Technical Overview, Server Requirements and Technical Flowcharts

Transaction Auditing, Activity Monitor, Segregation of Duties, Security Auditing, Security Reporting and Security Modeling for Lawson S3 and Infor CloudSuite

Author: Mike Nitka

2024

Kinsey Application Server Overview 3
WebSphere Application Flowchart – Lawson S3 4
Transaction Processing Flowchart – Lawson S3 5
Application Storage Flowchart – Lawson S3 6
Application Process Flowchart – CloudSuite (Landmark) 7
Transaction Processing Flowchart – CloudSuite (Landmark) 8
Hardware & Software Requirements (Lawson S3 and CloudSuite) 9
Kinsey Application Server (minimum requirements) 9
Server Operating System Options 9
Server Software (to be installed by Kinsey) 9
Lawson LDAP Configuration (Lawson S3 only) 9
Installed Web Sphere Components (Lawson S3 only) 10
Enterprise Applications 10
Service Bus 10
JMS Connection Factory 10
JMS Queues 10
JMS Activation Specification 10
Shared Library 10
Application Software and Connection Requirements 11
Connecting to the Kinsey VM 11
Lawson S3 Connection Requirements 11
Ports required to be open 11
Lawson & System Users Required (for all Lawson systems to be connected to Kinsey applications) 11
CloudSuite (Landmark) Connection Requirements 11
Option 1: INFOR Landmark non-expiring user account with minimum roles of: 11
Option 2: INFOR Service account with minimum roles of: 12
Troubleshooting (Lawson S3 Only) 13
Potential Lawson Problems 13
Kinsey Application Server Monitoring 14

Kinsey Application Server Overview

Kinsey recommends the installation of a virtual server, either Windows or Linux, for hosting the Kinsey applications; Tomcat, Java and either a MySQL or MariaDB database. This server will reside entirely within the constraints of the client network either on-prem or in the cloud. No client data will ever be stored on a server controlled by Kinsey and access to the Kinsey application server will be controlled by the client. The database contains 3 types of tables; system parameters, Landmark and/or Lawson metadata and client data. Certain system parameters are required for all Kinsey's applications that collect or send transactions from the INFOR CloudSuite and/or Lawson server to the Kinsey application server.

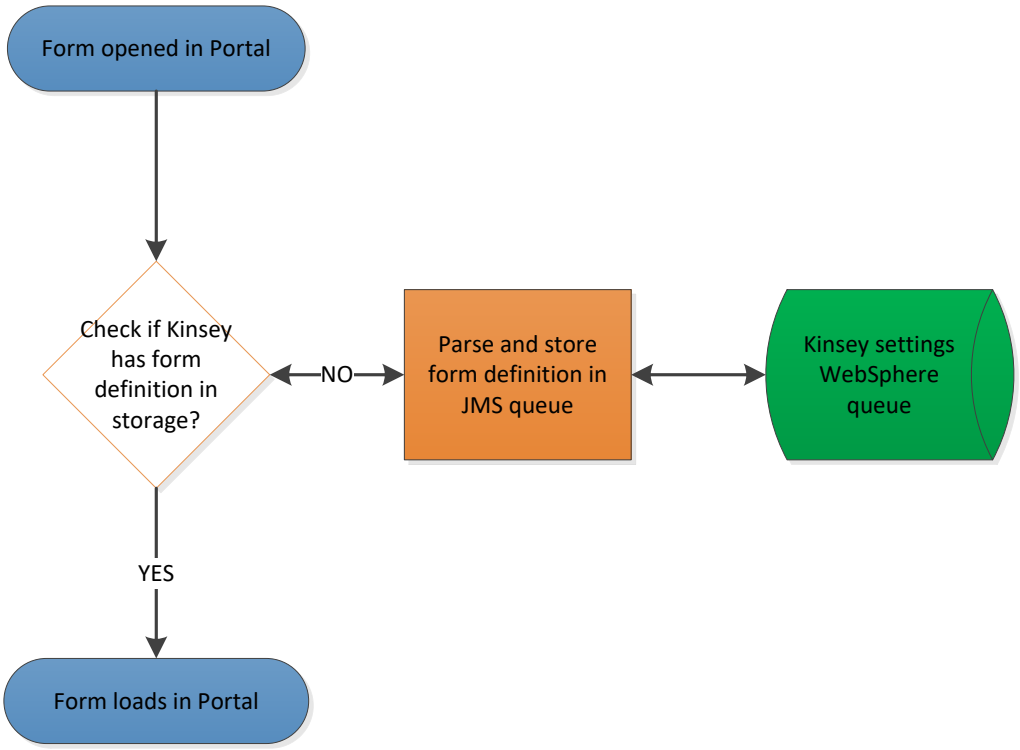
The metadata is used strictly for Kinsey reports. This includes information regarding Business Class (CloudSuite) and Token (Lawson S3) names, Business Class actions and Lawson S3 function code descriptions. This data is collected on the initial installation of the application and can be refreshed manually when INFO/Lawson applications are updated. Instructions on updating the metadata tables can be found in the Administration Guide.

