1
ssl.enabled.protocols=TLSv1.1
ssl.truststore.type=JKS
ssl.truststore.location=/home/streamsadmin/security/SIKafkaServerSSLTruststore.jks
ssl.truststore.password=YourPassword
ssl.keystore.location=/home/streamsadmin/security/SIKafkaServerSSLKeystore.jks
ssl.keystore.password=YourPassword
```

15. Save and close the file.

    Note: Ensure that the streamsadmin user has access to this file.

Starting the Apache Kafka services

After you start the Apache Kafka services, you must create topics for the IBM Surveillance Insight for Financial Services data.

Procedure

1. On the computer where Apache Kafka is installed, log on as the root user.
2. Go to the `/opt/kafka_2.10-0.10.0.1` directory.
3. Enter the following command to start the zookeeper process:

   `bin/zookeeper-server-start.sh config/zookeeper.properties &`
4. Enter the following command to start the Kafka process:

   `bin/kafka-server-start.sh config/server.properties &`

Installing Apache Solr on the Analytics node

Apache Solr is used to index unstructured data, such as emails, chats, and voice transcripts. You must install Apache Solr on the Analytics node.

For more information about Apache Solr, see the product documentation (lucene.apache.org/solr/6_3_0/index.html).

Procedure

1. Go to the `IS_FinancialMkts_SurveillanceInsight_2.0/Analytics/FinancialMkts_SurveillanceInsight_AnalyticsContent/Installables` directory where you deployed the solution files.
   By default, `IS_FinancialMkts_SurveillanceInsight_2.0` is in `/opt/IBM`.

   If you did not automatically decompress the content files, decompress `FinancialMkts_SurveillanceInsight_AnalyticsContent.zip` in the `IS_FinancialMkts_SurveillanceInsight_2.0/Analytics` directory.
2. In the `IBM Solr` directory, decompress `solr-6.3.0.tgz` to the `/opt` directory.
   For example, enter `tar xvf solr-6.3.0.tgz -C /opt`

Enabling SSL for Apache Solr

You must create a self-signed key to enable SSL for Apache Solr.

Procedure

1. On the computer where you installed Apache Solr, go to the *SolrInstallation*`/server/etc`.
2. Enter the following command to create a keystore.

   ```
   keytool -genkeypair -alias solr-ssl -keyalg RSA -keysize 2048 -keypass YourPassword -
   storepass YourPassword -validity 365 -keystore solr-ssl.keystore.jks -ext
   SAN=DNS:localhost,IP:XX.XX.XX.XX -dname "CN=XX.XX.XX.XX, OU=IBM, O=IBM, C=IN"
   ```
3. Go to the *SolrInstallation*`/bin` directory.
4. Open `solr.in.sh` in a text editor.
5. Uncomment and edit the following lines so that they match your environment.

   ```
   SOLR_SSL_KEY_STORE=etc/solr-ssl.keystore.jks
   SOLR_SSL_KEY_STORE_PASSWORD=YourPassword
   SOLR_SSL_TRUST_STORE=etc/solr-ssl.keystore.jks
   SOLR_SSL_TRUST_STORE_PASSWORD=YourPassword
   SOLR_SSL_NEED_CLIENT_AUTH=false
   SOLR_SSL_WANT_CLIENT_AUTH=false
   ```
6. Save and close the file.

Installing IBM Streams on the Analytics node

You must install IBM Streams on the analytics node computer. IBM Streams is a software platform that enables the development and execution of applications that process information in data streams. Incoming data is processed through IBM Streams and then output to the IBM Surveillance Insight for Financial Services data stores.

For more information about IBM Streams, see the product documentation (www.ibm.com/support/knowledgecenter/SSCRJU_4.2.0).

Before you begin

You must create a user for Streams. For example, create a `streamsadmin` user that belongs to the `streamsadmin` group. The user must exist before you can install the product.

Log in as the root user and use the following commands to add the `streamsadmin` user:

- Use the `groupadd` command to create the `streamsadmin` group. For example, in a terminal window, enter `groupadd streamsadmin`. The group must exist before you can add the user to the group.

- Use the useradd command to create the streamsadmin user and include the -g option to add the user to the group. For example, in a terminal window, enter useradd streamsadmin -g streamsadim.
- Use the passwd command to set the streamsadmin user's password. For example, enter passwd streamsadmin, and follow the prompts to set the password.

Procedure

1. Download IBM Streams 4.2 Fix Pack 2. For more information, see the IBM Streams Version 4.2 Fix Pack 2 page (http://www.ibm.com/support/docview.wss?uid=swg24043181). The Fix Pack contains a full version of the product.
2. Go to the directory where you downloaded the installation files, and decompress 4.2.0.2-IM-Streams-el6-x86_64-fp0002.tar.gz.
3. In the 4.2.0.2-IM-Streams-el6-x86_64-fp0002 directory, decompress Streams-4.2.0.2-x86_64-el6.tar.gz.
4. Go to the StreamsInstallFiles directory.
5. Start the installer by using the following command: ./IBMStreamsSetup.bin.
6. In the installer, on the **Select the edition to install** page, select **IBM Streams**, and click **Next**.
7. Ensure that you install all of the missing software packages that are identified on the **Software Dependencies** page.

