

TIBCO iProcess[®] Engine for Cloud

Configuration Guide

*Software Release 11.6.1
October 2017*

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE TIBCO IPROCESS ENGINE INSTALLATION GUIDE). USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIB, TIBCO, TIBCO Software, TIBCO Adapter, Predictive Business, Information Bus, The Power of Now, TIBCO iProcess are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

EJB, Java EE, J2EE, JMS and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. Please see the readme.txt file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

Copyright © 1994-2017 TIBCO Software Inc. ALL RIGHTS RESERVED.

TIBCO Software Inc. Confidential Information

Contents

Chapter 1 Introduction	1
Document Scope	2
Overview	3
Chapter 2 Configuring Virtual Machines (VM)	5
Configuring an Imported VM (RHEL)	6
Prerequisites	6
Procedure	6
Configuring an Amazon Provided Image	8
Prerequisites	8
Procedure	8
Chapter 3 Configuring Security Groups	9
Examples of Security Groups for TIBCO iProcess Engine	10
Example 1	10
Example 2	12
Example 3	14
Chapter 4 Configuring TIBCO iProcess Technology Plug-ins	17
Setting Parameters	18

Chapter 1 **Introduction**

This guide describes how to setup TIBCO iProcess[®] Engine and related components on the cloud.

Topics

- *[Document Scope, page 2](#)*
- *[Overview, page 3](#)*

Document Scope

The scope of this document is limited to setting up the below products on AWS, example databases, and their connectivity:

- TIBCO iProcess[®] Engine
- TIBCO iProcess[®] Workspace (Windows)
- TIBCO iProcess[®] Workspace (Browser)
- TIBCO iProcess[®] Workspace Plug-ins
- TIBCO iProcess[®] Technology Plug-ins

Although these products are designed to run on various platforms and against various databases, this document illustrates only a few combinations.

Overview

You can setup iProcess[®] Engine on AWS by importing and [Configuring Virtual Machines \(VM\)](#). Once you setup TIBCO iProcess[®] Suite on AWS, you need to configure security groups for your Virtual Private Cloud (VPC) to control inbound and outbound traffic. See [Configuring Security Groups](#) for details.

Chapter 2 **Configuring Virtual Machines (VM)**

This chapter explains how to configure an imported Red Hat® Enterprise Linux® (RHEL) image or an Amazon Provided Image (AMI).

Topics

- *[Configuring an Imported VM \(RHEL\), page 6](#)*
- *[Configuring an Amazon Provided Image, page 8](#)*

Configuring an Imported VM (RHEL)

The procedure below explains how you can configure values for an imported Virtual Machine (VM) in AWS for it to function correctly.

Prerequisites

Before you can configure a VM, you need to do the following:

1. Import a VM to AWS. For more information, see [VM Import/Export](#) on the AWS documentation page.
2. Launch the instance(s) on which you imported the VM for iProcess Engine and the database server. See [Launch Your Instance](#) on the AWS documentation page.

Procedure

1. Turn off firewall for all created instances.
2. Update database server files with the private IP of your domain on the instance where you imported iProcess Engine. For example, for an Oracle Database Server, update `tnsnames.ora` and `listener.ora` files.
3. Correct the machine name for node entry in `swpro.node_cluster` table. This is essential because the imported VM cannot be recognized by its old local machine name. You can use the following command to change the machine name.
`UPDATE swpro.node_cluster SET physical_machine_name='ip-172-31-5-148' where master=1;`
 where "ip-172-31-5-148" is the hostname of the machine. Alternately, you can run the `hostname` command to get the string to set the correct name here.
4. Remove old machine entries from `/etc/hosts` if any. This will help avoid errors due to a machine name mismatch.
5. Add a fixed port range. This step is important when you are using iProcess Engine in a firewalled environment. Adding a fixed port range restricts iProcess Engine processes to accept incoming RPC requested from within that port range. For more information, see *Administering Firewall Port Ranges in TIBCO iProcess Engine Administrator's Guide*. The following are commands to add a fixed port range.

- `swadm ADD_RANGE -p <port_number> -s <port_range>`
 Example: `swadm ADD_RANGE -p 46000 -s 20`
- `swadm SET_RANGE 1 <port_range_ID>`
 Example: `swadm SET_RANGE 1 1`

6. Add an AQ port range. The following is a command for the same.

Note: This step applies only if you are using an Oracle Database Server.

