For information on how to install and enable the IBM Business Process Manager (BPM) Analytics Technology Demonstration, follow the steps in each of the sections in this document.

Install Elasticsearch and Kibana

1. Install Elasticsearch by following the official guide at:

   https://www.elastic.co/guide/en/elasticsearch/reference/5.1/ installation.html

2. Install Kibana by following the official guide at:

   https://www.elastic.co/guide/en/kibana/5.1/setup.html

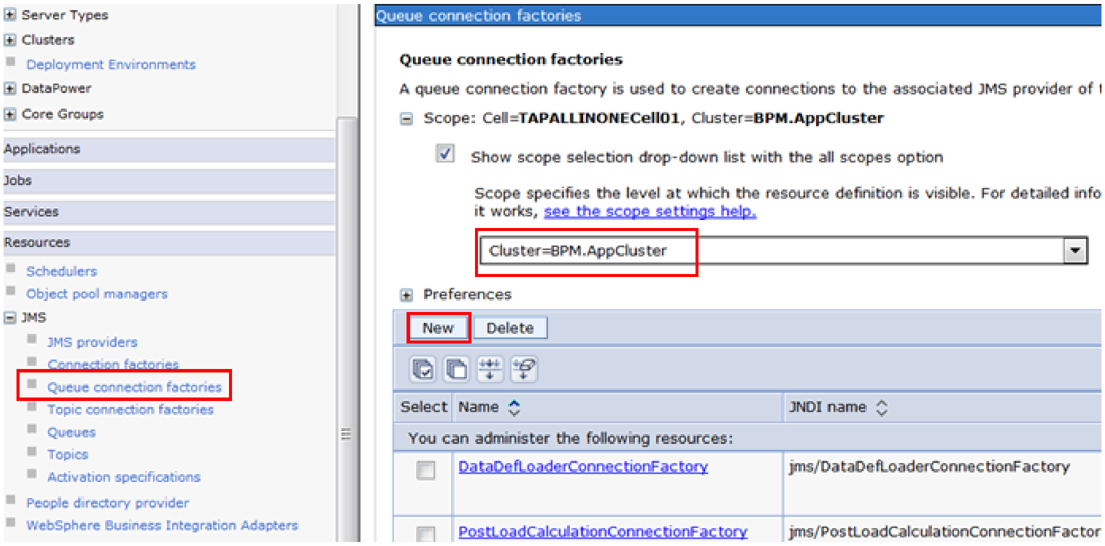
Enable the Dynamic Event Framework (DEF)

Create WebSphere resources

1. Create a JMS queue connection factory from the IBM Business Process Manager (BPM) administrative console, by clicking **Resources** > **JMS** > **Queue connection factories**.

2. Set the **Scope** to cluster, such as **Cluster=<*Cluster_Name*>**.

3. Click **New** to create a new JMS queue connection factory:



Queue connection factories

Queue connection factories

A queue connection factory is used to create connections to the associated JMS provider of

Scope: Cell=**TAPALLINONECell01**, Cluster=**BPM.AppCluster**

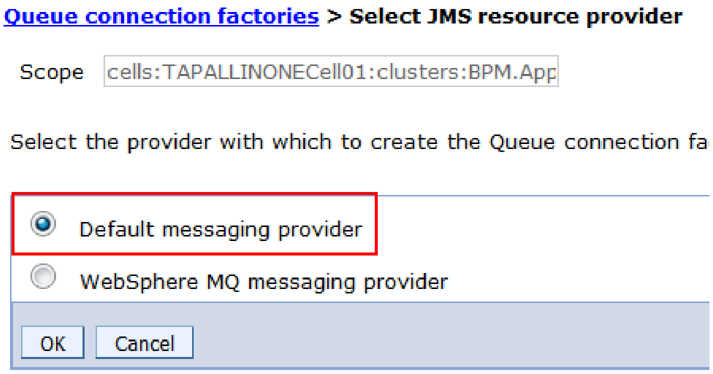
☑ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed info it works, see the scope settings help.

Cluster=BPM.AppCluster

Select	Name	JNDI name
You can administer the following resources:		
□	DataDefLoaderConnectionFactory	jms/DataDefLoaderConnectionFactory
□	PostLoadCalculationConnectionFactory	jms/PostLoadCalculationConnectionFactor

4. Select a JMS resource provider, such as **Default messaging provider** and click **OK**:



Queue connection factories > **Select JMS resource provider**

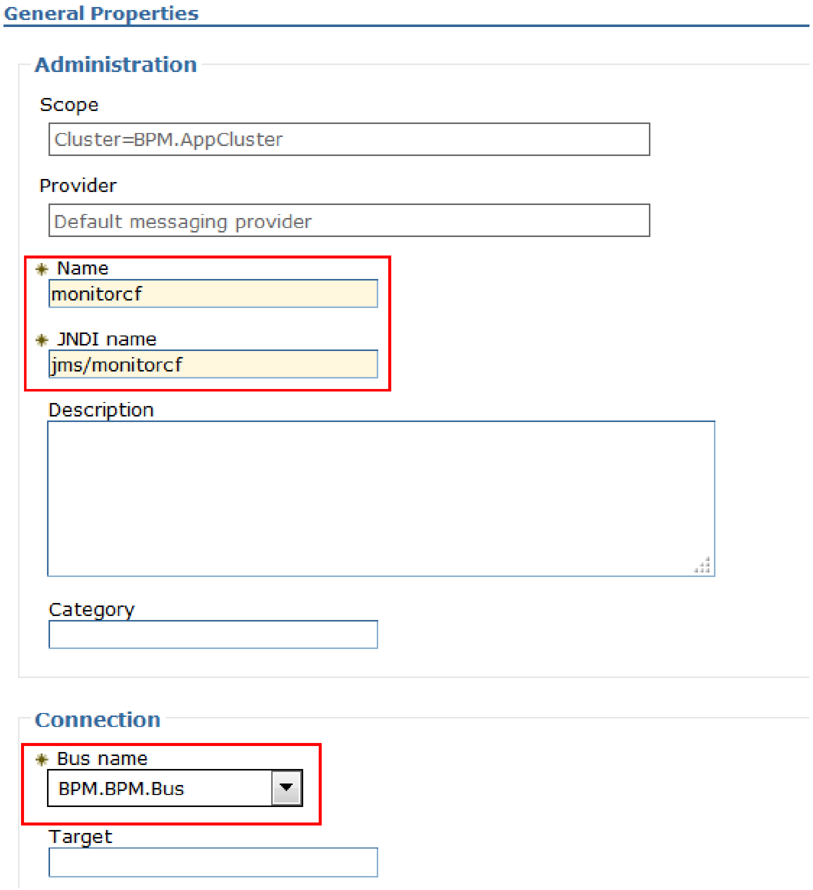
Scope cells:TAPALLINONECell01:clusters:BPM.App

Select the provider with which to create the Queue connection fa

● Default messaging provider

○ WebSphere MQ messaging provider

5. On next configuration page, assign "**Name**" and "**JNDI name**", and select **Bus** for DEF usage:



General Properties

Administration

Scope: Cluster=BPM.AppCluster

Provider: Default messaging provider

* Name: monitorcf

* JNDI name: jms/monitorcf

Description:

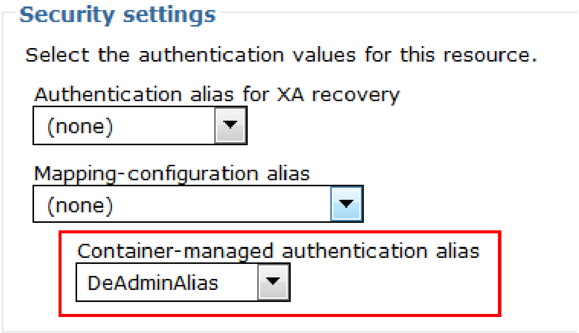
Category:

Connection

* Bus name: BPM.BPM.Bus

Target:

6. Select the authentication alias:



Security settings

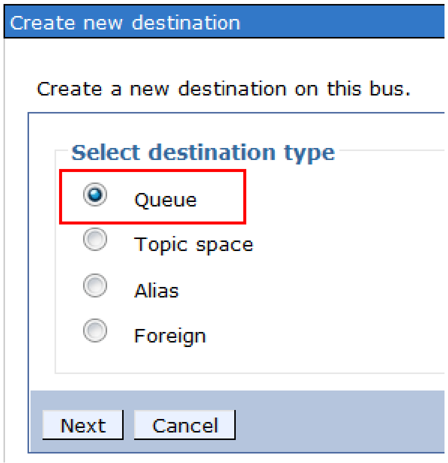
Select the authentication values for this resource.

Authentication alias for XA recovery: (none)

Mapping-configuration alias: (none)

Container-managed authentication alias: DeAdminAlias

7. Define a destination on the IBM BPM deployment environment bus by clicking **Service integration > Buses** and select the bus. Click **Destinations** and add a new queue destination. The destination type is **Queue**:



Create new destination

Create a new destination on this bus.

Select destination type

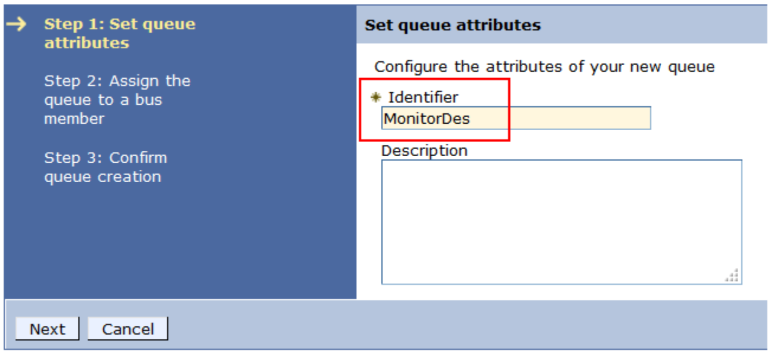
● Queue

○ Topic space

○ Alias

○ Foreign

Assign a queue identifier:



Step 1: Set queue attributes
Step 2: Assign the queue to a bus member
Step 3: Confirm queue creation

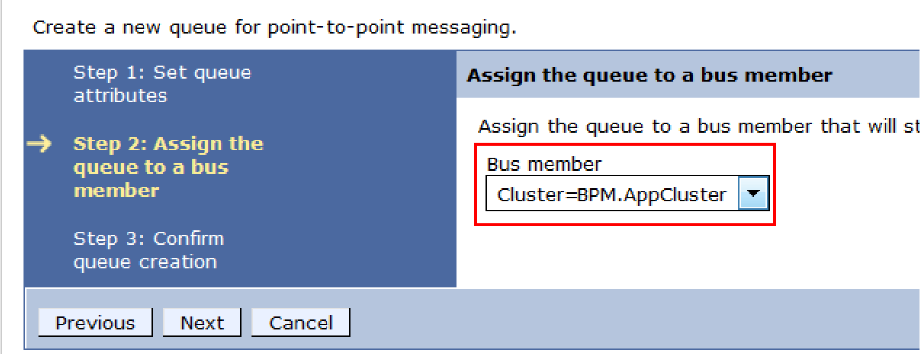
Set queue attributes

Configure the attributes of your new queue

* Identifier: MonitorDes

Description

Select the bus member:



Create a new queue for point-to-point messaging.