   For more information about installing the software packages for IBM Streams, see the IBM Streams documentation on IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSCRJU_4.2.0/com.ibm.streams.install.doc/doc/ibminfospherestreams-install-rpms-streams-package.html).
8. Enter a Streams user and group. This user runs the Streams services. If the user does not exist, it is created by the installer.
   For example, enter streamsadmin as the **User** and streamsadmin as the **Group**.
9. Click **Next**, and follow the steps in the wizard to install the product.
10. Decompress the IBM Watson Speech to Text for RHEL6 x86 64 installation files: Str-4.2.0.0-Wat-S2T-x86_64-el6.tar.gz

    ```
    tar xvf Str-4.2.0.0-Wat-S2T-x86_64-el6.tar.gz
    ```

    a) From that file, decompress Streams-4.2.0.0-Watson-S2T-x86_64-el6.tar.gz.
    b) Decompress Streams-4.2.0.0-Watson-S2T-x86_64-el6.tar.gz.
11. In the IBMWatson-speech2test directory, review the README.txt for more information about using IBM Watson Speech to Text

Securing communications for IBM Streams

You must import the public certificate that you created into the IBM Streams keystore.

Procedure

1. Enter the following command to import the public certificate:

   ```
   keytool -keystore /home/streamsadmin/security/SIDB2StreamsClient.jks -alias DB2Streams
   -import -file /home/db2inst1/SIDB2.arm
   ```
2. When prompted, enter the password that you used.

What to do next

When you install the product, you must verify the location and password for the keystore in the install_ecomm.sh script. The values that you need to ensure are correct are db2ssltruststore and db2ssltruststorepasswd.

Installing Apache Ant libraries on all nodes

You must install Apache Ant and Ant Contrib on all of the computers on which you will install a IBM Surveillance Insight for Financial Services component.

Procedure

1. Download Apache Ant from the Apache Ant website (ant.apache.org/srcdownload.cgi).

2. Decompress the downloaded file to any location.
3. Edit the `$HOME/.bash_profile` file to include the following:

   `$ANT_HOME=/path_to_ant`
4. Download the `ant-contrib-1.0b3.jar` file.
   For example, go to https://sourceforge.net/projects/ant-contrib/files/ant-contrib/1.0b3/, and download `ant-contrib-1.0b3-bin.zip`.
5. Copy `ant-contrib-1.0b3.jar` to the *`ANT_HOME`*`/lib` directory.

Installing IBM BigInsights

You must install IBM Open Platform before you can install IBM BigInsights®.

For more information about IBM BigInsights, see the product documentation (https://www.ibm.com/support/knowledgecenter/SSPT3X_4.2.0).

Procedure

1. Download the IBM repository for IBM Open Platform. For more information, see Downloading the IBM repository definition for the IBM Open Platform with Apache Spark and Apache Hadoop (https://www.ibm.com/support/knowledgecenter/SSPT3X_4.2.0/com.ibm.swg.im.infosphere.biginsights.install.doc/doc/bi_install_download_software.html) in the IBM BigInsights documentation.
2. Follow the steps in Running the installation package (https://www.ibm.com/support/knowledgecenter/SSPT3X_4.2.0/com.ibm.swg.im.infosphere.biginsights.install.doc/doc/bi_install_iop_biginsights.html#bi_install_IOP_BigInsights) to complete the installation.
   a) In step 17 of Running the installation package, select HDFS, YARN, and Ambari-Metrics.

      MapReduce2 and ZooKeeper should be automatically selected.
   b) When you are enabling the YARN service, select at least 2 NodeManager nodes.
   c) After the installation is complete, you can log in from the Ambari console to verify that all of the services are running.
3. Create a KDC instance, as described in Setting up a KDC manually (https://www.ibm.com/support/knowledgecenter/SSPT3X_4.2.0/com.ibm.swg.im.infosphere.biginsights.admin.doc/doc/admin_kerb_mankdc2.html).

   Note: You must disable 256-bit encryption. To do this, remove aes256-cts:normal from the supported_enctypes field of the `/var/kerberos/krb5kdc/kdc.conf` file.
4. Enable Kerberos in Ambari as described in Setting up Kerberos for IBM Open Platform with Apache Spark and Apache Hadoopclusters (https://www.ibm.com/support/knowledgecenter/SSPT3X_4.2.0/com.ibm.swg.im.infosphere.biginsights.admin.doc/doc/admin_iop_kerberos.html).
   a) You must create a separate non-root user on all YARN Node Managers that will be used to run Spark. Name the user `sifsuser`.
   b) As the Hadoop Distributed File System (hdfs) user, create a home directory on hdfs for `sifsuser`.

      For example, `hdfs dfs -mkdir /user/sifsuser`
   c) Add a principal by running `kadmin.local` as the root user, and entering the following in the prompt:

      ```
      addprinc -randkey sifsuser@IBM.COM
      ktadd -norandkey -k /etc/security/keytabs/sifsuser.keytab sifsuser@IBM.COM
      ```

      Then set the ownership on the new keytab file by entering the following in the prompt:

      ```
      chown sifsuser:hadoop /etc/security/keytabs/sifsuser.keytab
      chmod a+r /etc/security/keytabs/sifsuser.keytab
      ```
   d) Copy `sifsuser.keytab` to all of the YARN Node Manager nodes.
   e) Log in as the sifsuser and run the following command to initialize the Kerberos ticket:

      ```
      kinit –kt /etc/security/keytabs/sifsuser.keytab sifsuser@IBM.COM
      ```

Enabling Hadoop encryption

You must enable encryption in Hadoop.