— `swadm ADD_AQ_PORT_RANGE 1 <port_number> <port_range>`

Example: `swadm ADD_AQ_PORT_RANGE 1 48000 50`

Once you have configured the imported VM(s), you need to configure security groups for each VM in order to control inbound and outbound connections. See [Configuring Security Groups, page 9](#).

Configuring an Amazon Provided Image

The procedure below explains how you can configure values for an Amazon Provided Image (AMI) on AWS.

Prerequisites

Before you can configure an AMI, you need to do the following:

1. Install the below software on one or multiple instances (as per your preference):
 - TIBCO iProcess Engine
 - Database Server
2. Launch all created instances. See [Launch Your Instance](#) on the AWS documentation page.

Procedure

1. Turn off firewall for all created instances.
2. Add a fixed port range in the iProcess Engine configuration. This step is important when you are using iProcess Engine in a firewalled environment. Adding a fixed port range restricts iProcess Engine processes to accept incoming RPC requests from within that port range. For more information, see *Administering Firewall Port Ranges in TIBCO iProcess Engine Administrator's Guide*. The following are commands to add a fixed port range.
 - `swadm ADD_RANGE -p <port_number> -s <port_range>`
 Example: `swadm ADD_RANGE -p 46000 -s 20`
 - `swadm SET_RANGE 1 <port_range_ID>`
 Example: `swadm SET_RANGE 1 1`
3. Add an AQ port range. The following is a command for the same.

Note: This step applies only if you are using an Oracle Database Server.

 - `swadm ADD_AQ_PORT_RANGE 1 <port_number> <port_range>`
 Example: `swadm ADD_AQ_PORT_RANGE 1 48000 50`

Once you have configured the imported VM(s), you need to configure security groups for each VM in order to control inbound and outbound connections. See [Configuring Security Groups](#), page 9.

Chapter 3

Configuring Security Groups

A security group acts as a virtual firewall for your AWS instance to control inbound and outbound traffic. You can create multiple security groups to allow access as required.

When you launch an instance in a Virtual Private Cloud (VPC), you can assign the instance to up to five security groups. Security groups act at the instance level, not the subnet level. Therefore, each instance in your VPC can be assigned to a different set of security groups. This chapter provides examples of configuring security groups for iProcess Engine with different database servers.

Topics

- [*Examples of Security Groups for TIBCO iProcess Engine, page 10*](#)

Examples of Security Groups for TIBCO iProcess Engine

Although you can configure security groups as per your security protocols, the following are three typical security group configuration examples.

Example 1

If you plan to use iProcess® Workspace (Windows) instances within AWS to connect to TIBCO iProcess Engine, perform the following steps to appropriately configure security groups.

1. Launch an Elastic Compute Cloud (EC2) instance in your Virtual Private Cloud (VPC).
2. Name the created instance as 'ec2-OracleServer'. Install the Oracle Database Server on this instance.
3. Launch a second EC2 instance in your VPC.
4. Name the created instance 'ec2-iPE'. Install iProcess Engine on this instance.
5. Finally, launch a third EC2 instance in your VPC.
6. Name the created instance 'ec2-iPWW'. Install iProcess Workspace (Windows) on this instance.
7. Now, create security groups for all three EC2 instances.
 - Create security group sg-OracleServer for the instance ec2-OracleServer.
 - Create security group sg-iPE for the instance ec2-iPE.
 - Create security group sg-iPWW for the instance ec2-iPWW.
8. **Configure sg-OracleServer (Refer to the below table):**
 - a. Specify a custom TCP rule which would only allow machines (on an external domain) to access the Oracle Database server (the default port is 1521).
 - b. Specify a rule on ec2-OracleServer such that iProcess Engine can communicate with the database server.

Type	Protocol	Port Range	Source		Purpose
Custom TCP Rule	TCP	22	Custom	137.21.55.8/32	SSH to access the VM
All TCP*	TCP	0-65535	Custom	sg-iPE	To allow traffic from members of sg-iPE

Type	Protocol	Port Range	Source		Purpose
Oracle-RDS	TCP	1521	Custom	137.21.55.8/32	To access Oracle database from an external machine

Note - 137.21.55.8/32 is used as an illustration IP address, replace this with your own IP address.