Step 1: Set queue attributes
Step 2: Assign the queue to a bus member
Step 3: Confirm queue creation

Assign the queue to a bus member

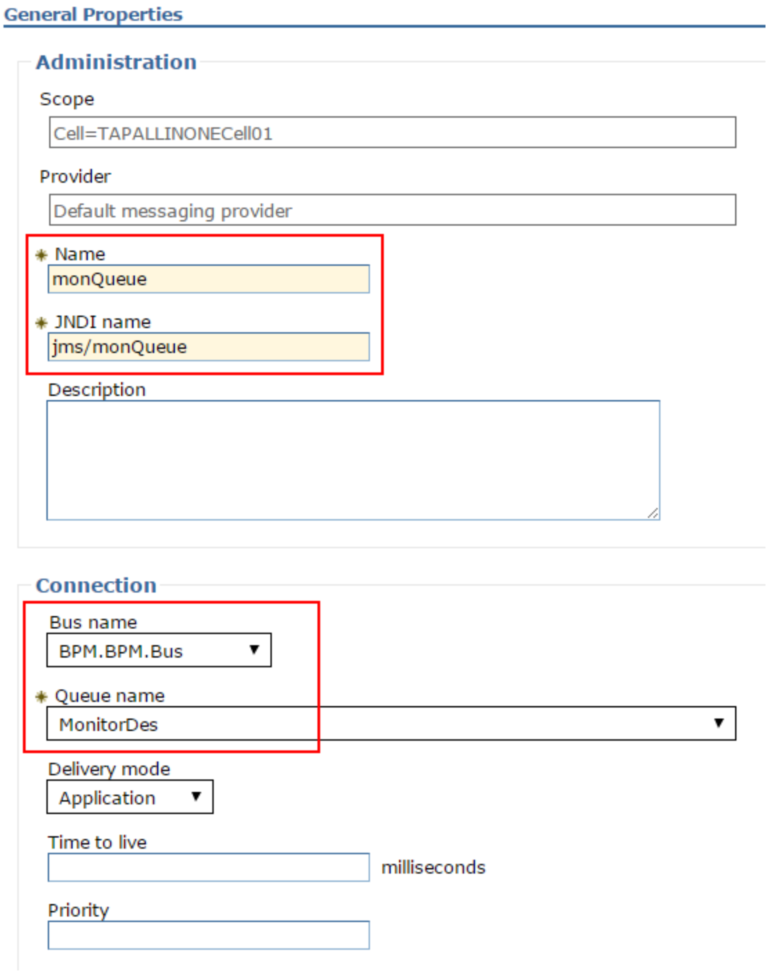
Assign the queue to a bus member that will st

Bus member: Cluster=BPM.AppCluster

Create a JMS queue

1. Create a JMS queue by clicking **Resources > JMS > Queues**, select **Scope** to Cell, such as **Cell=<*Cell_Name*>**.

2. Click **New** to create a new JMS queue, and select **Default messaging provider** as the JMS resource provider. On the configuration page, assign "**Name**" and "**JNDI name**", select Bus, and select the destination created in previous section as the Queue name:



General Properties

Administration

Scope: Cell=TAPALLINONECell01

Provider: Default messaging provider

* Name: monQueue

* JNDI name: jms/monQueue

Description:

Connection

Bus name: BPM.BPM.Bus

* Queue name: MonitorDes

Delivery mode: Application

Time to live: milliseconds

Priority:

Update the SampleConfigureEventsToJMS.py script

SampleConfigureEventsToJMS.py is a sample script that has been provided to help enable DEF. It is located in <*Install_Root*>/BPM/Lombardi/tools/def.

1. Edit the sample script to update each of the fields according to settings set in the previous sections:

defListenterId: A string value that uniquely identifies this listener.

eventQueueJndiName: A string value that refers to the JNDI name of the queue resource created in WebSphere.

eventQueueCFJndiName: A string value that refers to the JNDI name of the queue connection factory resource created in WebSphere.

eventQueueCF_AuthorizationAlias: A string value that refers to the authorization alias created in WebSphere.

2. Specify the subscription array. Each subscription in the subscriptions array is a single string with a '/' separator for each of the seven part keys. A comma is used to separate each subscription. The seven part keys are:

Application Name / Version / ComponentType / Component Name / Element Type /

Element Name / Nature

For a description of each of the parts, see the following topic:

https://www.ibm.com/support/knowledgecenter/en/SS7NQD_8.5.7/com.ibm.wbpm.mon.imuc.doc/intro/intro_event_point_key.html

To listen for every event for all applications, use the wildcard character as shown in the following example:

```
subscriptions=[
'*/*/*/*/*/*/*'
]
```

The following example shows how you might register to receive events for the Hiring Sample:

```
subscriptions=[
'HSS/*/BPD/*/PROCESS/*/*',
'HSS/*/BPD/*/ACTIVITY/*/*',
'HSS/*/BPD/*/GATEWAY/*/*',
'HSS/*/BPD/*/EVENT/*/*'
]
```

3. Run the sample script from the command line. Go to the bin directory under your deployment manager profile home directory and run the SampleConfigureEventsToJMS.py script. **Note:** Ensure that the support cluster (where DEF runs) is running before you run the script:

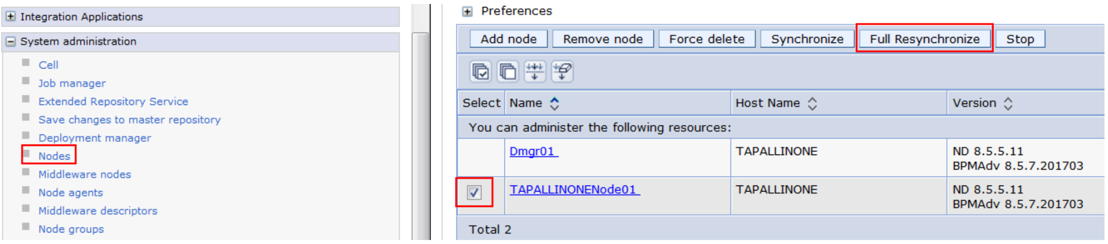
```
wsadmin-langjython -f <Script_Location>/SampleConfigureEventsToJMS.py
```

4. Run the SampleReloadDEF.py script to reload DEF. From a command line, go to the bin directory under your deployment manager profile home directory, run the following command:

```
wsadmin-langjython-f <Script_Location>/SampleReloadDEF.py
```

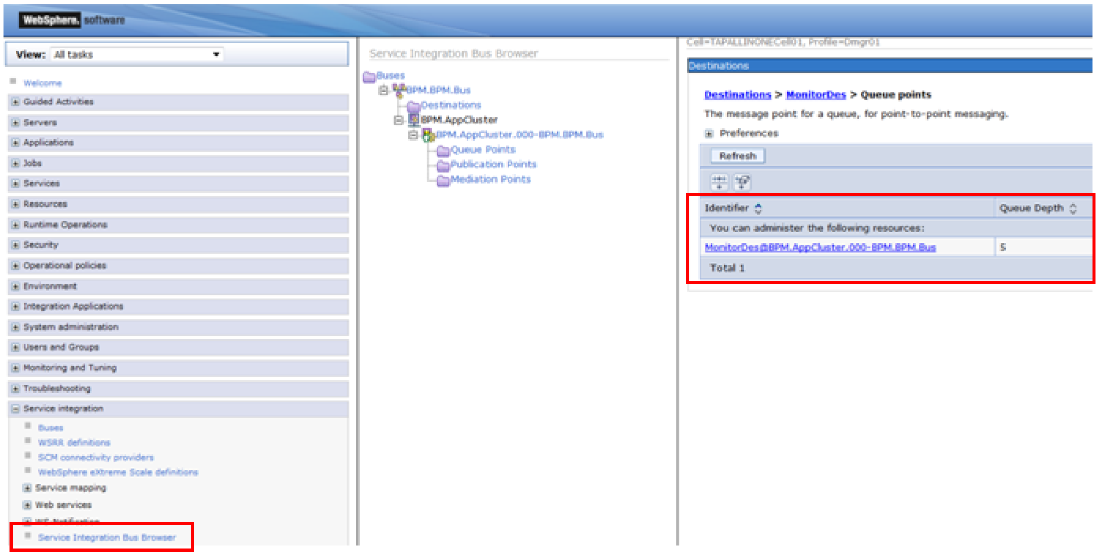
After running the sample script, a defconfig.xml file is created in the dmgr_profile_home/config/cells/cellName directory.

5. From the admin console, select **System administration > Nodes**, select nodes, and click **FullSynchronize**:



Select	Name	Host Name	Version
You can administer the following resources:			
	Dmgr01	TAPALLINONE	ND 8.5.5.11 BPMAdv 8.5.7.201703
☑	TAPALLINONENode01	TAPALLINONE	ND 8.5.5.11 BPMAdv 8.5.7.201703
Total 2			

6. Validate that DEF was enabled successfully by starting a process in process portal. Select **Service Integration > Service Integration Bus Browser**, click into the bus destination which DEF used. The queue depth should be larger than 0:



Destinations > MonitorDes > Queue points

The message point for a queue, for point-to-point messaging.

Identifier	Queue Depth
You can administer the following resources:	
MonitorDes@BPM.AppCluster.000-BPM.BPM.Bus	5
Total 1	

How to disable Performance Data Warehouse (PDW)

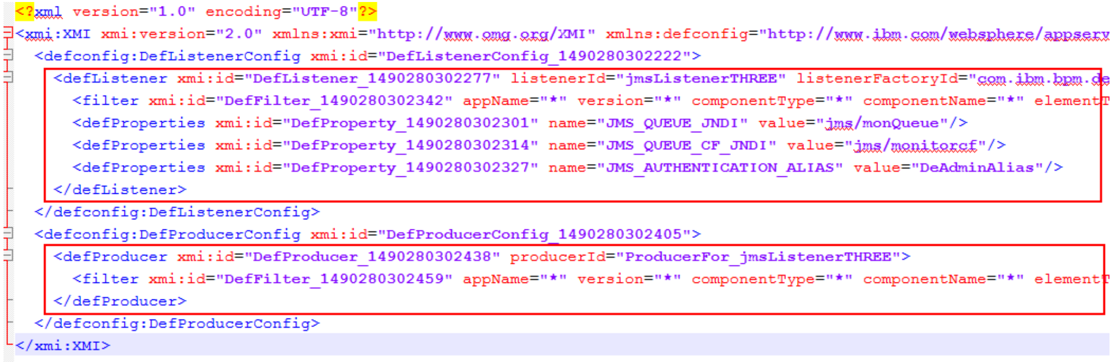
If you want to disable PDW after enabling DEF, refer to https://developer.ibm.com/answers/questions/167196/disabling-tracking-data-generation-for-a-process-s.html

How to disable the Dynamic Event Framework (DEF)

If you want to disable DEF once you have finished with the Analytics function, follow these steps:

1. To delete the generated DEF configuration, go to <*Install_Root*>/profiles/<Dmgr_Profile>/config/cells/<*Cell_Name*>/defconfig.xml. Delete the following configurations:

- defListener
- defProducer

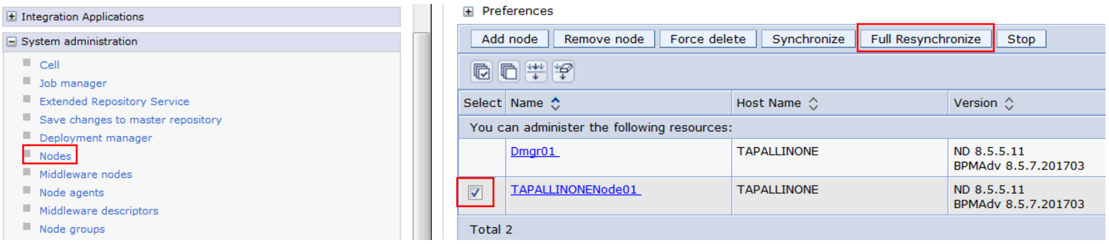


```
<?xml version="1.0" encoding="UTF-8"?>
<xmi:XMI xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI" xmlns:defconfig="http://www.ibm.com/websphere/appserv
  <defconfig:DefListenerConfig xmi:id="DefListenerConfig_1490280302222">
    <defListener xmi:id="DefListener_1490280302277" listenerId="jmsListenerTHREE" listenerFactoryId="com.ibm.bpm.de
      <filter xmi:id="DefFilter_1490280302342" appName="*" version="*" componentType="*" componentName="*" elementT
      <defProperties xmi:id="DefProperty_1490280302301" name="JMS_QUEUE_JNDI" value="jms/monQueue"/>
      <defProperties xmi:id="DefProperty_1490280302314" name="JMS_QUEUE_CF_JNDI" value="jms/monitorcf"/>
      <defProperties xmi:id="DefProperty_1490280302327" name="JMS_AUTHENTICATION_ALIAS" value="DeAdminAlias"/>
    </defListener>
  </defconfig:DefListenerConfig>
  <defconfig:DefProducerConfig xmi:id="DefProducerConfig_1490280302405">
    <defProducer xmi:id="DefProducer_1490280302438" producerId="ProducerFor_jmsListenerTHREE">
      <filter xmi:id="DefFilter_1490280302459" appName="*" version="*" componentType="*" componentName="*" elementT
    </defProducer>
  </defconfig:DefProducerConfig>
</xmi:XMI>
```

2. Run the SampleReloadDEF.py script to reload DEF. From a command line, go to the bin directory under your deployment manager profile home directory, run the following command:

```
wsadmin-langjython-f <Script_Location>/SampleReloadDEF.py
```

3. From the admin console, select**System administration >Nodes**, select nodes, click **Full Resynchronize**:



Select	Name	Host Name	Version
You can administer the following resources:			
	Dmgr01	TAPALLINONE	ND 8.5.5.11 BPMAdv 8.5.7.201703
☑	TAPALLINONENode01	TAPALLINONE	ND 8.5.5.11 BPMAdv 8.5.7.201703
Total 2			

Configure and install the BPMEventEmitter

Prerequisites and key words

Before configuring and installing the BPMEventEmitter file, you should:

a. Enable the DEF message generation per the instruction on BPM server. At a minimum, you will need the **JMS monitor queue** and the **event queue JNDI name**.

b. Know the target Elasticsearch server hosts. If security is enabled on the server, ensure that you have the **username**, **password** and **SSL/TLS related settings**.

Update the configuration file

1. Open the file **BPMEventEmitter.war** (provided as an artifact of this Technology Demonstration) with a zip tool, such as 7zip. Within the package, the configuration file is in BPMEventEmitter.war/WEB-INF/classes/config.yml

The configuration file is in YAML format:

```
# the configuration properties for the kafka if have
# the raw json events will be wrote to the kafka topic directly
# topic can be created automatically if it's not exist
# kafka bootstrap server(s) can be a list, separated by the comma
# by default, it's disabled
kafkaConfiguration:
kafka.bootstrap.servers: localhost:9092
monitor.topic: bpm-monitor-topic
enabled:false

# the configuration properties for the elastic search
# elastic search is the default event consumer
# the monitor event will be transformed to the query(kibana) optimized format
# before write to the ES as document
esConfiguration:
hosts: localhost:9200
enabled:true
# the following properties should be enabled when elastic search security is on
username: elastic
password:<xor>d3hrdXJEeXU=
httpsTrustType:
trustFileLocation:
hostnameVerifier:

# the identity for this BPM environment
# it can be the cell name or other proper identity
bpmCellName: bpmCell01

# the ES index name
esIndex: monitor
```

2. Update the values per your environment and save the updated file back to the war package. See below for more information about the configuration fields. **Note**: If you do not have Kafka installed on your environment, keep the default value and leave enabled set to “false”:

bpmCellName: Used as a field value of the generated message. If you want to analyze messages from different BPM clusters, update this field to different names across different BPM clusters.

esIndex: Used as the Elasticsearch index name where the generated data is stored.

esConfiguration: The configuration for Elasticsearch servers.

Hosts: Lists all server addresses in the Elasticsearch cluster. If you have not enabled security (SSL/TLS) on your Elasticsearch, use your IP directly. For example: 192.168.0.1:9200,127.0.0.1:9200

If you enabled security (SSL/TLS). You must input the https prefix to the address to announce that the HTTPS protocol should be used. For example: https://192.168.0.1:9200,https://127.0.0.1:9200

username and **password:** Used when you enable basic authentication on your Elasticsearch cluster. For the password field, you can use plain text or use an encoded password. You can use **EventSummaryAgent** to encode your password by running the encodePassword function to get the encoded value as shown below:

```
EventSummaryAgent -encodePassword elastic

<xor>cXxraGFIdw==
```

If you enabled SSL/TLS on your Elasticsearch, you must set the **httpsTrustType** per the type you used. Three kinds are supported: ALL, CRT and JKS.

ALL: The application accepts all HTTPs communication. It should be used for test purposes only.

CRT: Provide the CA certificate file (.crt) to support that the application accepts certain HTTPs connections. In this option, you must provide the **trustFileLocation** setting with an absolute address. Ensure that the BPM server can access that file. For example:

```
httpsTrustType: CRT

trustFileLocation: /opt/IBM/BPM/elasticSearch.crt
```

Default: The agent accepts HTTPs communication accepted by the JVM default settings.

hostnameVerifier: Accepts Boolean values, leave as “false” in the production environment. If you are using the test environment which uses a CRT certificate including a wrong host or IP address, you can set that to true for testing purposes only.

Security tips

Before enabling the Elasticsearch security, you can leave all of the security related fields empty or remove them from the configuration file to disable those settings.

After enabling the Elasticsearch security by installing X-Pack or protected that by using Nginx, you should provide the correct value for the fields.

For example:

```
hosts: https://<some_address>:9200
# the following properties should be enabled when elastic search security is on
username: elastic
password:<xor>cXxraGFIdw==
httpsTrustType: CRT
trustFileLocation: /opt/IBM/BPM/elastcisearch.crt
hostnameVerifier:false
```

This means that the Elasticsearch server protected with TLS and basic authentication. You have the CRT certification file located on /opt/IBM/BPM/elasticsearch.crt, and the CRT has the correct host/IP address to the server.

Prepare the IBM BPM environment

The application will use JMS Activation specifications (AS) and Queues JNDI values to monitor the DEF events. Before installing the application, you must create the related JMS Activation specification first. For WebSphere Application Server Activation specifications and Queues, refer to the following topic:

https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/SIBJMSActivationSpec_DetailForm.html

The default AS JNDI and Queue JNDI used by our application will be:

AS: jms/defAS

Queue: jms/monQueue

You can create the activation specification and DEF monitor queue with that value. If you created the monitor queue or AS before with another name, you can update the value on file BPMEventEmitter.war/WEB-INF/ ibm-ejb-jar-bnd.xml or update that value after the application is installed (see the next section of this document for more information).

For the default settings, assign the following when creating the AS:

Name: Any custom name

JNDI name: Use jms/ defAS

Destination type: Queue

Destination JNDI name: The Queue JNDI when you enable DEF on your server. Default will be jms/monQueue

Bus name: The bus name where the DEF message queue is located

Security Settings > Authentication alias: By default, Bus security is enabled on the BPM server. You must select the alias with Bus access, the default can be CellAdminAlias.

Install the BPMEventEmitterWAR on the IBM BPM server

1. Log into the BPM server admin console, the default address is: http://<Server_Address>:9060/admin

2. Expand **Applications** > **Application Types** > **WebSphere enterprise applications** in the left panel. In the right panel click **Install**.

3. **Select** the BPMEventEmitter.war file in local disk or input the remote address for that file, click **Next**.

4. **Select** Fast Path, click **Next**.

For “Step 1: Select installation options”, if you do not have any special access control on your server, click **Next**.

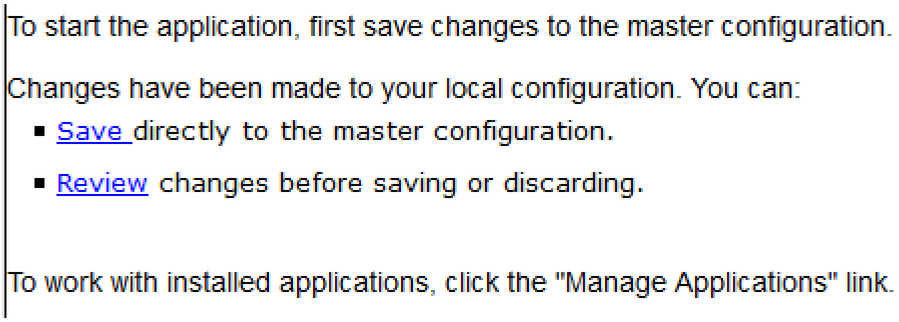
For “Step 2: Map modules to servers”, if you are using single cluster environment. Using default. If you are using golden topology with three cluster, you can map the application on support cluster only.

For “Step 3: Map context roots for Web modules”, click **Next**.

For “Step 4: Metadata for modules”, click **Next**.

For “Step 5: Summary”, click **Finish**.

If the installation is successful, you will see a Save link as shown below:



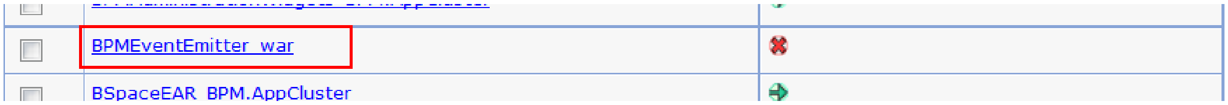
To start the application, first save changes to the master configuration.

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

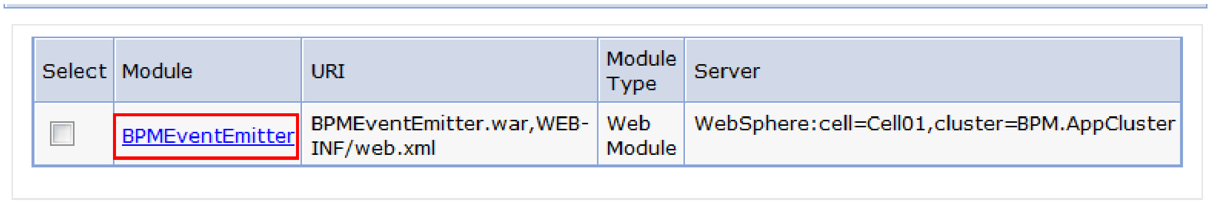
To work with installed applications, click the "Manage Applications" link.