Procedure

1. Create a service user. For example, `useradd kms`.
2. Copy the Hadoop-KMS package to the home directory.
   For example, enter the following command:

   ```
   cp /usr/iop/current/hadoop-client/mapreduce.tar.gz /home/kms/mapreduce.tar.gz
   ```
3. Extract the archive.
   For example, enter the following command:

   ```
   export KMS_ROOT=/home/kms/
   cd $KMS_ROOT
   tar -xvf mapreduce.tar.gz
   ```
4. Start the KMS server.
   a) If you do not have the JAVA_HOME variable set, run the following command:

   ```
   export JAVA_HOME=/usr/jdk64/java-1.8.0-openjdk-1.8.0.77-0.b03.el7_2.x86_64/jre
   ```

   Ensure that you use the appropriate path for your environment.

   b) Go to the `$KMS_ROOT/hadoop/sbin/` directory.
   c) Enter the following command: `./kms.sh run`

   Wait until you see that the server started.
5. From the Ambari console, update the KMS server.
   a) In the Ambari console, click the HDFS service.
   b) Click **Configs** > **Advanced**.
   c) Add the following values:

Configuration section	Key	Value1
Advanced core-site	hadoop.security.key.provider.path	kms://http@<KMS Server IP>:16000/kms
Advanced hdfs-site	dfs.encryption.key.provider.uri	kms://http@<KMS Server IP>:16000/kms

6. Generate a key as a regular user.
   a) Log on as a regular user, such as ambari-qa.
   b) Create the key by entering the following command: `hadoop key create ambariqa-key`
7. Create an encryption zone for the `/user/sifsuser` directory.
   a) Log in as the hdfs user.
   b) Run the following commands:

   ```
   hdfs crypto -createZone -keyName ambariqa-key -path /user/sifsuser
   hdfs dfs -chown sifsuser:hadoop /user/sifsuser
   ```

   Tip: If you encounter any errors, you can check the following log directories:

   - `/var/log/hadoop/hdfs`
   - `/var/log/ambari-server`
   - `/var/log/ambari-agent`
   - `/var/lib/ambari-agent/data`
8. Verify that the contents are encrypted.
   a) Log in as the sifsuser.

b) Copy a test data file to the `/user/sifsuser` directory.

c) Run the following commands:

```
hdfs dfs –put testdata.txt /user/sifsuser/
hdfs dfs -cat /user/sifsuser/testdata.txt
hdfs dfs -cat /.reserved/raw/user/sifsuser/testdata.txt
```

This should show decrypted, clear text data.

Run the following command:

```
hdfs dfs -cat /.reserved/raw/user/sifsuser/testdata.txt
```

This should show encrypted data.

Note: If the Kerberos session has expired, you can run the `kinit` command.

Installing Apache Spark

The Apache Spark installer is provided with the IBM Surveillance Insight for Financial Services installation.

For more information about Apache Spark, see the product documentation (https://spark.apache.org/docs/2.0.2/).

Procedure

1. Go to the `IS_FinancialMkts_SurveillanceInsight_2.0/Analytics/Installables` directory where you deployed the solution files.
   By default, `IS_FinancialMkts_SurveillanceInsight_2.0` is in `/opt/IBM`.
2. Extract `spark-2.0.2-hadoop2.7.tar.gz` to the `/home/sifsuser/spark202` directory on the YARN Resource Manager and Node Manager computers.
3. log in as the sifsuser.
4. Edit the `.bashrc` file to include the following environmental variables:

```
export HADOOP_CONF_DIR=/usr/iop/4.2.0.0/hadoop/conf
export SPARK_HOME=/home/sifsuser/spark202/
export JAVA_HOME= /usr/jdk64/java-1.8.0-openjdk-1.8.0.77-0.b03.el7_2.x86_64/jre
```

5. From the Ambari console, do the following steps.

   a) Click **Yarn** > **Configs** > **Advanced**, and under **Application Timeline Server**, clear **yarn.timeline-service.enabled**.

   b) Click **MapReduce2** > **Configs** > **Advanced**, and under **Custom mapred-site**, add a property that is named `iop.version` and enter the value `4.2.0.0`.

   c) Save the changes.

   d) Restart the services in the Ambari console.

Configuring IBM Streams

You must create and start a domain for IBM Streams.

For more information about configuring IBM Streams, see IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSCRJU_4.2.0/com.ibm.streams.cfg.doc/doc/creating-basic-domain-and-instance.html).

Procedure

1. Log on to the computer where you installed IBM Streams, and change to the IBM Streams user.
   For example, `su streamsadmin`.