9. Configure sg-iPE (Refer to below table):

- a. Specify a rule on ec2-iPE such that the database server can communicate with the iProcess Engine.
- b. Specify a rule on ec2-iPE such that the iProcess Workspace (Windows) can communicate with the iProcess Engine.

Type	Protocol	Port	Source		Purpose
Custom TCP Rule	TCP	22	Custom	137.21.55.8/32	SSH
All TCP*	TCP	0-65535	Custom	137.21.55.8/32	To allow traffic from members of sg-OracleServer
All TCP*	TCP	0-65535	Custom	sg-iPWW	To allow traffic from members of sg-iPWW

Note - 137.21.55.8/32 is used as an illustration IP address, replace this with your own IP address.

10. Configure sg-iPWW (Refer to the below table):

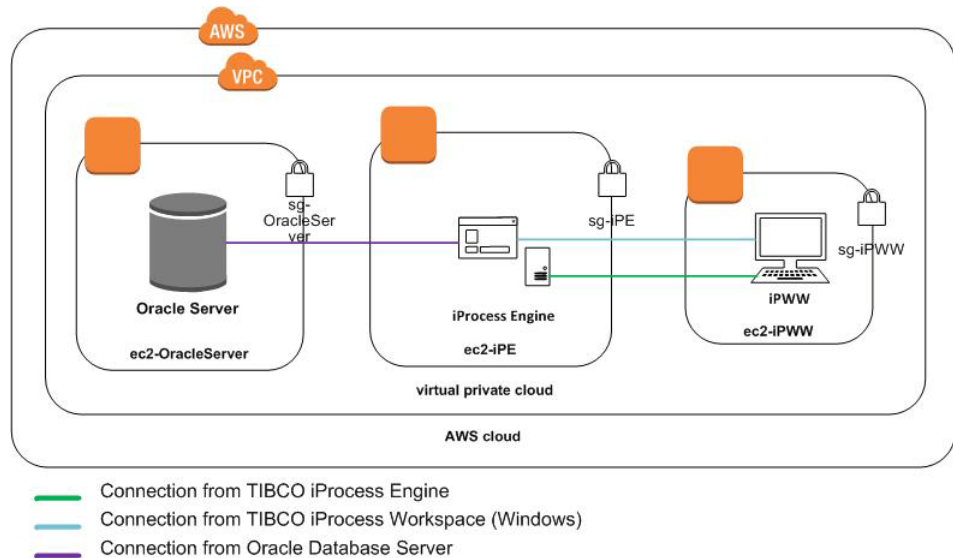
- a. Specify a rule on ec2-iPWW such that the iProcess Engine can communicate with the iProcess Workspace (Windows).
- b. Specify Remote Desktop (RDP) rule to allow access to ec2-iPWW from an external domain.

Type	Protocol	Port Range	Source		Purpose
RDP	TCP	3389	Custom	137.21.55.8/32	Remote Desktop Connection

Note - 137.21.55.8/32 is used as an illustration IP address, replace this with your own IP address.

Once you configure these security groups, your setup will look something like the below illustration.

(*) Note - Since the setup in this example includes iProcess Engine, database server, and iProcess Workspace (Windows) within AWS, you can open all ports for the instances to communicate among themselves.



Example 2

If you plan to connect to iProcess Engine from an external machine which has iProcess Workspace (Windows) installed, perform the following steps to appropriately configure security groups.

1. Launch an EC2 instance in your VPC.
2. Name the created instance 'ec2-OracleServer'. Install the Oracle Database Server on this instance.
3. Launch a second EC2 instance in your VPC.
4. Name the created instance ec2-iPE. Install iProcess Engine on this instance.
5. Install iProcess Workspace (Windows) on the client machine (on an external domain). See *TIBCO iProcess Workspace (Windows) Installation* for more information.
6. Now, create security groups for the two EC2 instances:
 - Create sg-OracleServer for the instance ec2-OracleServer.
 - Create sg-iPE for the instance ec2-iPE.

7. Configure sg-OracleServer (Refer to the below table):

- a. Specify a custom TCP rule which would only allow machines (on an external domain) to access the Oracle Database server (the default port is 1521).
- b. Specify a rule on ec2-OracleServer such that iProcess Engine can communicate with the database server.

Type	Protocol	Port Range	Source		Purpose
Custom TCP Rule	TCP	22	Custom	137.21.55.8/32	SSH to access the VM
All TCP	TCP	0-65535	Custom	sg-iPE	To allow traffic from members of sg-iPE
Oracle-RDS	TCP	1521	Custom	137.21.55.8/32	To access Oracle database from an external machine

Note - 137.21.55.8/32 is used as an illustration IP address, replace this with your own IP address.