5. After clicking Save, the application is installed:



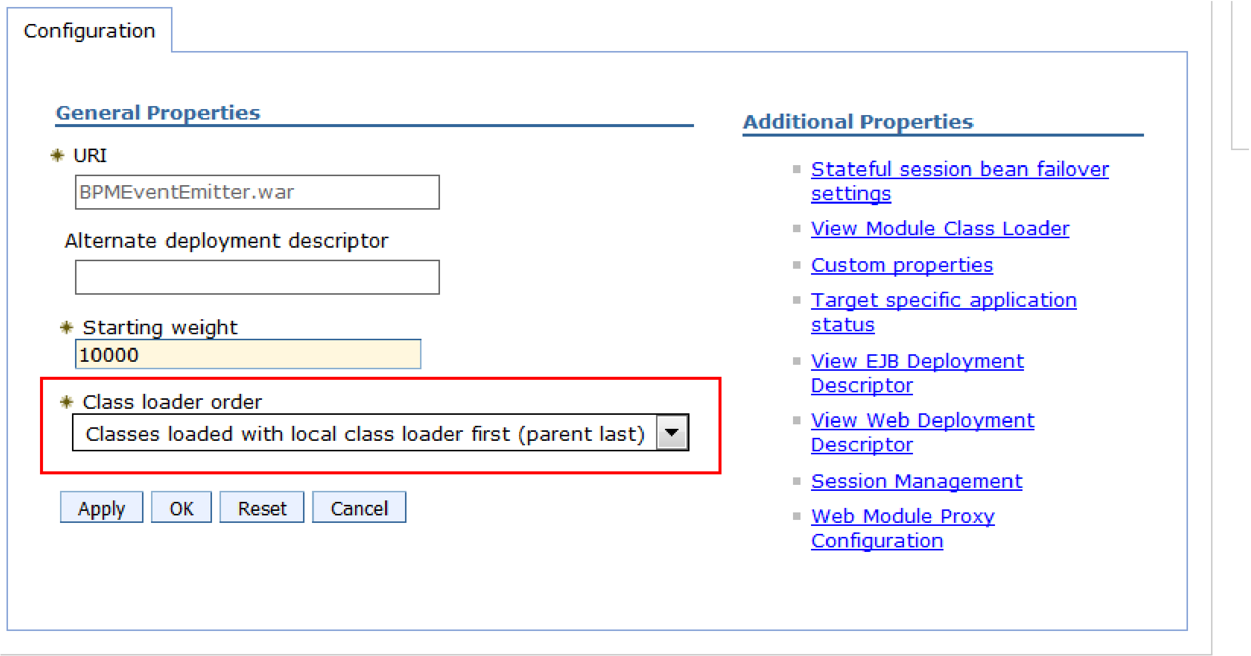
☐	BPMEventEmitter_war	✖
☐	BSpaceEAR_BPM.AppCluster	➔

6. There some **post actions** needed. Click the application name to open the configuration page. In the **Modules** section, click **Manage Modules.** Click BPMEventEmitter to open the module configuration page.



Select	Module	URI	Module Type	Server
☐	BPMEventEmitter	BPMEventEmitter.war,WEB-INF/web.xml	Web Module	WebSphere:cell=Cell01,cluster=BPM.AppCluster

7. In the configuration page, update the Class loader order from Parent first to Parent last as shown below:



Configuration

General Properties

* URI

BPMEventEmitter.war

Alternate deployment descriptor

* Starting weight

10000

* Class loader order

Classes loaded with local class loader first (parent last)

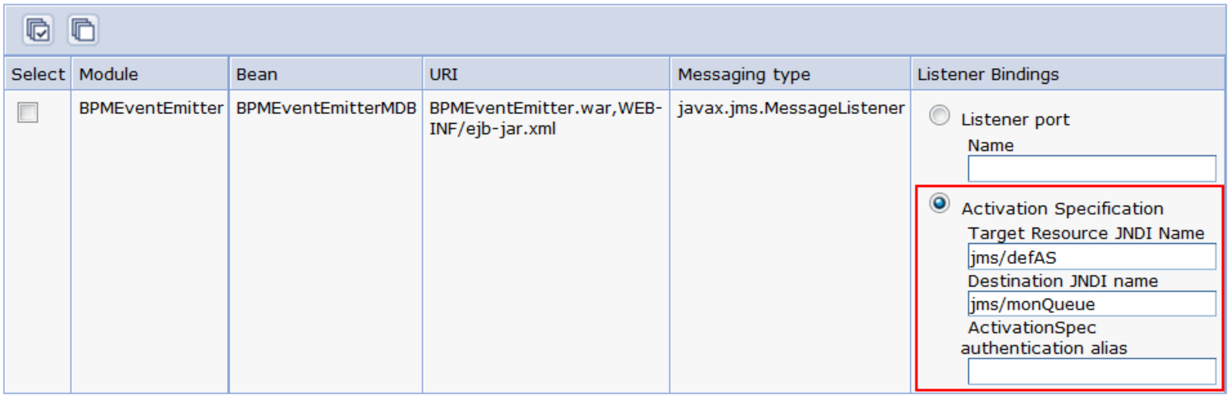
Additional Properties

- Stateful session bean failover settings
- View Module Class Loader
- Custom properties
- Target specific application status
- View EJB Deployment Descriptor
- View Web Deployment Descriptor
- Session Management
- Web Module Proxy Configuration

8. Click **OK** and in the follow up page and click **Save** to save the change to the main WAS configuration.

Optional: If the AS and queue JNDI used is not the default value, and you have not updated them before installing the application, you can update that in the following page:

Enterprise Applications > BPMEventEmitter_war > Message Driven Bean listener bindings



Select	Module	Bean	URI	Messaging type	Listener Bindings
□	BPMEventEmitter	BPMEventEmitterMDB	BPMEventEmitter.war,WEB-INF/ejb-jar.xml	javax.jms.MessageListener	○ Listener port Name ● Activation Specification Target Resource JNDI Name jms/defAS Destination JNDI name jms/monQueue ActivationSpec authentication alias

Optional: If you enabled Java 2 Security on your server, when starting the application you may receive an exception similar to the following:

```
SecurityManag W   SECJ0314W: Current Java 2 Security policy reported a potential
violation of Java 2 Security Permission. Refer to the InfoCenter for further
information.

Permission:

modifyThreadGroup : Access denied ("java.lang.RuntimePermission"
"modifyThreadGroup")
```

You must update the was.policy file to grant this application access. Further details on this are available from: https://www.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/tsec_waspolicyfile.html

For this application, you must update the following file:

`profile_root/config/cells/cell_name/applications/BPMEventEmitter_war.ear/deployments/BPMEventEmitter_war/META-INF/was.policy`

Update the contents as shown below:

```
//
// Template policy file for enterprise application.
// Extra permissions can be added if required by the enterprise
application.
//
// NOTE: Syntax errors in the policy files will cause the enterprise
application FAIL to start.
//       Extreme care should be taken when editing these policy files.
It is advised to use
//       the policytool provided by the JDK for editing the policy files
//       (WAS_HOME/java/jre/bin/policytool).
//

grant codeBase "file:${application}" {
  permission java.lang.RuntimePermission "stopThread";
  permission java.lang.RuntimePermission "modifyThread";
  permission java.lang.RuntimePermission "modifyThreadGroup";
  permission java.lang.RuntimePermission "createSecurityManager";
};

grant codeBase "file:${jars}" {
};

grant codeBase "file:${connectorComponent}" {
};

grant codeBase "file:${webComponent}" {
};


grant codeBase "file:${ejbComponent}" {

};
```

Start the application

After the application is installed, it can process the messages. The application will retrieve message from the DEF monitor event queue, transform them into JSON objects, and target the Elasticsearch server.

1. Start the application on the admin console page. The default address is: http://<Server_Address>:9060/admin

2. After logging in, expand **Applications** > **Application Types** > **WebSphere enterprise applications** in the left panel. In the right panel, select BPMEventEmitter_war then click **Start**.

After a successful start, you may see a log entry in SystemOut.log similar to the following:

```
[3/21/17 15:29:49:509 IST] 0000b44b LifeCycleMana I   I:  DEF2ES MDB
started.

[3/21/17 15:29:49:509 IST] 0000b44b ConfigConnect I   I: Kafka connection
disabled.

[3/21/17 15:29:49:727 IST] 0000b44b ConfigConnect I   I: ElasticSearch
connection created.
```

For any issues, check the Troubleshooting section at the end of this document.

Install, configure and run the EventSummaryAgent

The EventSummaryAgent is an agent application which will monitor the new events added in the configured Elasticsearch index and then generate summary events.

Prerequisites and key words

Before configuring the EventSummaryAgent, you must:

a. Know the target Elasticsearch server hosts. If security is enabled on server, know the **username**, **password** and **SSL/TLS related settings**.
b. Know the Elasticsearch **index** used to store the data generated by BPMEventEmitter.
c. Have a working JVM installed and correct JAVA_HOME set.

Install and update the configuration file

In the package, find the **EventSummaryAgent.tar file** and save it to the server where you will run this agent. You can find the sample configuration file inEventSummaryAgent/conf/EventSummaryAgent.yml

The configuration file is in YAML format:

```
#Facade type: elasticSearch
facadeType:elasticSearch
esDataIndex: monitor
#Time gap used by event picker in milliseconds
pickerTimeGap: 60000
# Enable the sample Business Data processor
enableBusinessDataSample:false
# Quality of service. Provided two mode now: strictMode | ignoreError
# strickedMode- will retry when meet error to prevent data lost on summary types.
# ignoreError - Will ignore error and continue processing. The summary type may not
complete when error happens.
qualityOfService:strickedMode
# the configuration properties for the elastic search
esConfiguration:
hosts: localhost:9200
# the following properties should be enabled when elastic search security is on
username: elastic
password:<xor>cXxraGFIdw==
httpsTrustType:
trustFileLocation:
hostnameVerifier:
esEventSourceFacadeConfiguration:
# Index used to store progress data
persistentDataIndex:oiprogress
# Type used to store progress data
persistentDataType:readcursor
```

Update the values per your environment, you can update directly or save a copy and update:

facadeType: Keep the default value.

esDataIndex: Used as the Elasticsearch index name where it gets the events generated by BPMEventEmitter and stores the generated data.

pickerTimGap: A time gap used internal to prevent random data order. The suggested time is at least 10 seconds. The value is in milliseconds.

enableBusinessDataSample: As the business data content is related to applications, there is no common solution for how to generate a business data summary. A sample business data handle has been provided which can generate a business data summary with process instance ID and monitor group ID. By default, this is disabled, you can enable it by assigning a value “true”.

qualityOfService: Quality of service which is used to control the agent behavior when errors are received. There are two available modes:

strickedMode - will retry when an error is received to prevent data lost on summary types.

ignoreError - will ignore the error and continue processing. The summary type may not complete when an error occurs.

esConfiguration: The configurations for Elasticsearch servers.

Hosts: Lists all of the server addresses in the Elasticsearch cluster. If you have not enabled security (SSL/TLS) on your Elasticsearch, you can use the IP directly. For example: 192.168.0.1:9200,127.0.0.1:9200

If you enabled security (SSL/TLS), you must input an “https” prefix to the address to announce that the communicate should use HTTPS protocol. For example: https://192.168.0.1:9200,https://127.0.0.1:9200

username and **password:** Used when you enabled basic authentication on your Elasticsearch cluster. For password field, you can use plain text or use anencoded password. You can use the **EventSummaryAgent**to encode your password. You can run encodePassword function to get the encoded value as shown below:

```
EventSummaryAgent.sh/bat -encodePassword elastic

<xor>cXxraGFIdw==
```

If you enabled SSL/TLS on your Elasticsearch, you must set the **httpsTrustType** per the type you used. Three kinds are supported: ALL, CRT and JKS.