2. Go to the `/home/streamsadmin` directory.

3. Create a `.bashrc` file, and add the following lines:

```
source /opt/ibm/InfoSphere_Streams/4.2.0.2/bin/streamsprofile.sh
export SIFS_HOME=/home/streamsadmin
export HADOOP_HOME=/usr/iop/4.2.0.0/hadoop
```

4. Save and close the file.
5. If IBM Streams is not installed on one of the Hadoop cluster nodes, do the following steps:
   a) Copy the `/usr/iop/4.2.0.0/hadoop` and `/usr/iop/4.2.0.0/hadoop-hdfs` directories from one of the cluster nodes to the `/home/streamsadmin/Hadoop/` on the IBM Streams server.
   b) Edit the streamsadmin user `.bashrc` file to include the following line:

   ```
   export HADOOP_HOME=/home/streamsadmin/Hadoop/hadoop
   ```

   c) Copy the `/etc/krb5.conf` file from the KDC computer to the computer where IBM Streams is installed.

Install the Surveillance Insights artifacts

After you have deployed the components and installed the prerequisite software, you can run the scripts to install the IBM Surveillance Insight for Financial Services artifacts.

Replacing the IBM Streams Java™ file

After you install IBM Streams, you must replace a JAR file with on that is provided by the IBM Surveillance Insight for Financial Services installer.

Procedure

1. On the computer where you installed the IBM Surveillance Insight for Financial Services base components, go to the `/opt/IBM/ IS_FinancialMkts_SurveillanceInsight_2.0/ Services/ FinancialMkts_SurveillanceInsight_ServicesContent` directory.
2. Copy `ibmjgssprovider.jar` to the `/opt/ibm/InfoSphere_Streams/4.2.0.0/java/jre/lib` directory.

   Replace the existing `ibmjgssprovider.jar` file.

Installing the base component artifacts

To install the IBM Surveillance Insight for Financial Services base component artifacts, you must run scripts on each node computer.

Procedure

1. Create the SIFS database and load the master data on the database node computer.
   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_2.0/Database/ FinancialMkts_SurveillanceInsight_DatabaseContent/bin` directory.
   b) Open the `build.properties` file and update the file with the appropriate values for your environment.
   c) Run the following command: `sh Install_DB.sh sifs`
2. Create the users and groups, shared libraries, deploy the applications to WebSphere Application Server on the services node computer, create the SIFS repository, and start the Apache Solr services.
   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_2.0/Services/ FinancialMkts_SurveillanceInsight_ServicesContent/bin` directory.
   b) Open the `build.properties` file and update the file with the appropriate values for your environment.
   c) Run the following command: `sh Install_Services.sh`
3. Create the IBM Streams domain and instance, copy some jar files, and copy Streams projects to the home directory on the analytics node computer.
   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_2.0/Analytics/ FinancialMkts_SurveillanceInsight_AnalyticsContent/bin` directory.

b) Open the `build.properties` file and update the file with the appropriate values for your environment.

c) Run the following command: `sh Install_Analytics.sh`

4. Copy some jar files and properties files on the BigData node computer.

   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_2.0/BigData/FinancialMkts_SurveillanceInsight_BigDataContent/bin` directory.

   b) Open the `build.properties` file and update the file with the appropriate values for your environment.

   c) Run the following command: `sh Install_BigData.sh`

Installing the e-comms component artifacts

To install the IBM Electronic Communication Surveillance Analytics component artifacts, you must run scripts on the analytics node, services node, and BigData node computers.

Procedure

1. Log on to the analytics node computer.

   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_EComm_2.0/Analytics/FinancialMkts_SurveillanceInsight_AnalyticsContent/ecomm/bin` directory.

   b) Open the `build.properties` file and update the file with the appropriate values for your environment.

   c) Run the following command: `sh Install_Analytics.sh`

2. Log on to the services node computer.

   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_EComm_2.0/Services/FinancialMkts_SurveillanceInsight_ServicesContent/bin` directory.

   b) Open the `build.properties` file and update the file with the appropriate values for your environment.

   c) Run the following command: `sh Install_Services.sh`

3. Log on to the BigData node computer.

   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_EComm_2.0/BigData/FinancialMkts_SurveillanceInsight_BigDataContent/ecomm/bin` directory.

   b) Open the `build.properties` file and update the file with the appropriate values for your environment.

   c) Run the following command: `sh Install_BigData.sh`

Installing the voice component artifacts

To install the IBM Voice Surveillance Analytics component artifacts, you must run scripts on the analytics node and BigData node computers.

Procedure

1. Log on to the analytics node computer.

   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_Voice_2.0/Analytics/FinancialMkts_SurveillanceInsight_AnalyticsContent/Voice/bin` directory.

   b) Open the `build.properties` file and update the file with the appropriate values for your environment.

   c) Run the following command: `sh Install_Analytics.sh`

2. Log on to the BigData node computer.

   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_Voice_2.0/BigData/FinancialMkts_SurveillanceInsight_BigDataContent/Voice/bin` directory.

   b) Open the `build.properties` file and update the file with the appropriate values for your environment.

   c) Run the following command: `sh Install_BigData.sh`

Installing the Trade Surveillance component artifacts

To install the IBM Trade Surveillance Analytics component artifacts, you must run scripts on the analytics node and BigData node computers.

