Plato Infrastructure Services Installation Guide

Release 14.4.0.0.0

Part No. F29963-01

March 2020

Plato Infrastructure Services Installation Guide

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/

Table of Contents

1. Preface

1.1 Introduction

This guide would help you to install the Plato infrastructure services on designated environment.
It is assumed that all the prior setup is already done related with WebLogic 12c installation, WebLogic managed server creation and Oracle DB installation.
It is recommended to use dedicated managed server for each of the Plato infrastructure services.

1.2 Audience

This document is intended for WebLogic admin or ops-web team who are responsible for installing the OFSS banking products.

1.3 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1.4 Organization

This installation user guide would allow you to install following services in same order

- WebLogic system environment settings
- Plato Discovery Service
- Plato Config Service
- Plato API Gateway Service
- Plato UI Config Service
- Plato O
- Plato Orch Service
- Security configuration and tool installation

1.5 Related Documents

- Common Core Services Installation Guide
- Day 0 Setup Guide
- LDAP Setup Guide
- ANNEXURE-1
- Oracle Banking Credit Facilities Process Management Pre-Installation Guide
- Oracle Banking Credit Facilities Process Management Services Installation Guide
- Oracle Banking Credit Facilities Process Management User Interface Installation Guide
- Oracle Banking Credit Facilities Process Management Conductor Process Installation Guide
- Security Management System Services Installation Guide
- SSL Setup Guide

2. Database Setup

2.1 Introduction

In this section you are going to setup database related configuration for PLATO Installation. Before you proceed ensure pre-installation setup is done.

2.2 Pre-requisite

Before you proceed with the document, ensure Schema’s are being created. It is recommended to have different schema for **Plato** and **Plato Security**. To configure Plato security refer Security Configuration chapter.
To know server’s port no refer ANNEXURE-1. “**How to check port no”** section.

Ensure to configure Placeholder parameters in Weblogic server for Plato Config service, SetDomain.Env. To know more, refer ANNEXURE-1. “**Place Holder update for Plato-Config-Services”** section.

3. Domain and Cluster Configuration

3.1 Plato Infrastructure Domain Configuration

3.1.1 Prerequisites

- Machine should have Java JDK1.8.0_241 has installed.
- Oracle Fusion Middleware 12cR2 12.2.1.4 has to be installed on the machine.

3.1.2 Domain Creation and Configuration

It is recommended to have different managed server in one domain for each application. For Creating Domain and Configuration please refer to ANNEXURE-1 “**How to create and Cluster Configuration”.**

4. Data Sources Creation

4.1 Prerequisite

Before you proceed with Data source creation Please make sure Domain and cluster configuration steps completed.

4.2 Data sources List

The table below lists the data sources to be created on each managed server prior to deployment of applications onto managed servers.

Data source Name	Data source JNDI	Targets
PLATO	jdbc/PLATO	Config Server, API Gateway Server
PLATOSEC	jdbc/PLATO_SECURITY	
PLATO_UI	jdbc/PLATO_UI_CONFIG	Plato UI Config Server
CONDUCTOR	jdbc/PLATO-O	Plato-O, Plato Orch Server

For creating data source in please refer ANNEXURE-1 “**How to create Data sources section”.**

5. Deployments

5.1 Pre-requisite

Before you proceed with below, please make sure previous steps are completed.

5.2 Deployments List

Below table give details of the deployments required on each Server for the Plato application to run. Deploy one after other in the same given order.

Application	Archive name	OSDC path	Targets
plato-discovery-service	plato-discovery-service-5.0.0.war	{**unzip the file**}Plato\plato-discovery-service\App	Discovery Server
plato-config-service	plato-config-service-5.0.0.war	{**unzip the file**}Plato\plato-config-service\App	Config Server
Plato-api-gateway	plato-api-gateway-5.0.0.war	{**unzip the file**}Plato\plato-api-gateway \App\	Api Gateway
Plato-ui-config-service	Plato-ui-config-service-5.0.0.war	{**unzip the file**}Plato\plato-api-gateway \App\	Plato UI Config
Plato-O	conductor-server-v2.24.2.war	{**unzip the file**}Plato\plato-api-gateway \App\	Plato-O
Plato-Orch-Service	Plato-Orch-Service-5.0.0.war	{**unzip the file**}Plato\plato-api-gateway \App\	Plato-Orch-Service

5.3 Steps to Deploy as Application

To deploy application please refer ANNEXURE-1. "**How to deploy section**".
[Note: After deploying "plato-discovery-service" it is recommended not to restart and refresh the server.]

6. Restarts and Refresh

Once everything is deployed, the managed servers. And for each application call path “/refresh” for refreshing the configuration properties.

6.1 Restarting Servers

To restart the server please refer to ANNEXURE-1.”**How to restart**” section.

7. Security Configuration and Tools Installation

7.1 Pre-requisite

Before you proceed with below, please make sure LDAP server details is provided to you- Like LDAP_URL, USER_STORE, LDAP_SERVER_CREDENTIAL_SALT, LDAP_SERVER_USER, LDAP_SERVER_BASE, LDAP_SERVER_CREDENTIAL, LDAP_USER_SEARCH_BASE, LDAP_USER_PREFIX, CORS_ALLOWED_ORGINS, LDAP_SERVER_CREDENTIAL_SALT etc.