ALL: The application accepts all HTTPs communication. It should be used for test purposes only.

CRT: Provide the CA certificate file (.crt) to support that the application accepts certain HTTPs connections. In this option, you must provide the **trustFileLocation** setting with an absolute address. Ensure that the BPM server can access that file. For example:

```
httpsTrustType: CRT

trustFileLocation: /opt/IBM/BPM/elasticSearch.crt
```

Default: The agent accepts HTTPs communication accepted by the JVM default settings.

hostnameVerifier: Accepts Boolean values, leave as “false” in the production environment. If you are using the test environment which uses a CRT certificate including a wrong host or IP address, you can set that to true for testing purposes only.

Security tips

Before enabling the Elasticsearch security, you can leave all of the security related fields empty or remove them from the configuration file to disable those settings.

After enabling the Elasticsearch security by installing X-Pack or protected that by using Nginx, you should provide the correct value for the fields.

For example:

```
hosts: https://<some_address>:9200
# the following properties should be enabled when elastic search security is on
username: elastic
password:<xor>cXxraGFIdw==
httpsTrustType: CRT
trustFileLocation: /opt/IBM/BPM/elastcisearch.crt
hostnameVerifier:false
```

This means that the Elasticsearch server is protected with TLS and basic authentication. You have the CRT certification file located on /opt/IBM/BPM/elasticsearch.crt, and the CRT has the correct host/IP address to the server.

Command line parameters

Usage of the EventSummaryAgent:

```
EventSummaryAgent.sh/bat -configFile<configFileLocation> | -
encodePassword<passwordValue> | -help
```

-configFile<configFileLocation>: Use this parameter to start the agent. The config file location is the file location you created.

-encodePassword<passwordValue>: Use this parameter to generate an encoded password as indicated in the configuration.

-help: Will print help message.

For any issues, check the troubleshooting section at the end of this document.

Start the EventSummaryAgent

To start the EventSumaryAgent, run the following command at the utility's <*root_folder*>/bin:

For Linux:

```
./EventSummaryAgent.sh -configFile../conf/EventSummaryAgent.yml
```

For Windows:

```
EventSummaryAgent.bat -configFile ../conf/EventSummaryAgent.yml
```

If the agent starts successfully, you may find a log entry similar to the following:

```
<time stamp>com.ibm.bpm.mon.oi.combine.EventSummaryAgentdoJob
INFO: I: Start getting process/activity events from the data source.
```

This message indicates that the agent is ready to begin processing the messages.

To stop the utility, send the kill signal using Ctrl+C from the command window, it will stop the EventSummaryAgent.

When running the EventSummayAgent in the background, use the "kill -2 <process_id>" to stop it.

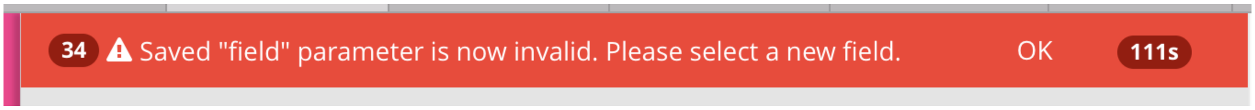
Import the dashboard definition

Prerequisites and key words

Before importing the dashboard definition **BPMDefaultDashboard.json** to Kibana, you should:

1. Ensure **BPMEventEmitter.war** is started
2. Ensure **EventSummaryAgent** is started

Note: You should have one process instance with a user task completed before importing the dashboard definition, otherwise you may receive the following error due to a Kibana limitation (https://github.com/elastic/elasticsearch/issues/22438):



34 ⚠ Saved "field" parameter is now invalid. Please select a new field.

Create an index alias (Optional)

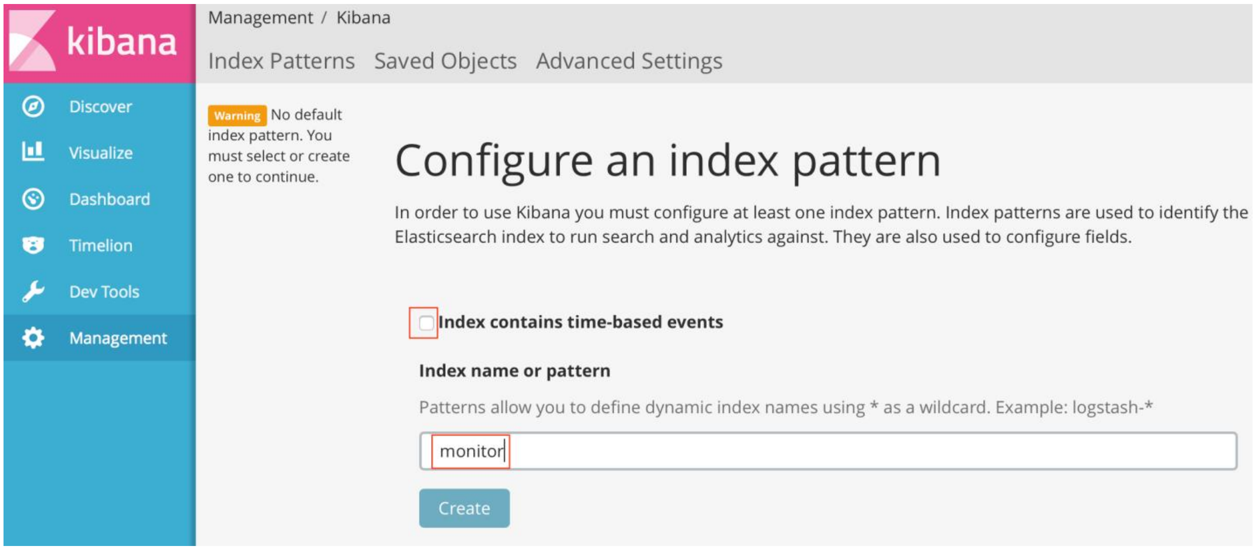
If you are not using **monitor** as the index name, you need to map all the indexes you used to **monitor** alias. For the detail API, refer to https://www.elastic.co/guide/en/elasticsearch/reference/master/indices-aliases.html

The following example is using a REST API in Kibana Dev Tools to set **monitor** as alias of index **monitor2**:

```
POST /_aliases
{
  "actions" : [
    { "add" : { "index" : "monitor2", "alias" : "monitor" } }
  ]
}
```

Create Index Patterns

1. In Kibana, click **Management** > **Index Patterns**, uncheck **Index contains time-based events.**
2. Enter **monitor** as the **Index name or** pattern, click **Create:**



Warning No default index pattern. You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

□ Index contains time-based events

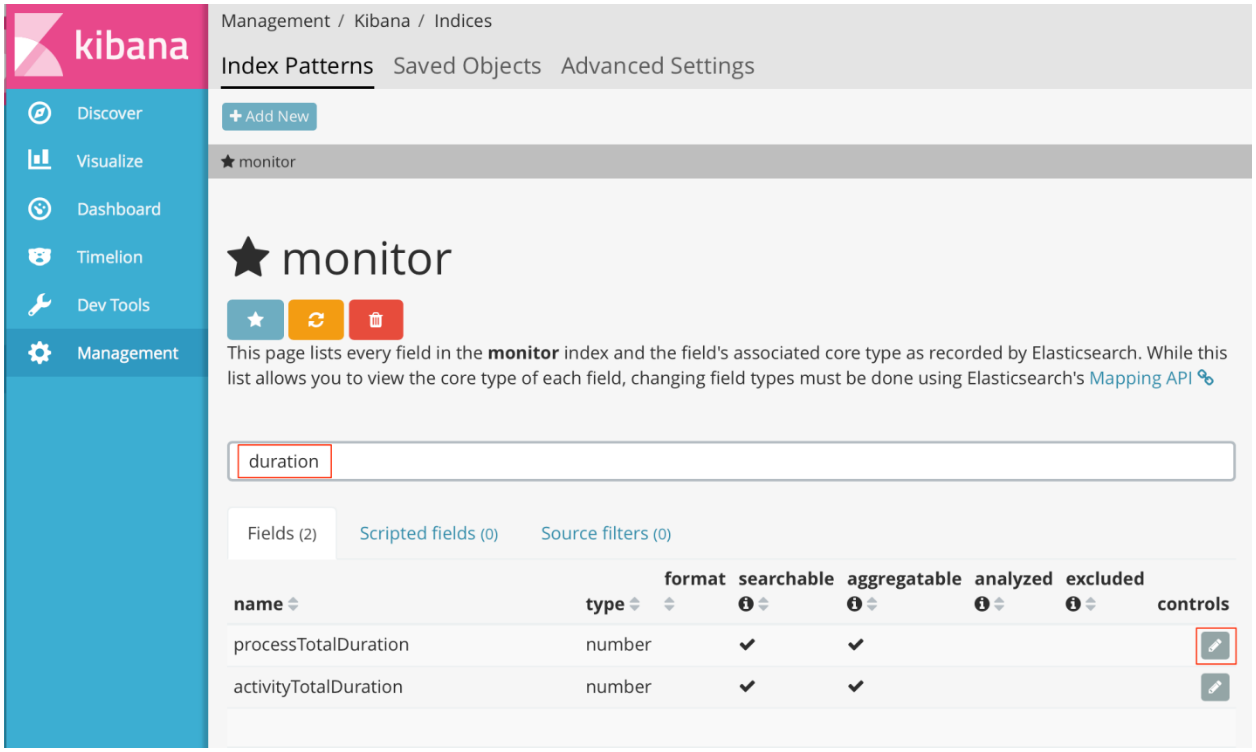
Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