Depending on the applications purchased the client data can consist of anything from transaction level data to security settings. Security data is collected via a scheduled process that generally runs every night. You can also run the processes manually as needed. Instructions on updating the client tables can be found in the Administration Guide. This application will never collect or store user passwords.

Transaction Auditing and Activity Monitor data are collected real time for the S3 application and on short intervals for CloudSuite (Landmark). There are no scheduled task required for collection transaction data.

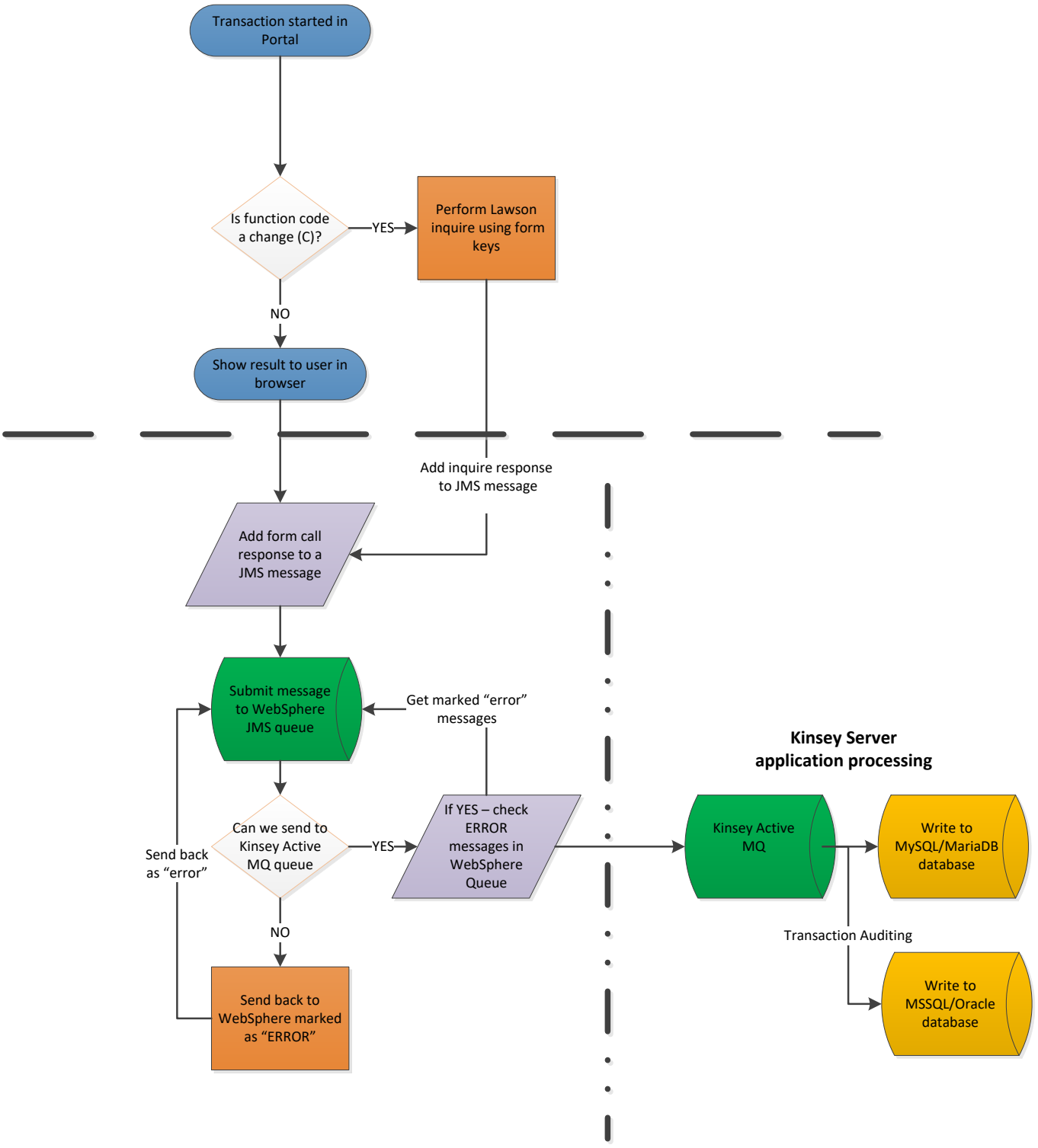
WebSphere Application Flowchart – Lawson S3