7.1.1 Plato Security JWT

Plato security module enables securing API micro services with JWT (JSON Web Tokens). JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties. JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed.

7.1.2 Plato Security Configuration

Plato recommend to create new schema for security to keep the security related database objects at one place. If the environment is configured for multi-tenant, we require a security schema per tenant.
All the Plato security configurations are maintained at SECURITY_CONFIG table
Steps to configure in the table:

1. Change the below KEY with provided LDAP details

LDAP_SERVER_CREDENTIAL_SALT	Enter LDAP server Credential salt e.g. 0.9482628451234567
CORS_ALLOWED_ORGINS	valid host names (comma delimited)
LDAP_URL	Enter LDAP Server URL Example: ldap://localhost:12345
LDAP_SERVER_USER	Enter LDAP Server USERID Example: uid=admin
LDAP_SERVER_BASE	Enter LDAP server BASE Example: dc=oracle,dc=com
LDAP_SERVER_CREDENTIAL	Enter LDAP server encripted password using provided jwr algorithm Example: m0o/F3UvlwvBSv5C/TSckA== (use plato encryption utlity to generate encrypted password)
LDAP_USER_SEARCH_BASE	Enter LDAP User search Base Example: ou=people
LDAP_USER_PREFIX	Enter LDAP User Prefix Example: uid

7.1.3 User Store

Plato supports following user stores for authentication
Users Maintained at table.

1. Plato security can authenticate the users maintained at table (APP_USER) in the security schema. However we do not recommend to use this option.
2. LDAP user store.
3. Plato security can integrate with LDAP server to authenticate the users.
4. For production deployment, the LDAP server should be an industry standard production grade server.

8. Zipkin Server Setup

8.1 Introduction

In this section you are going to install recommended Zipkin server for tracing and monitoring the micro services calls

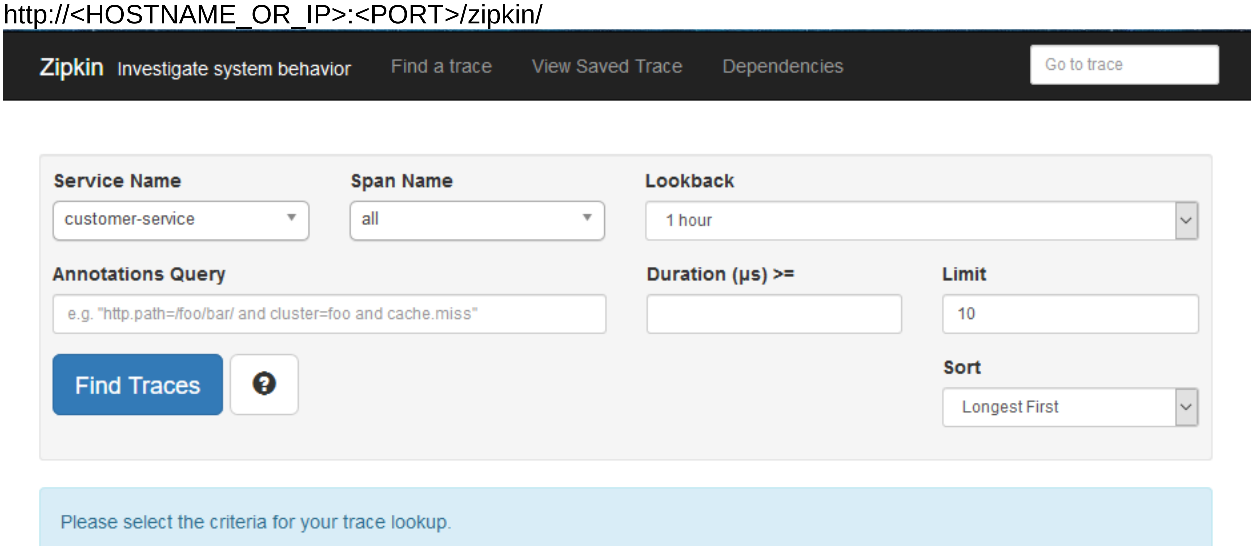
8.1.1 Download the Artifact

Before proceeding with the below steps ensure Plato database setup section completed.
Zipkin Server 2.6.0 should be downloaded and store in local file system to execute on host machine.
Zipkin Server 2.6.0 JAR location: https://zipkin.io/pages/quickstart

Running the Zipkin Server
Zipkin server could be run by using the following syntax.
java -jar <location of zipkin-server-2.6.0-exec.jar> &
Here, & is added to execute it in background mode. On Windows, you can ignore it.
Zipkin runs on default port 9411.

8.1.2 Accessing the Zipkin Server

You can access the zipkin server by hitting the following URL
http://<HOSTNAME_OR_IP>:<PORT>/zipkin/



9. Logging Area

9.1 Introduction

This part of the document will talk about the logs area where after deployment of Plato Applications in WebLogic server.

9.1.1 Logging Area:-

Plato Application writes logs in the below area of the server-
<WEBLOGIC_DOMAIN_CONFIG_AREA>/ logs/plato-api-gateway.log
Let’s assume a domain has been created **platoinfra_domain** in the following area of the server “/scratch/oracle/middleware/user_projects/domains/platoinfra_domain”. Logging area for Plato would be **/scratch/oracle/middleware/user_projects/domains/platoinfra_domain/logs.**