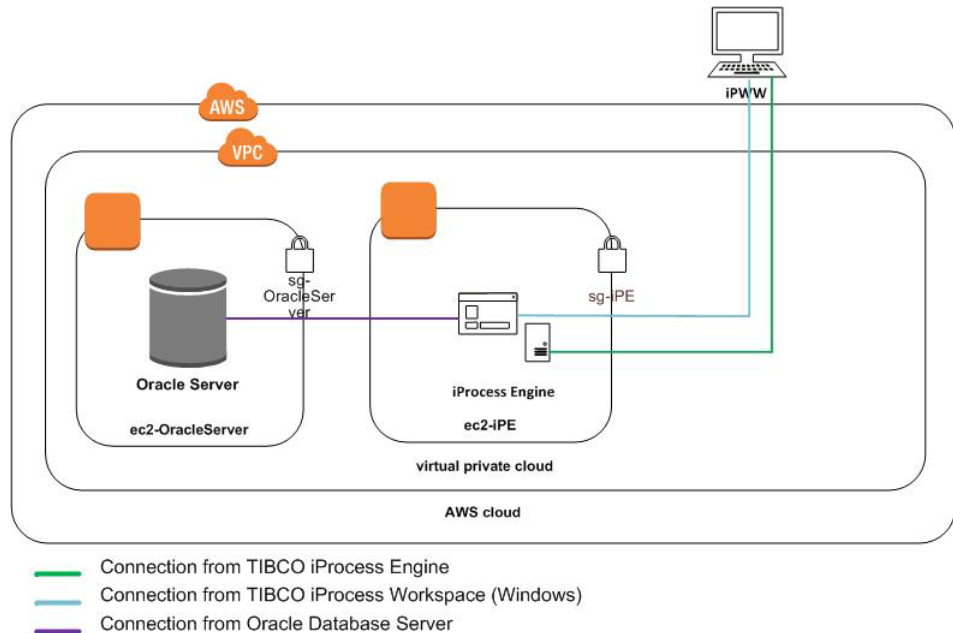
8. Configure sg-iPE (Refer to the below table):

- a. Specify a rule on ec2-iPE such that database server can communicate with the iProcess Engine.
- b. Specify a custom TCP rule (for example: 46000-46020) to restrict the number of inbound connections to ec2-iPE.
- c. Specify a custom TCP rule which would only allow client machines (on an external domain) to access the iProcess Engine on RPC port (the default is 111).

Type	Protocol	Port Range	Source		Purpose
Custom TCP Rule	TCP	22	Custom	137.21.55.8/32	SSH to access the VM
Custom TCP Rule	TCP	46000-46020	Custom	137.21.55.8/32	Port range used by iProcess Engine
All TCP	TCP	0-65535	Custom	sg-Oracle-Server	To allow traffic from members of sg-OracleServer
Custom TCP Rule	TCP	111	Custom	137.21.55.8/32	To access iProcess Engine

Note - 137.21.55.8/32 is used as an illustration IP address, replace this with your own IP address.

Once you configure these security groups, your setup will look something like the below illustration.



Example 3

If you plan to connect to iProcess Engine using iProcess[®] Workspace (Browser), perform the following steps to appropriately configure security groups.

1. Launch an EC2 instance in your VPC
2. Name the created instance **ec2-OracleServer**. Install the Oracle Database Server on this instance.
3. Launch a second EC2 instance in your VPC.
4. Name the created instance **ec2-iPETomcat**. Install iProcess Engine and iProcess Workspace (Browser) on this instance.
5. Create security groups for the two EC2 instances:
 - Create **sg-OracleServer** for instance **ec2-OracleServer**.
 - Create **sg-iPETomcat** for instance **ec2-iPETomcat**.

6. Configure sg-OracleServer (Refer to the below table):

- a. Specify a custom TCP rule which would only allow machines (on an external domain) to access the Oracle Database server (the default port is 1521).
- b. Specify a rule on ec2-OracleServer such that iProcess Engine can communicate with the database server.