**Related to Transaction Auditing and Activity Monitoring only*

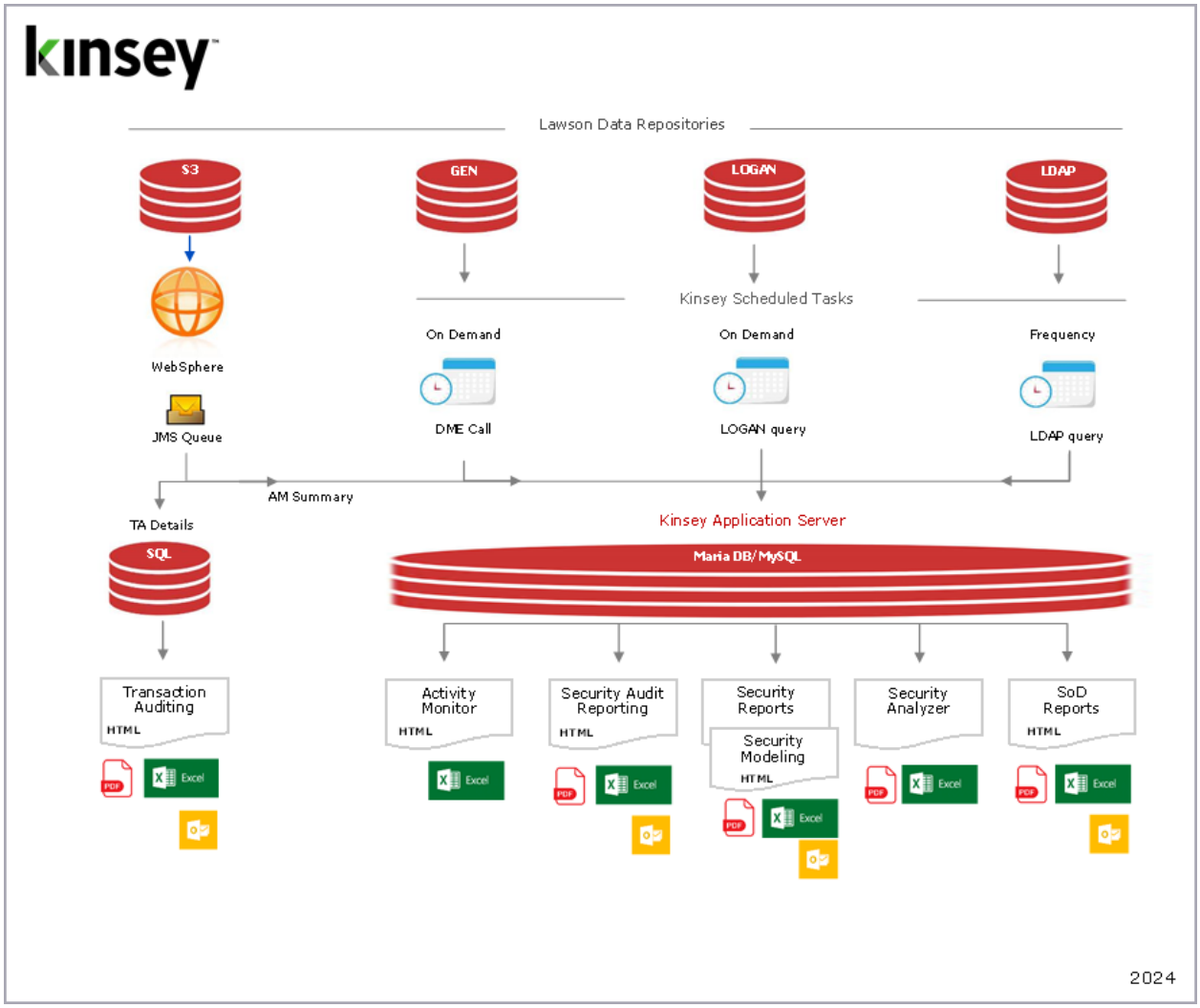


Transaction Processing Flowchart – Lawson S3