Procedure

1. Log on to the analytics node computer.
   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_Trade_2.0/Analytics/FinancialMkts_SurveillanceInsight_AnalyticsContent/Trade/bin` directory.
   b) Open the `build.properties` file and update the file with the appropriate values for your environment.
   c) Run the following command: `sh Install_Analytics.sh`
2. Log on to the BigData node computer.
   a) Go to the `/opt/IBM/IS_FinancialMkts_SurveillanceInsight_Trade_2.0/BigData/FinancialMkts_SurveillanceInsight_BigDataContent/Trade/bin` directory.
   b) Open the `build.properties` file and update the file with the appropriate values for your environment.
   c) Run the following command: `sh Install_BigData.sh`

Deploying PartyRiskScoring

You must manually deploy the PartyRiskScoring Spark job.

Procedure

1. Locate and open the `sifs.spark.properties` file in a text editor.
2. Edit the file to include the following line:

   ```
   PartyRiskDateWindow=N
   ```

   Where `N` is a positive number that indicates the number of days to look back in history for alerts.
3. Run the following submit command for the Spark job:

   ```
   ./spark-submit --class com.ibm.sifs.scoring.PartyRiskScoring  --master local --
   driver-memory 1g
   --executor-memory 2g --keytab /etc/security/keytabs/spark.keytab --principal
   sifsuser@EXAMPLE.COM
   --jars ~/spark201/jars/spark-yarn_2.11-2.0.2.jar --
   conf="spark.driver.extraClassPath=
   /home/sifsuser/lib/db2jcc4.jar:/home/sifsuser/lib/:/home/sifsuser/spark201/jars/*"
   --conf="spark.yarn.jars=/home/sifsuser/spark201/jars/spark-yarn_2.11-2.0.2.jar"
   --conf="spark.executor.extraClassPath=
   /home/sifsuser/lib/db2jcc4.jar:/home/sifsuser/lib/:/home/sifsuser/spark202/jars/
   *"
   /home/sifsuser/lib/PartyRiskScoring.jar /home/sifsuser/sifs.spark.properties
   ```

   Note: Ensure that the paths are appropriate for your environment.

Configure SAML security

IBM Surveillance Insight for Financial Services uses SAML 2.0 to allow single sign-on.

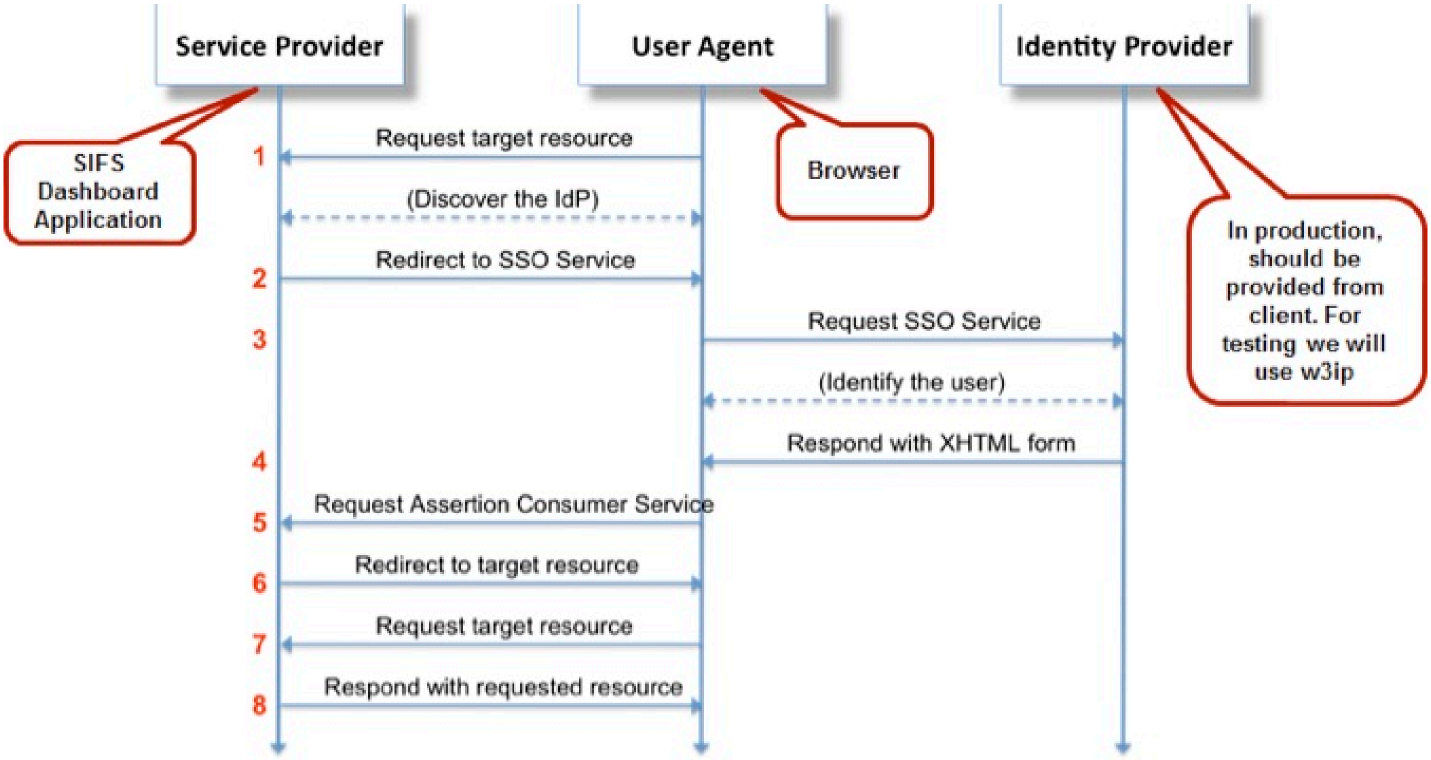


Figure 6: SAML configuration

Installing SAML Assertion Consumer Service (ACS) sample application

Install the Assertion Consumer Service (ACS) sample application to validate the SAML response that comes from the identity provider.