monitor

3. Search **Duration**, you will see two fields: **processTotalDuration** and **activityTotalDuration**

4. Click ✎ beside **processTotalDuration**



Management / Kibana / Indices

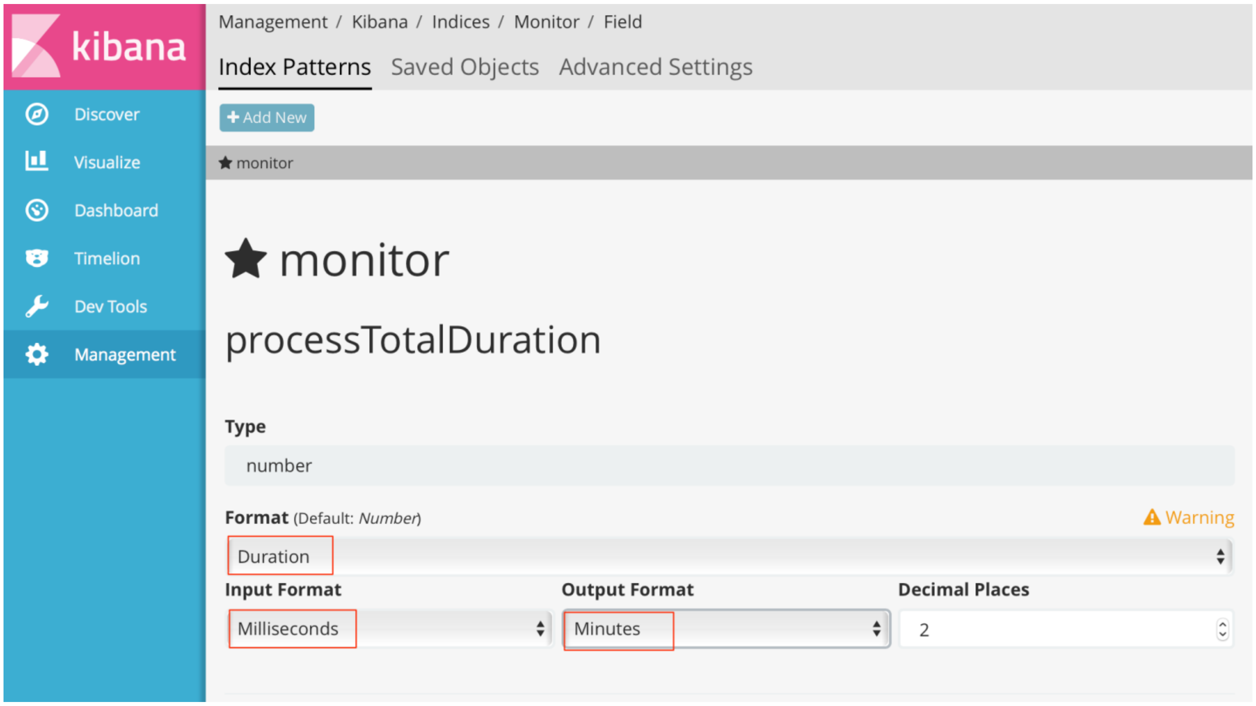
★ monitor

This page lists every field in the **monitor** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API

duration

name	type	format	searchable	aggregatable	analyzed	excluded	controls
processTotalDuration	number		✓	✓			✎
activityTotalDuration	number		✓	✓			✎

5. Select **Duration** for Format, **Milliseconds** for Input Format, **Minutes** for Output Format. This will help to transform processTotalDuration from Milliseconds to Minutes.



Management / Kibana / Indices / Monitor / Field

★ monitor

processTotalDuration

Type: number

Format (Default: *Number*): Duration

Input Format: Milliseconds

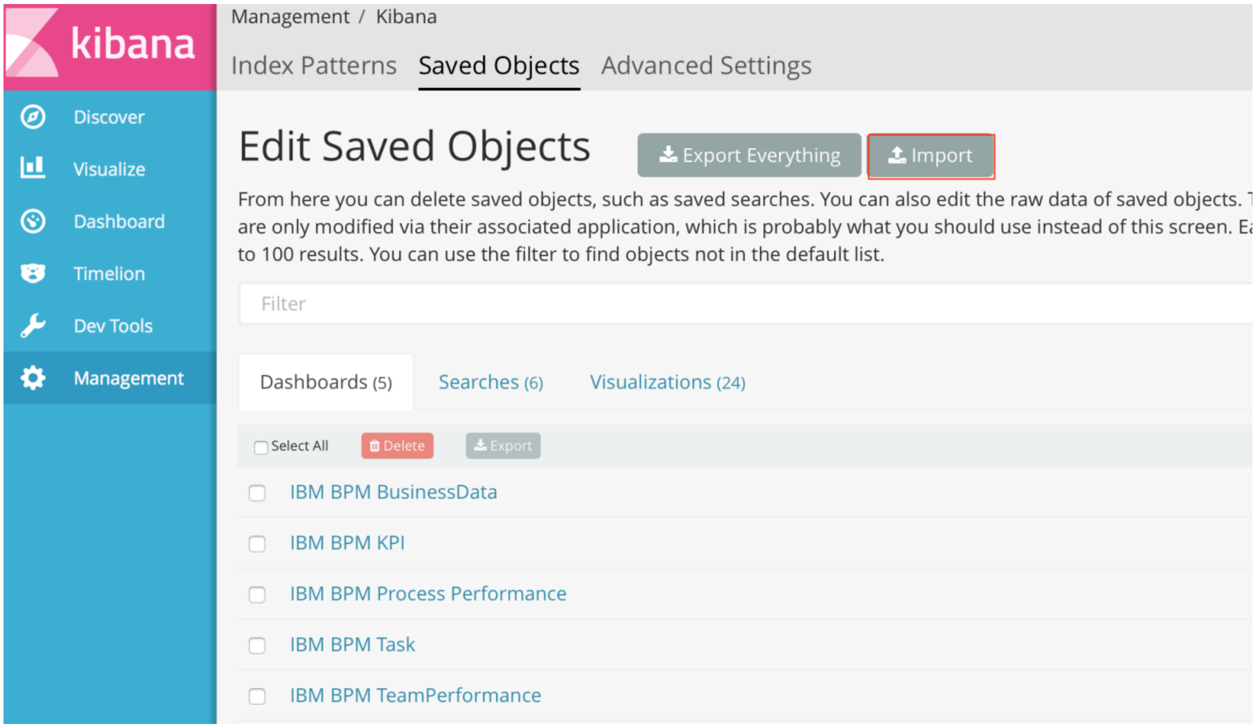
Output Format: Minutes

Decimal Places: 2

6. Repeat step d to step f to change the format for activityTotalDuration.

Import the dashboard definition

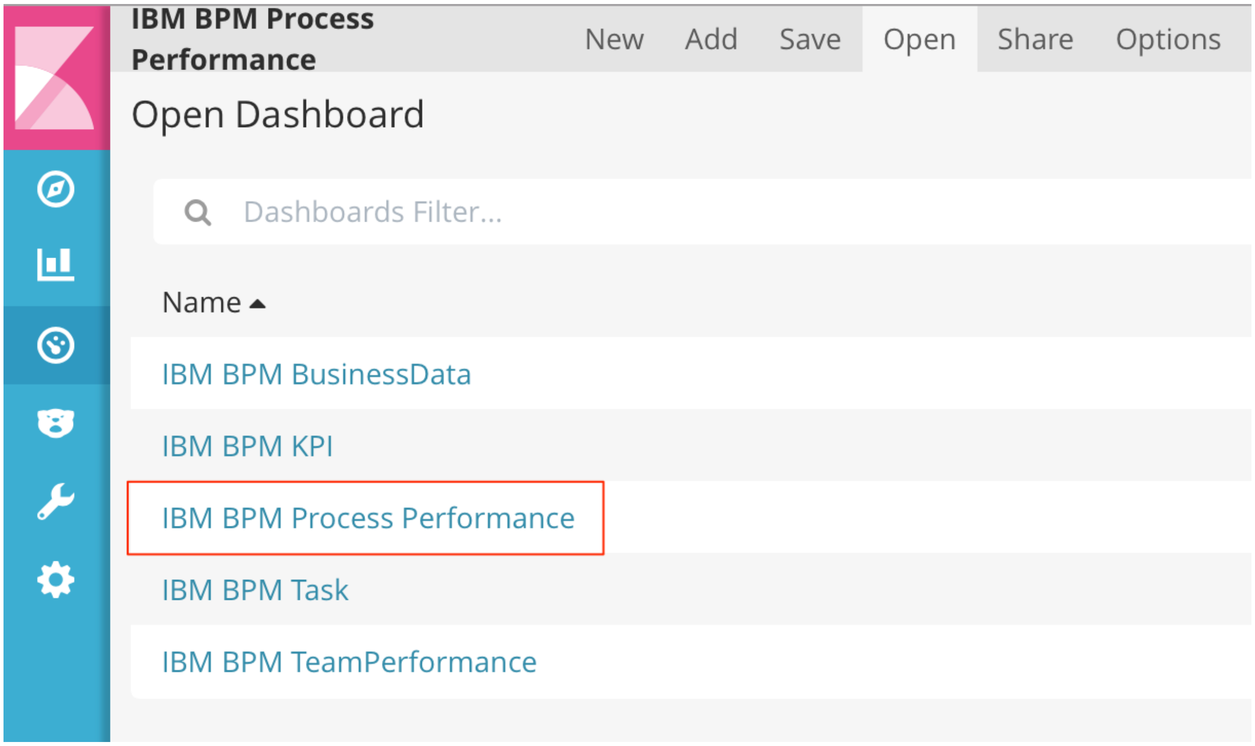
1. In Kibana, select **Management** > **Saved Objects**.
2. Click **Import**, select **BPMDefaultDashboard.json**.
3. After importing, you can see **5** extra Dashboards, **6** extra Searches, and **24** extra Visualizations:



From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. T are only modified via their associated application, which is probably what you should use instead of this screen. Ea to 100 results. You can use the filter to find objects not in the default list.

Open the imported dashboard

In Kibana, select **Dashboard**, open **IBM BPM Process Performance:**



IBM BPM Process Performance

New Add Save Open Share Options

Open Dashboard

Dashboards Filter...

Name ▲

IBM BPM BusinessData

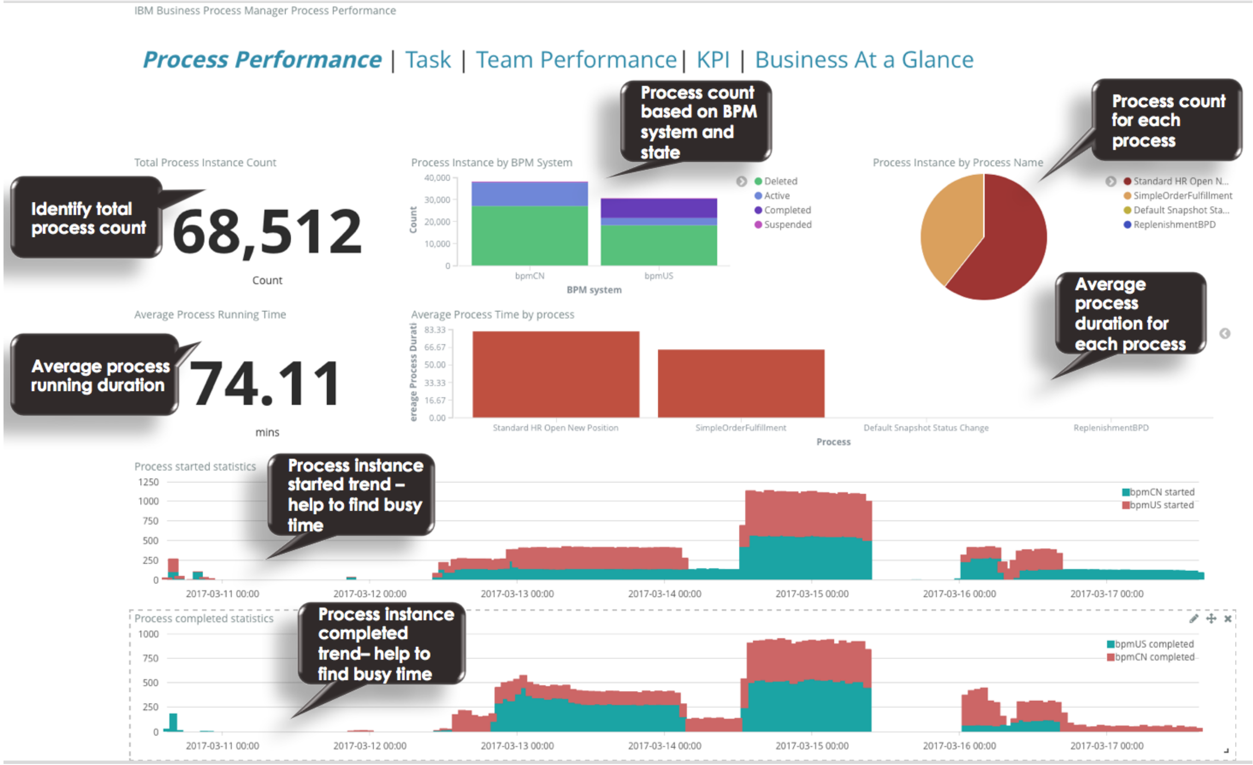
IBM BPM KPI

IBM BPM Process Performance

IBM BPM Task

IBM BPM TeamPerformance

1. Select **Process Performance** to switch to the Process Performance dashboard which is the default dashboard to display process related statistics