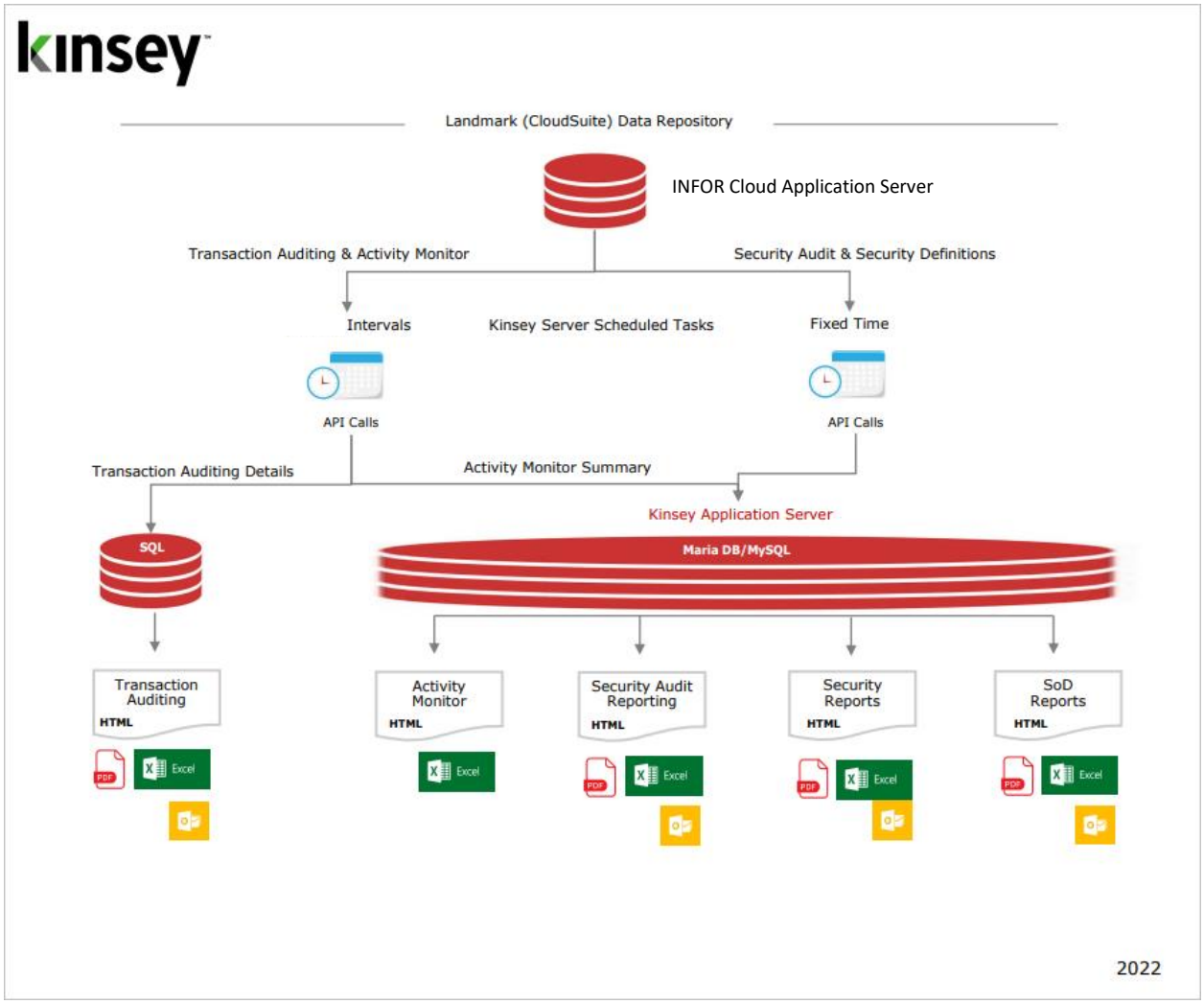
**Related to Transaction Auditing and Activity Monitoring for Lawson S3 only*