The ACS is provided with the WebSphere Application Server installation.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. Install the application EAR file. The application is `/opt/IBM/WebSphere/AppServer/installableApps/WebSphereSamlSP.ear`.
4. In a terminal window, go to the `/opt/IBM/WebSphere/AppServer/bin` directory.
5. Run the following command:

   ```
   wsadmin -f installSamlACS.py install <nodeName> <serverName>
   ```

   Or, you can run this command:

   ```
   wsadmin -f installSamlACS.py install <clusterName>
   ```

   Where *nodeName* is the name of the node of the target application server, *serverName* is the server name of the target application server, and *clusterName* is the name of the application server cluster.
6. If IBM HTTP Server is installed in your environment, open the WebSphere Admin Console.

7. Under **Applications**, click **Application Types** > **WebSphere enterprise applications**.
8. Click **WebSphereSamlSP**.
9. Under **Modules**, click **Manage Modules**.
10. In the **Clusters and servers** list, select the web server and the WebSphere Application Server or cluster where you want to install the application.
11. Select **WebSphereSamlPSWeb**, and click **Apply**.
12. Click **Save**, and synchronize the server node.
13. Under **Environment**, click **Update global Web server plug-in configuration**, and click **OK**.
14. Under **Servers**, click **Server Types** > **Web Server**.
    a) Select the server, and click **Generate Plug-in**.
    b) Select the server, and click **Propogate Plug-in**.
15. Restart the web server.
    a) In a terminal window, enter the following command to stop the server: `/opt/IBM/HTTPServer/bin/apachectl stop`.
    b) In a terminal window, enter the following command to start the server: `/opt/IBM/HTTPServer/bin/apachectl start`.

Configuring the SAML trust association interceptor

You must configure the SAML trust association interceptor (TAI).

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *servername* is the name or IP address for the computer where you installed WebSphere Application Server.
3. Under **Security**, click **Global security**.
4. Under **Web and SIP security**, click **Trust association**.
5. Select **Enable trust association**, and click **OK**.
6. Click **Save**.
7. Under **Web and SIP security**, click **Trust association**.
8. Under **Additional Properties**, click **Interceptors**.
9. Click **New**.
10. Enter `com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor` in **Interceptor class name**.
11. Add the following **Custom properties**.

Name	**Value**

`sso_1.sp.acsUrl`	`https://<hostname>:<sslport>/samlsps/sifssaml`
	Where hostname is the host name of the server where `WebSphereSamlSP.ear` is installed and sslport is the Web server SSL port number (WC_defaulthost_secure).
	For example:
	`https://`*`servername`*`:9443/samlsps/sifssaml`
	or
	`https://`*`servername`*`:443/samlsps/sifssaml`

`sso_1.sp.idMap`	`idAssertion`

12. Click **OK**, and click **Save**.
13. Under **Security**, click **Global security**, and then click **Custom properties**.

14.Click **New**.

15.Add the following properties.

Name	Value
com.ibm.websphere.security.DeferTAItoSSO	com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor
com.ibm.websphere.security.InvokeTAIbeforeSSO	com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor

16.Click **OK**, and click **Save**.

17.Synchronize the nodes.

18.Restart the WebSphere Application Server application server, node, and deployment manager instances.

a) Stop the application server: `/opt/IBM/WebSphere/AppServer/profiles/`*`profileName`*`/bin/stopServer.sh` *`serverName`* `-username` *`admin-user`* `-password` *`admin-pword`*

b) Stop the node: `/opt/IBM/WebSphere/AppServer/profiles/`*`profileName`*`/bin/stopNode.sh -username` *`admin-user`* `-password` *`admin-pword`*

c) Stop the deployment manager: `/opt/IBM/WebSphere/AppServer/bin/stopManager.sh -username` *`admin-user`* `-password` *`admin-pword`*

d) Start the deployment manager: `/opt/IBM/WebSphere/AppServer/bin/startManager.sh`

e) Start the node: `/opt/IBM/WebSphere/profiles/`*`profileName`*`/bin/startNode.sh`

f) Start the application server: `/opt/IBM/WebSphere/profiles/`*`profileName`*`/bin/startServer.sh` *`serverName`*

Configuring a single sign-on identity provider

You must configure a partnership between the WebSphere Application Server SAML service provider and the external SAML identity provider. You do this by importing a metadata file from the identity provider.

Procedure

1. Go to the `/opt/IBM/WebSphere/AppServer/bin` directory.
2. Run the following command to start the command line utility:

```
./wsadmin.sh -lang jython
```

3. At the prompt, enter the following command:

```
AdminTask.importSAMLIdpMetadata('-idpMetadataFileName <IdPMetaDataFile> -idpId 1 -ssoId 1 -signingCertAlias <idpAlias>')
```

Where *`<IdPMetaDataFile>`* is the full path and file name of the identity provider metadata file, and *`<idpAlias>`* is an alias name that you specify for the imported certificate.