Process count based on BPM system and state

Process count for each process

Identify total process count

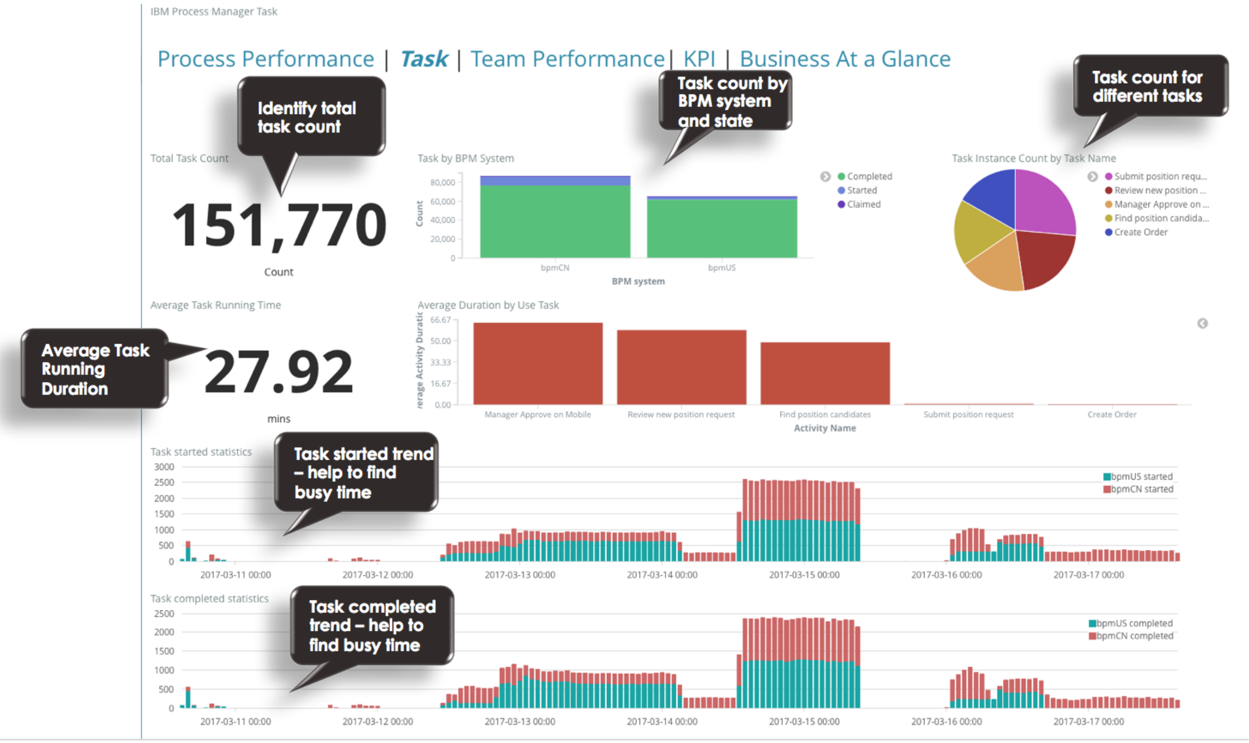
Average process duration for each process

Average process running duration

Process instance started trend – help to find busy time

Process instance completed trend– help to find busy time

2. Select **Task** to switch to the Task dashboard which is the default dashboard to display user task related statistics.
Note: This dashboard is only for **User Task**. System Task and other activities are not taken into consideration.



Identify total task count

Task count by BPM system and state

Task count for different tasks

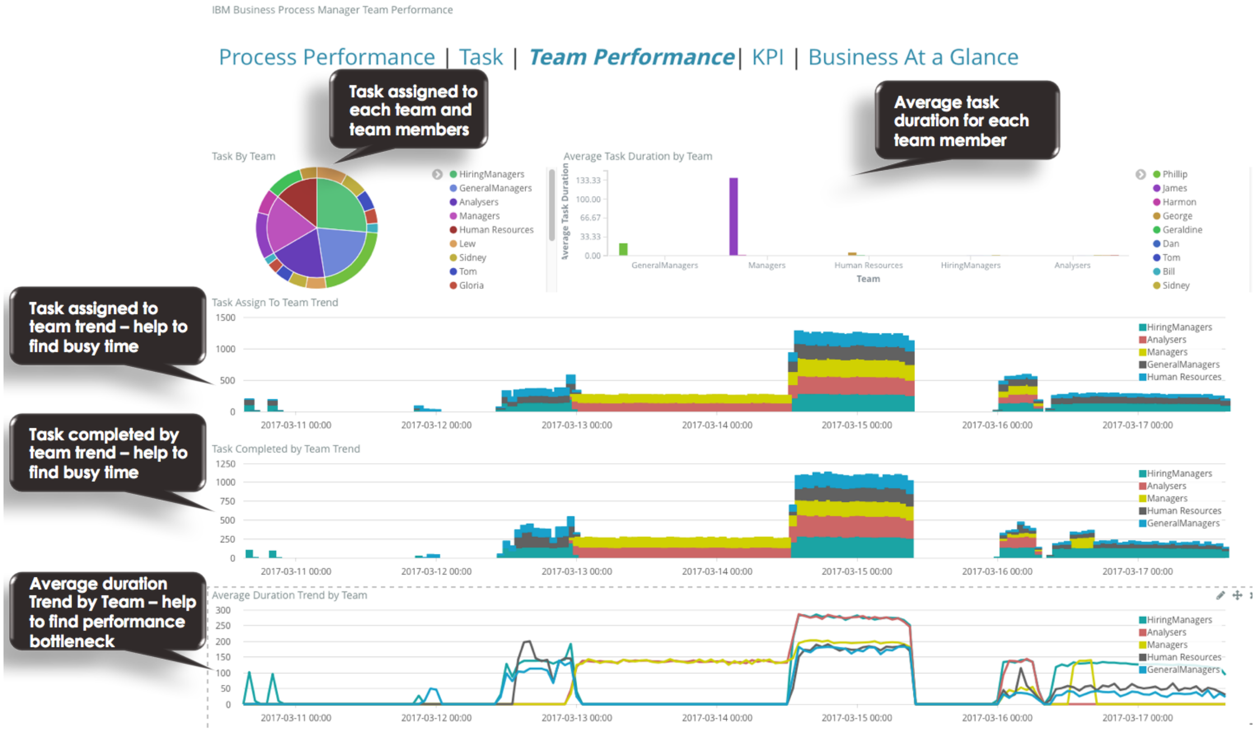
Average Task Running Duration

Task started trend – help to find busy time

Task completed trend – help to find busy time

3. Select **Team Performance** to switch to the Team Performance dashboard which is the default dashboard to display team related statistics.
Note: This dashboard is only for **User Task**. System Task and other activities are not taken into

consideration.



IBM Business Process Manager Team Performance

Process Performance | Task | *Team Performance*| KPI | Business At a Glance

Task assigned to each team and team members

Average task duration for each team member

Task assigned to team trend – help to find busy time

Task completed by team trend – help to find busy time

Average duration Trend by Team – help to find performance bottleneck

4. Select **KPI** to switch to the KPI dashboard which is an empty dashboard. You can add your custom KPI visualization here.

IBM Business Process Manager KPI

Process Performance | Task | Team Performance| *KPI* | Business At a Glance

5. Select **Business At a Glance** to switch to the Business Data dashboard. You can add your custom business data visualization here.

IBM Business Process Manager BusinessData

Process Performance | Task | Team Performance| KPI | *Business At a Glance*

Import the Hiring Sample Dashboard (Optional)

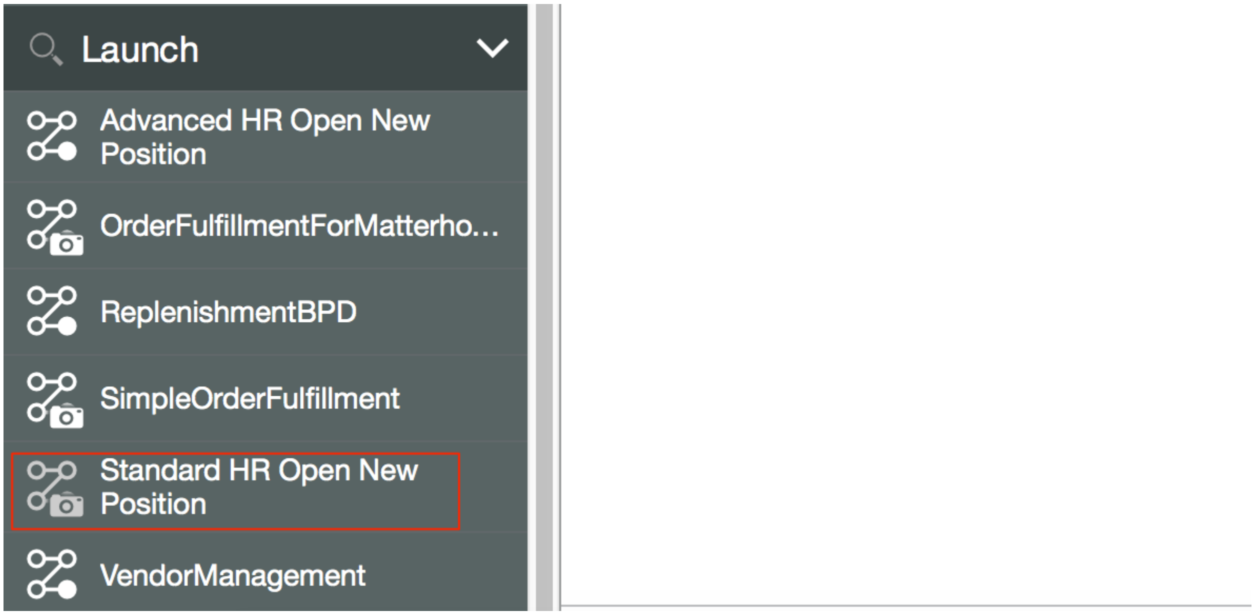
Included is a sample Business Data dashboard for the Hiring Sample. To import it, follow these steps:

1. Modify **EventSummaryAgent.yml** for EventSummaryAgent (EventSummaryAgent/conf/EventSummaryAgent.yml) to enable the sample Business Data processor