Application Storage Flowchart – Lawson S3

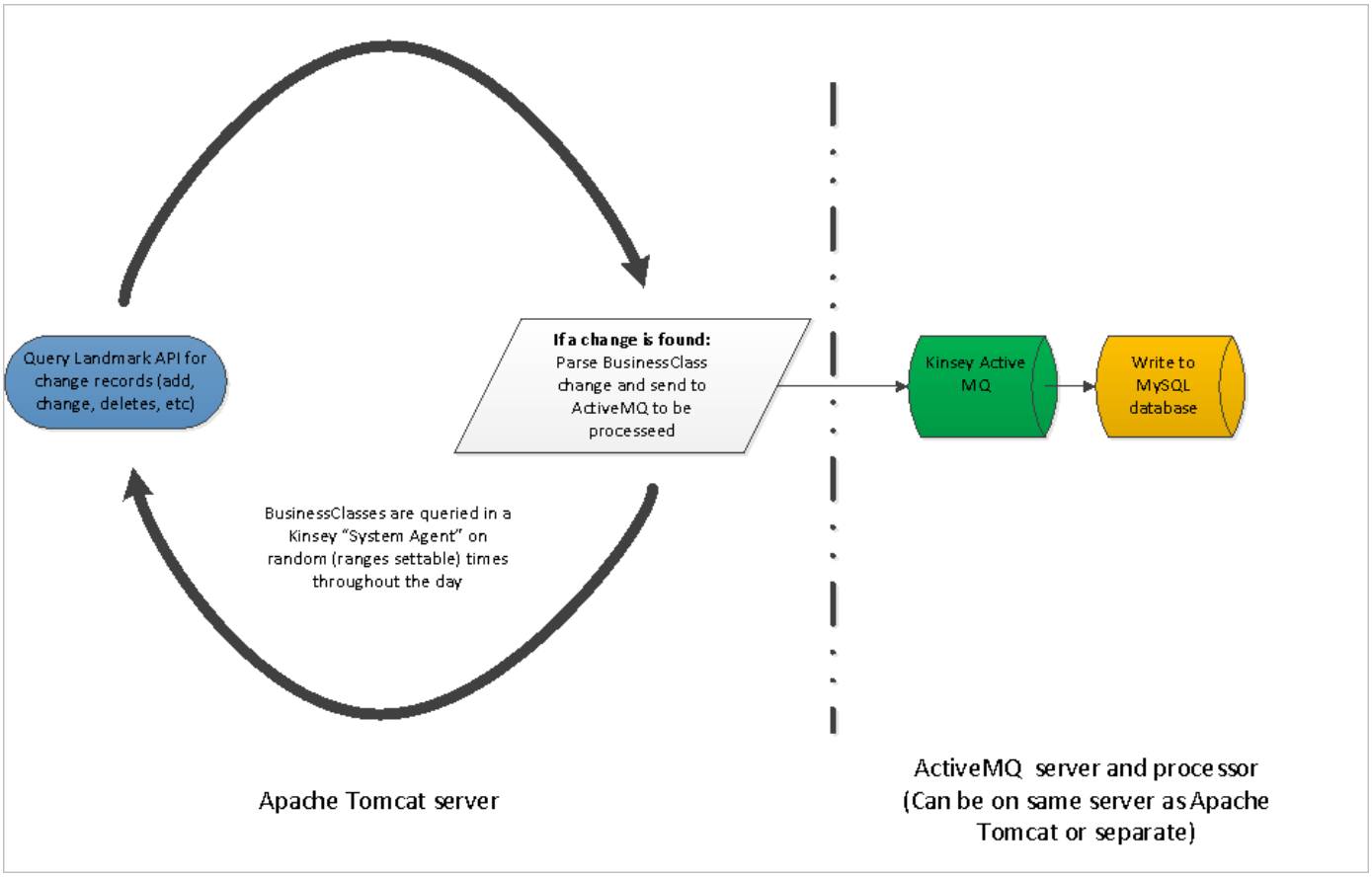


Application Process Flowchart – CloudSuite (Landmark)



Transaction Processing Flowchart – CloudSuite (Landmark)

**Related to Transaction Auditing and Activity Monitoring for Landmark only*



Hardware & Software Requirements (Lawson S3 and CloudSuite)

Kinsey Application Server (minimum requirements)

- 4 Core CPU
- 12 GB RAM (16 GB Optimal)
- 50 GB free Hard Drive space (not including OS)
    - Activity Monitor and Transaction Auditing may require modified sizing requirements

Server Operating System Options

- Windows 2012 through current release
- Linux (kernel version 4.x or above)

Server Software (to be installed by Kinsey)

- MariaDB (v 10.5+)
- Apache Tomcat (v 10.x)
- OpenJDK (v 17+)
- Active MQ Artemis

Lawson LDAP Configuration (Lawson S3 only)

If LDAP Paging is **not** used by Lawson, then the LDAP server *MaxPageSize* may need to be adjusted.

This setting is different – depending on the Lawson LDAP server flavor:

- For Microsoft ADAM LDAP Servers
    - MaxPageSize - http://support.microsoft.com/kb/315071
- For Tivoli LDAP Server
    - SetMaxSize - http://www-01.ibm.com/support/docview.wss?uid=swg21285866

The **MaxPageSize** size limit should be set to:
Unlimited **or** *(Lawson user count) x (Lawson possible identity count) x 1.5*

For example: (500 Lawson users) x (5 possible identities) x 1.5 = 3750 is the **MaxPageSize** number to use.

Installed Web Sphere Components (Lawson S3 only)

**Related to Transaction Auditing and Activity Monitoring only*

Access to Web Sphere admin console