Enter the following command to save the configuration:

```
AdminConfig.save()
```

4. Open a web browser.
5. In the address bar, type the address for the WebSphere Admin Console.

The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.

6. Under **Security**, click **Global security**.
7. Under **Web and SIP security**, click **Trust association**.
8. Under **Additional Properties**, click **Interceptors**, and click `com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor`.
9. Confirm the settings.

10.Under **Security**, click **SSL certificate and key management**.

11.Under **Related Items**, click **Key stores and certificates**.

12. Click **CellDefaultTrustStore** or **NodeDefaultTrustStore**.
13. Under **Additional Properties**, click **Signer certificates**.
14. Confirm the SAML settings.
15. In the command line utility, add the identity provider realms to the list of inbound trusted realms.

    ```
    AdminTask.addTrustedRealms('[-communicationType inbound -realmList <realm1|realm2|
    realm3>]')
    ```

    Where *realm1*, *realm2*, and *realm3* are the realms that must be added.

    Enter the following command to save the configuration:

    ```
    AdminConfig.save()
    ```

    Enter the following command to quite the console:

    ```
    quit
    ```
16. In the WebSphere Admin Console, under **Security**, click **Global security**.
17. Under **User account repository**, click **Configure**.
18. Under **Related Items**, click **Trusted authentication realms - Inbound**.
19. Ensure that the realms that you added are present.
20. Under **Security**, click **Global security**.
21. Click **Web and SIP security** > **Trust association**.
22. Under **Additional Properties**, click **Interceptors**.
23. In the table, click **com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor**, and add the following properties.

Name	Value
`sso_1.idp_1.certAlias`	This value represents the keystore alias where the signing certificate was added to the WebSphere configuration. For a network deployment, the certificate is usually added to the CellDefaultTrustStore. For a base installation, it is usually added to the NodeDefaultTrustStore. For example: `sifssamlsso`
`sso_1.sp.useRealm`	The realm of the identity provider application. The value for this property can be found in the SAML response from the identity provider under the issuer attribute. For example: `https://w3id.alpha.sso.ibm.com/auth/sps/samlidp/saml20`

Name	Value
`sso_1.sp.login.error.page`	The identity provider (IDP) application specifies the IDP-Initiated Login URL ,which is what must be configured here. **Note:** The value should be a URL where redirection after authentication happen. For deep linking, this query parameter should not be specified. For example: `https://`*`hostname`*`/auth/sps/samlidp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://`*`hostname`*`:`*`port`*`/samlsps/sifssaml&NameIdFormat=email`
`sso_1.sp.groupName`	The value of this attribute is used as groups in the subject which will ultimately be used for mapping to application roles. Check the SAML response from the identity provider application to determine the value for this property. Any SAML attribute key can be used.
`sso_1.sp.filter`	`request-url%=/surveillance`
`sso_1.sp.EntityID`	Enter the same value as is used for the `sso_1.sp.acsUrl` value. For example: `https://`*`hostname`*`:`*`port`*`/samlsps/sifssaml`
`sso_1.sp.useRelayStateForTarge`	For deep linking to work, this attribute value should be set to `true` or `false`. If you enter `false`, specify the target query string for `sso_1.sp.login.error.page` attribute.

24.Click **Save**.

25.Synchronize the nodes.

26.Restart the WebSphere Application Server application server, node, and deployment manager instances.

a) Stop the application server: `/opt/IBM/WebSphere/profiles/`*`profileName`*`/bin/stopServer.sh` *`serverName`* `-username` *`admin-user`* `-password` *`admin-pword`*

b) Stop the node: `/opt/IBM/WebSphere/profiles/`*`profileName`*`/bin/stopNode.sh -username` *`admin-user`* `-password` *`admin-pword`*

c) Stop the deployment manager: `/opt/IBM/WebSphere/AppServer/bin/stopManager.sh -username` *`admin-user`* `-password` *`admin-pword`*

d) Start the deployment manager: `/opt/IBM/WebSphere/AppServer/bin/startManager.sh`

e) Start the node: `/opt/IBM/WebSphere/profiles/`*`profileName`*`/bin/startpNode.sh`

f) Start the application server: `/opt/IBM/WebSphere/profiles/`*`profileName`*`/bin/stopServer.sh` *`serverName`*

Exporting service provider metadata

Each identity provider that is used with your WebSphere Application Server service provider must be configured to add the service provider as an SSO partner. The procedure for adding the service provider partner to an identity provider depends on the specific identity provider. For more information about adding a service provider partner for SSO, see the documentation for your identity provider.

You can either export the WebSphere Application Server service provider metadata, and import it to the identity provider, or you can manually configure the identity provider to add the service provider.

To add the service provider as a federation partner to an identity provider, you must provide the URL of the Assertion Consumer Service (ACS) of the service provider. This value is the -acsUrl parameter that you used when you enabled the SAML trust association interceptor (TAI) ("Configuring the SAML trust association interceptor" on page 34).

If the identity provider can use a metadata file to add the service provider as a federation partner, you can use the following wsadmin command-line utility command to export the service provider metadata file.

