



Technical Overview, Appliance Requirements and Technical Flowcharts

**Transaction Auditing, Activity Monitor,
Segregation of Duties, Security Auditing and
Security Reporting**

Author: Mike Nitka

A large, abstract graphic at the bottom of the page consists of several overlapping, semi-transparent geometric shapes in shades of green and grey, creating a layered, architectural effect.

2018

Contents

Kinsey Application Server Overview3
 Virtual Server System Settings3
Kinsey Application Server Installation4
Lawson Portal Listener/Auditor Overview.....5
Kinsey Application Flowchart.....6
Hardware Requirements.....7
 Kinsey Application Server (VMware or Hyper-V)7
 Server Operating System Options7
 Server Software (to be installed by Kinsey).....7
Application Software and Connection Requirements8
 Supported Software Versions.....8
 Connection Requirements.....8
 Lawson & System Users Required8
 Server Information9
 Installation steps for Kinsey WebSphere 7.0 application10
Troubleshooting.....11
 Potential Lawson Problems11
 Kinsey Application Server Monitoring.....12

Kinsey Application Server Overview

Kinsey recommends the installation of a virtual server to host the Kinsey applications, Tomcat, Java and either a MySQL or MariaDB database. The database contains 3 types of tables; system parameters, Lawson metadata and client data. The system parameters are required for Kinsey's WebSphere application. The WebSphere application will send transactions from the Lawson server to the Kinsey application server. This is only the case for customers running Transaction Auditing or Activity Monitor (Listener).

The Lawson metadata is used strictly for Kinsey reports. This includes information about form names and function code descriptions. This data is collected on the initial installation of the application and can be refreshed manually when 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 LDAP security settings. However, unless you are running Kinsey's Transaction Auditing application Lawson application data will never be collected. Security (LDAP) 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.

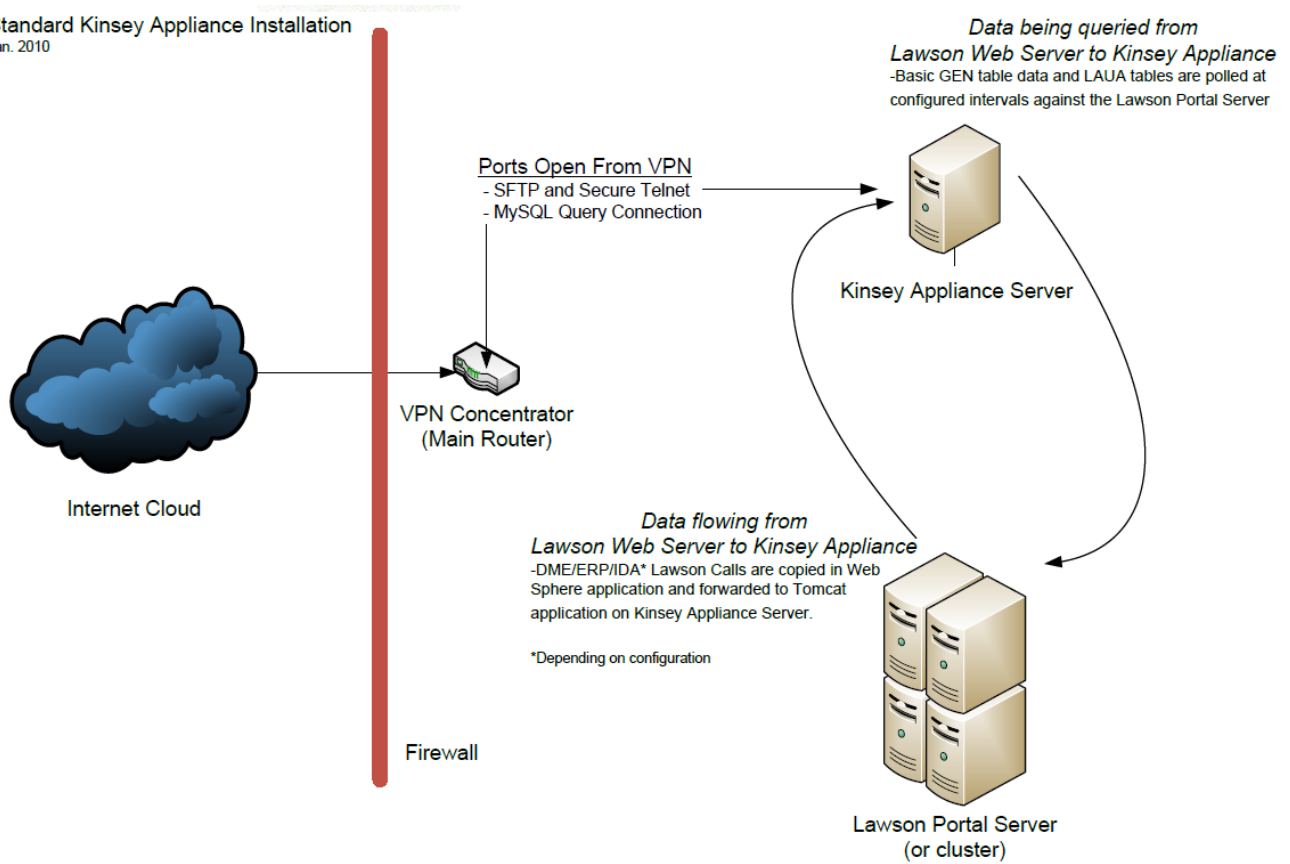
Transaction Auditing and Activity Monitor (Listener) data are collected real time. There is not a scheduled task for these processes.