Enterprise Applications

- KKFilter
- KKFilterConfiguration

Service Bus

- KKFilterBus

JMS Connection Factory

- KKQConnectionFactory

JMS Queues

- KKQueue
- KKSettings

JMS Activation Specification

- KKJMSActivationSpec

Shared Library

- KKSharedLib

Application Software and Connection Requirements

Connecting to the Kinsey VM

Kinsey requires Remote desktop access with an account that has administrator privileges on the server.

(i.e. VPN, Secure Link, Citrix)

Lawson S3 Connection Requirements

Ports required to be open

From Kinsey server to Lawson environment –

1. Lawson Portal port (port examples: 80, 443)
2. Lawson LDAP port (port examples: 389, 40000)

From Lawson environment to Kinsey – (applies on to AM or TA)

1. Port – 61617 (Active MQ JMS Server)

Lawson & System Users Required (for all Lawson systems to be connected to Kinsey applications)

Lawson Portal non-expiring service account with access to:

1. All *GEN* product line tables (required only during installation)
2. All token (form) access in application product lines (minimum access "Inquire only" to all tokens – required only during installation)
3. File access to *LSAUDIT* table in *LOGAN* product line (ongoing access)
4. File access to *EMPLOYEE* table in primary application product line (ongoing access)

Lawson LDAP service account with access to:

1. Read entire LDAP tree structure that Lawson security is stored in (minimum access is "Read-Only")

NOTE: This is not a Lawson Security account, but rather a LDAP structure browser user similar to what you would use to connect with jxplorer or in Lawson's install.cfg.