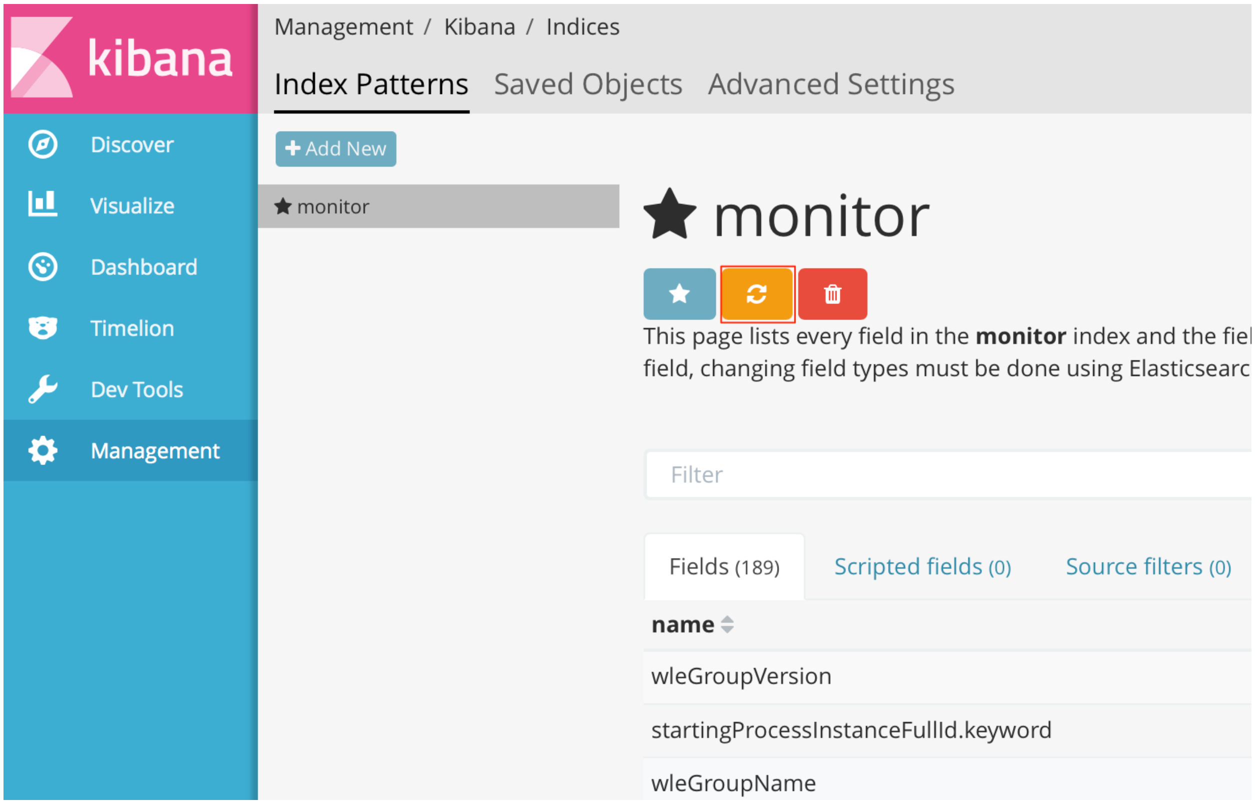
```
# Enable the sample Business Data processor
enableBusinessDataSample:true
```

2. Restart EventSummaryAgent.
3. In BPM Process Portal, run a process instance for Standard HR Open New Position in Hiring Sample and **COMPLETE** it.

   Note: You need to **complete** a process instances to ensure that all of the raw data of Elasticsearch index is included.


Launch
Advanced HR Open New Position
OrderFulfillmentForMatterho...
ReplenishmentBPD
SimpleOrderFulfillment
Standard HR Open New Position
VendorManagement

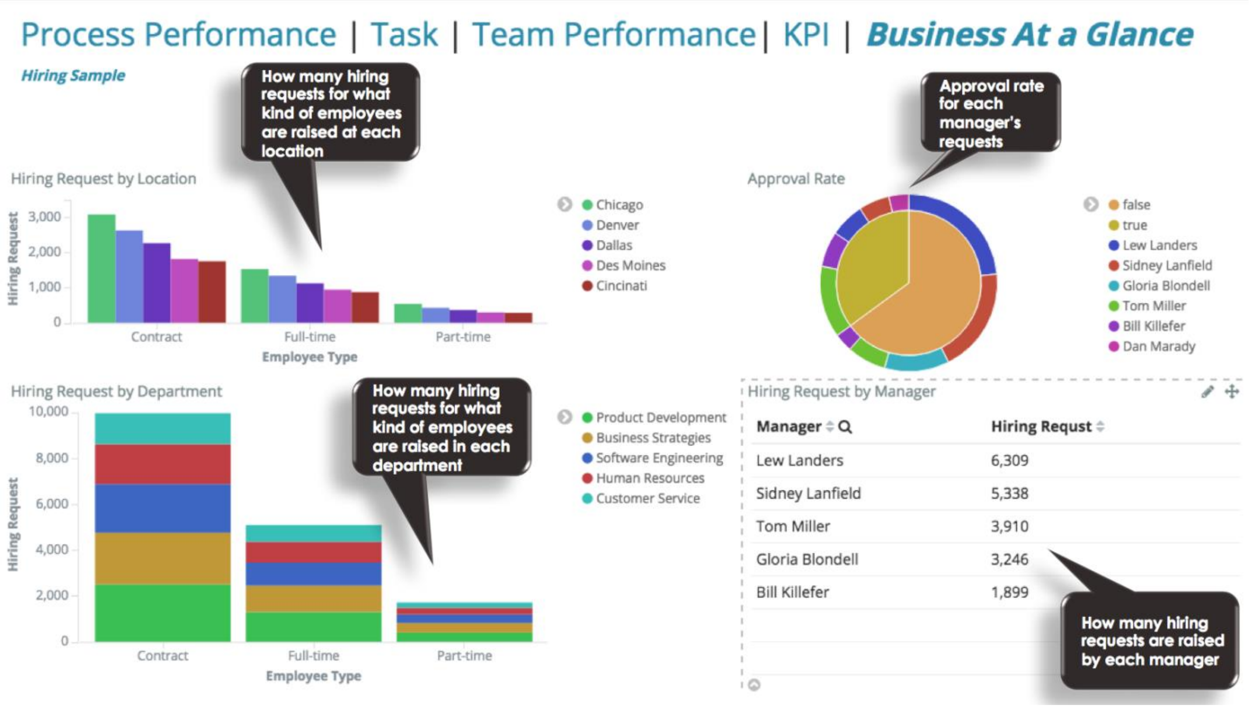
4. Click **Management > Index Patterns**, select **monitor** index, click ⟳. Kibana will retrieve the new fields for Business Data that are generated in the Elasticsearch index.



This page lists every field in the **monitor** index and the fiel
field, changing field types must be done using Elasticsearc

name
wleGroupVersion
startingProcessInstanceFullId.keyword
wleGroupName

5. In Kibana, click **Management** > **Saved Objects**, click **Import**, select **HiringSampleDashboard.json.**
6. Click **Business At a Glance** to see the custom Business Data dashboard for the Hiring Sample.


Process Performance | Task | Team Performance | KPI | Business At a Glance
Hiring Sample
How many hiring requests for what kind of employees are raised at each location
Approval rate for each manager's requests
Hiring Request by Location
Hiring Request
3,000
2,000
1,000
0
Contract
Full-time
Part-time
Employee Type
Chicago
Denver
Dallas
Des Moines
Cincinati
Approval Rate
false
true
Lew Landers
Sidney Lanfield
Gloria Blondell
Tom Miller
Bill Killefer
Dan Marady
Hiring Request by Department
How many hiring requests for what kind of employees are raised in each department
10,000
8,000
6,000
4,000
2,000
0
Contract
Full-time
Part-time
Employee Type
Product Development
Business Strategies
Software Engineering
Human Resources
Customer Service
Hiring Request by Manager
How many hiring requests are raised by each manager

Manager	Hiring Requst
Lew Landers	6,309
Sidney Lanfield	5,338
Tom Miller	3,910
Gloria Blondell	3,246
Bill Killefer	1,899

Troubleshooting

Troubleshooting when the event was not generated

If you find the dashboard at Kibana was not updated correctly or has no new events coming in, you need start from the BPMEventEmittertoEventSummaryAgent section of this document to troubleshoot.

1. Check if the DEF event can be generated by IBM BPM
    - Stop the BPMEventEmitter temporarily. Use the WAS admin console, select **Service integration > Service Integration Bus Brower > *Your_BUS_name*> Destinations > *Your_DEF_destination* > Queue points**
    - At this page, because the DEF event consumer – BPMEventEmitter - has been stopped, you can see the DEF events stuck at this queue, and the queue depth is increasing.
    - Otherwise, check the steps in Enable the Dynamic Event Framework (DEF) at BPM to make sure DEF was successfully enabled.

2. Check if the ProcessEvent and ActivityEvent document can be generated at the Elasticsearch
    - Get the basic count of ProcessEvent by running the following command at Kibana's Dev Tools:

      ```
      GET monitor/ProcessEvent/_count
      ```

      Note: the monitor is the default index name, which is configurable, replace it according to your configuration.

    - Get the basic count of the ActivityEvent by running the following command at the Kibana's Dev Tools:

      ```
      GET monitor/ActivityEvent/_count
      ```

    - Start the BPMEventEmitter, after this step, you should see the count of the ProcessEvent and ActivityEvent increase. Otherwise, check the BPMEventEmitter's log, which belongs to the SystemOut.log at the server host the BPMEventEmitter WAR.

3. Check if the ProcessSummary and ActivitySummary type document can be generated at the Elasticsearch
    - Stop the EventSummaryAgent
    - Get the basic count of ProcessSummary by running the following command at the Kibana's Dev Tools:

      ```
      GET monitor/ProcessSummary/_count
      ```

    - Get the basic count of the ActivitySummary by running the following command at the Kibana's Dev Tools:

      ```
      GET monitor/ActivitySummary/_count
      ```

    - After the ProcessEvent and ActivityEvent document count increases, you can start the EventSummaryAgent to see if it works.

After the EventSummaryAgenthas been started (by default it is one minute) the EventSummaryAgent will start to pick up new event type documents and the number of the summary type document will increase. Check the logs at the <*EventSummaryAgent_Root*>/log folder if you found the summary type documents has not increased.

Troubleshooting the exceptions

Ensure that you change the WAR module's "Class loader order" to "Classes loaded with local class loader first (parent last)" if either of these exceptions are received in the SystemOut.log:

Exception 1	`CNTR0020E: EJB threw an unexpected (non-declared) exception during invocation of method "onMessage" on bean "BeanId(BPMEventEmitter_war#BPMEventEmitter.war#BPMEventEmitterMDB, null)". Exception data: java.lang.NoSuchMethodError: org/apache/http/HttpHost.create(Ljava/lang/String;)Lorg/apache/http/HttpHost;`
Exception 2	`0000b44b LifeCycleMana E class com.ibm.bpm.mon.oi.LifeCycleManageBeanstartMethod E: Create elastic search index mapping failed with exception. java.io.IOException: listener timeout after waiting for [10000] ms`

Potential event lost

If your DEF queue depth did not configure properly, it has the potential for the event to be lost.

The default queue depth: The high message threshold is 50000. If your BPMEventEmitter was not started or the event producer created the events faster than the consumer, the events which exceed the threshold will be lost.

Tune this number to match your system's peak time to avoid failure of the event consumer.

For more information of this exception, see:

http://www-01.ibm.com/support/docview.wss?uid=swg21624736