Procedure

1. In a terminal window, go to the `/opt/IBM/WebSphere/AppServer/bin` directory.
2. Run the following command to start the wsadmin command-line utility:

   ```
   ./wsadmin.sh -lang jython
   ```
3. Run the following command:

   ```
   AdminTask.exportSAMLSpMetadata('-spMetadataFileName <spMetaDataFile> -ssoId 1')
   ```

   Where *<spMetaDataFile>* is the full path and name of the service provider metadata file.

   The command creates a `/tmp/spMetadata.xml` metadata file.
4. Import the `/tmp/spMetadata.xml` metadata file into your identity provider application. For more information, see the documentation for your identity provider.

Mapping the application security role to the SAML group

You must map the identity provider groups to the SIFSDashboard roles.

Procedure

1. Open a web browser.
2. In the address bar, type the address for the WebSphere Admin Console.

   The Admin console address is `http://`*`servername`*`:9060/ibm/console` where *`servername`* is the name or IP address for the computer where you installed WebSphere Application Server.
3. Under **Applications**, click **Application Types** > **WebSphere enterprise applications**.
4. Click **SIFSDashboard.war**.
5. Under **Detail Properties**, click **Security role to user/group mapping**.
6. Select a role, and click **Map Groups**.
7. In the **User realm** box, select the identity provider realm that the users are in, and click **Search**.
8. Select the group, and click the arrow to add the group.

   If the realm cannot be searched, enter the **Group short name** and **Unique group ID** values, and click the arrow to add the group.
9. Click **OK**.
10. Click **Save**.
11. Restart WebSphere Application Server.

Use SLM tags to track licensing

Software License Metric (SLM) tag files provide a standardized capability for a product to report its consumption of license metrics (resources that are related to the use of the software asset). After SLM is enabled in a product, a runtime XML file is generated to self-report its license usage. The SLM tag files are based on the ISO/IEC 19770-4 standard draft for Resource Utilization Measurement.

The SLM tag files are stored in XML format, and new metric records are appended to the end of the file.

The following is a sample SLM tag for the voice component:

```
<SchemaVersion>2.1.1</SchemaVersion>
  <SoftwareIdentity>
```

```
     <PersistentId>a490d40f839049ea881d9aedf8b3d60f</PersistentId>
        <Name>IBM Voice Surveillance Analytics</Name>
        <InstanceId>/home/test/</InstanceId>
 </SoftwareIdentity>
         <Metric logTime="2017-05-17T01:01:41+05:30">
         <Type>FEED</Type>
         <SubType>TOTAL_VOICE_SECONDS</SubType>
         <Value>1821</Value>
         <Period>
                 <StartTime>2017-04-17T01:01:41+05:30</StartTime>
                <EndTime>2017-05-17T01:01:41+05:30</EndTime>
        </Period>
       </Metric>
```

The following is a sample SLM tag for the trade component:

```
<SchemaVersion>2.1.1</SchemaVersion>
   <SoftwareIdentity>
      <PersistentId>c6ede63c6002493f82281c89982fcc32</PersistentId>
      <Name>IBM Trade Surveillance Analytics</Name>
      <InstanceId>/home/test/</InstanceId>
     </SoftwareIdentity>
          <Metric logTime="2017-05-17T01:06:23+05:30">
          <Type>USER</Type>
          <SubType>NO_OF_PARTY</SubType>
          <Value>151</Value>
          <Period>
                <StartTime>2017-05-16T01:06:23+05:30</StartTime>
                <EndTime>2017-05-17T01:06:23+05:30</EndTime>
          </Period>
         </Metric>
```

The following is a sample SLM tag for the e-comm component:

```
<SchemaVersion>2.1.1</SchemaVersion>
   <SoftwareIdentity>
      <PersistentId>fe953daa1dbc4446905c4b3dd21e8f81</PersistentId>
      <Name>IBM Electronic Communication Surveillance Analytics</Name>
      <InstanceId>/home/test/</InstanceId>
   </SoftwareIdentity>
  <Metric logTime="2017-05-17T01:07:06+05:30">
       <Type>USER</Type>
       <SubType>NO_OF_PARTY</SubType>
       <Value>151</Value>
       <Period>
           <StartTime>2017-05-16T01:07:06+05:30</StartTime>
           <EndTime>2017-05-17T01:07:06+05:30</EndTime>
      </Period>
</Metric>
```

When IBM Surveillance Insight for Financial Services is installed, the SLM tag files (`*.slmtag`) are available on the data node computer in the `/var/ibm/common/slm` directory.

The SLM scripts are configured to run as cron jobs.

Updating your software tag file if you change product usage

If you change your usage of IBM Surveillance Insight for Financial Services, such as to a non-production environment from a production environment, you must switch the software tags for your installation.

Follow these steps to change your usage to non-production or to change your usage back to production.

Procedure

1. Go to the /opt/IBM/IS_FinancialMkts_SurveillanceInsight_2.0/Analytics/tag_prod_nonprod directory.
2. Open the build.properties file in the text editor, modify the settings, and save the file.
3. Run the following command:

   ```
   ./Switch_Tag_SIFS.sh
   ```
4. Repeat steps 1 -3 on each IBM Surveillance Insight for Financial Services node.

Appendix A. 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.

The following terms are trademarks or registered trademarks of other companies:

- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Index