CloudSuite (Landmark) Connection Requirements

User requirement (for all Landmark systems to be connected to Kinsey applications)

Option 1: INFOR Landmark non-expiring user account with minimum roles of:

- IEFINBaseSystemAndDataAccessViewOnly_ST
- Admin_ST
- ApplicationAdministrator_ST
- GHRUSers
- Infor-SuiteUser
- SecurityAdministrator_ST
- IFSApplicationAdmin

Option 2: INFOR Service account with minimum roles of:

- IEFINBaseSystemAndDataAccessViewOnly_ST
- Admin_ST
- ApplicationAdministrator_ST
- GHRUSers
- Infor-SuiteUser
- SecurityAdministrator_ST
- IFSApplicationAdmin

And the information found in the service account file from INFOR: (or simply provide the file)

- AK - Access Key
- SK - Secret Key
- CI - Client ID
- CS - Client Secret
- PU – Access Token URL
- OT – URL Get Token

Troubleshooting (Lawson S3 Only)

Potential Lawson Problems

Portal screens aren't responding. (Lawson S3 only)

Applies to: Transaction Auditing, Activity Monitor(Listener)

It's critical that the Kinsey application server is fully operational prior to starting Lawson. More specifically, Tomcat and MySQL/MariaDB must be running on the Kinsey application server. Kinsey's WebSphere application will try to connect to the Kinsey application server and retrieve configuration settings stored in the Kinsey SQL tables. If a connection cannot be made, Lawson's Portal application will not respond correctly.

Note: The Kinsey application server can be restarted anytime without stopping Lawson. When the Kinsey application server is offline you will not be able to collect data from the Lawson server for reporting purposes, but it will not impact Lawson. See the "WebSphere Hangs" section below for exception to this note.

Corrective Steps

Restart Lawson after each step until Lawson Portal is responding

1. Make sure the Kinsey application server is running, if not start the server and validate that you can access the Kinsey portal page.
2. Restart the SQL database (i.e. MySQL/MariaDB) and Tomcat on the Kinsey application server in that sequence and validate that you can access the Kinsey portal page.
3. If Lawson still won't start then reboot the Kinsey application server and validate that you can access the Kinsey portal page.
4. If Lawson still won't start then deactivate Activity Monitor (Listener). (refer to the installation guide for more information)

If Activity Monitor (Listener) needs to be deactivated please schedule time with Kinsey to evaluate the condition of the Kinsey application server prior to reactivating the application. Possible problems include hardware failure, network configuration changes (i.e. Lawson or application server IP address changes), database (i.e. MySQL/MariaDB) corruption, potentially full hard drive or a JAVA update may have changed the settings.

WebSphere hangs (Lawson S3 only)

Applies to: Transaction Auditing, Activity Monitor (Listener)

The Kinsey application uses the JMS queues to collect and send data to the Kinsey application server. If the Kinsey server is unable to received messages for any reason the JMS queues will hold the transactions until the Kinsey server is back online. This is similar to an email message being stuck in the outbox. If the Kinsey server is left off-line for an extended period of time the JMS queues can fill up and potentially fill up the hard drive where the WebSphere system logs are kept. By default the WebSphere JMS queues will store 500MB of data per node.

Kinsey does not change this setting. For instance, if you have 5 nodes on your system you need to make sure you have at least 2.5GB of available hard drive space on the same drive where the WebSphere logs are kept.

Provided you have sufficient room on the drive and the 500MB limit is reached the JMS queue will stop accepting new messages (AM and TA data). This will not cause the system to crash but these transactions will not be collected by the Kinsey application. Once the Kinsey application server is back online any transactions still in the queue will be sent to the Kinsey server.

Corrective Steps:

1. Validate that you have enough room on your log drive to hold 500MB x # of nodes.
2. Manually purge the JMS queue and restart WebSphere

Kinsey Application Server Monitoring

This is a list of items that should be monitored on the Kinsey Windows server:

PORT CHECK:

MySQL/MariaDB – Port 3306

Should return something similar to:

J5.6.20t>♥%h`*K{M ☻ Ç§#_75D6"FwG=<mysql_native_password

TOMCAT – Port 80

PING:

Kinsey Server (for network connection check)

For Linux Installations Only

SERVICE CHECK (if possible):

MySQL - (service mysqld status) OR (ps -ef | grep mysql)

TOMCAT - (ps -ef | grep tomcat)