Type	Protocol	Port Range	Source		Purpose
Custom TCP Rule	TCP	22	Custom	137.21.55.8/32	SSH to access the VM
All TCP	TCP	0-65535	Custom	sg-iPE	To allow traffic from members of sg-iPE
Oracle-RDS	TCP	1521	Custom	137.21.55.8/32	To access Oracle database from an external machine

Note - 137.21.55.8/32 is used as an illustration IP address, replace this with your own IP address.

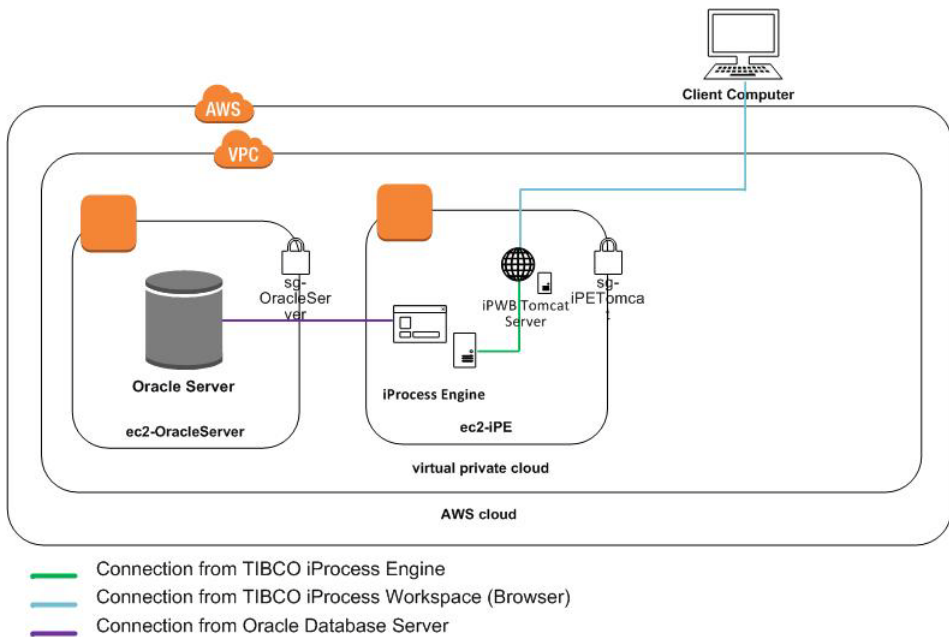
7. Configure sg-iPETomcat (Refer to the below table):

- a. Specify a rule on ec2-iPETomcat such that the database server can communicate with iProcess Engine.
- b. Specify a custom TCP rule which would only allow client machines (on an external domain) to access the iProcess Workspace (Browser) (the default port is 8080).

Type	Protocol	Port Range	Source		Purpose
Custom TCP Rule	TCP	22	Custom	137.21.55.8/32	SSH
All TCP	TCP	0-65535	Custom	sg-Oracle-Server	To allow traffic from members of sg-OracleServer
Custom TCP Rule	TCP	8080	Custom	137.21.55.8/32	Apaxe Tomcat Server - To connect to iProcess Workspace (Browser)

Note - 137.21.55.82/3 is used as an illustration IP address, replace this with your own IP address.

Once you configure these security groups, your setup will look something like the below illustration.



Chapter 4

Configuring TIBCO iProcess Technology Plug-ins

This section describes how to configure iProcess[®] Technology Plug-ins installed over iProcess Engine.

Topics

- [*Setting Parameters, page 18*](#)

Setting Parameters

For iProcess Technology Plug-ins to function correctly, you need to explicitly set the "java.rmi.server.hostname" property with the public IP of the AWS machine.

- **Linux/Unix:** Edit SWJVM_OPTIONS line in \$SWDIR/eajava/scripts/env.sh to append `-Djava.rmi.server.hostname=<iProcess Engine FQDN>`
- **Windows:** Edit SWJVM_OPTIONS environment variable to append `-Djava.rmi.server.hostname=<iProcess Engine FQDN>`

For example (on both Windows and Linux):

```
SWJVM_OPTIONS="-Dsun.lang.ClassLoader.allowArraySyntax=true  
-Djava.rmi.server.hostname=ec2-52-66-190-210.ap-south-1.compu  
te.amazonaws.com"
```

Appendix A **Appendix A - Related Documents**

This appendix lists documents that you could refer to in case you need more help.

Document Title	Link or Description
AWS Documentation	https://aws.amazon.com/documentation
Troubleshooting Connecting Instance	http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html