Virtual Server System Settings

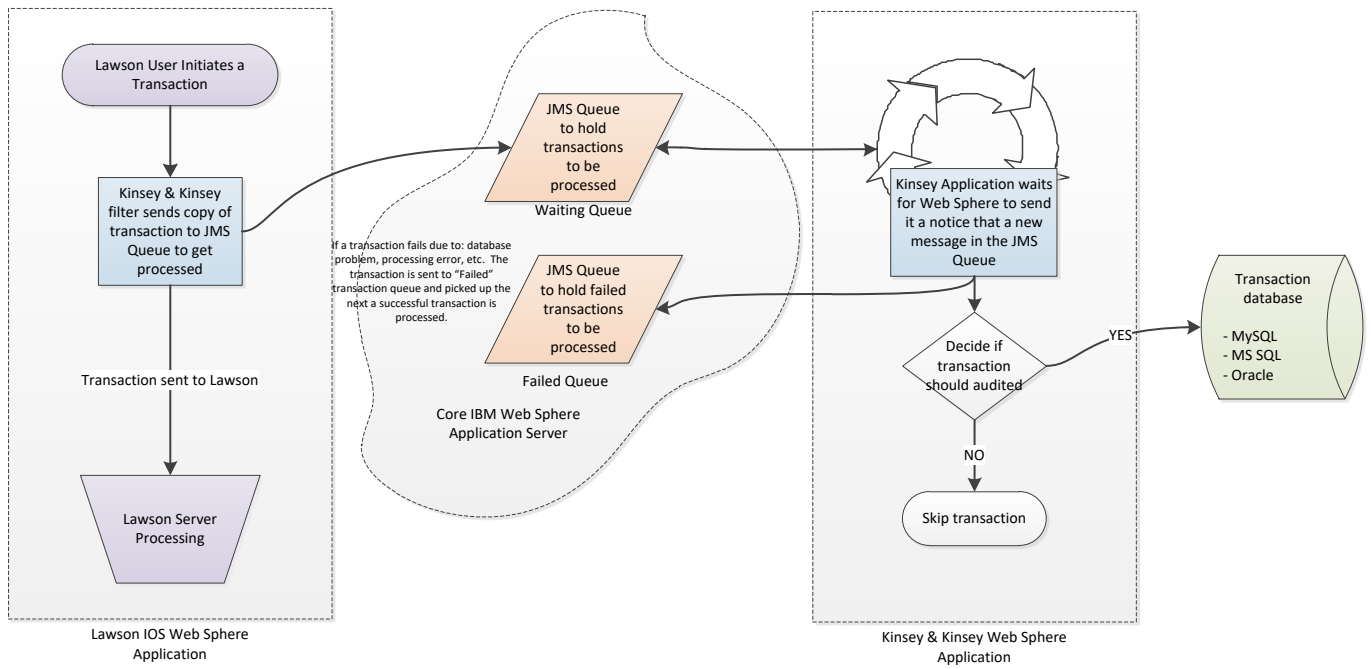
1. Kinsey Application Server Memory (8 GB min)
 - This is a minimum requirement and can vary greatly depending on the OS and the size of the customers' security model. We will always recommend more memory for a Windows server than for a Linux server.
2. If LDAP Paging is used by Lawson
 - ADAM and Tivoli page sizes are based on how Lawson is set. Kinsey does not make a change to these settings.
3. If LDAP Paging **is not** used by Lawson
 - If using Tivoli then the maximum records has to be set to (Users x Identities available).

Kinsey Application Server Installation

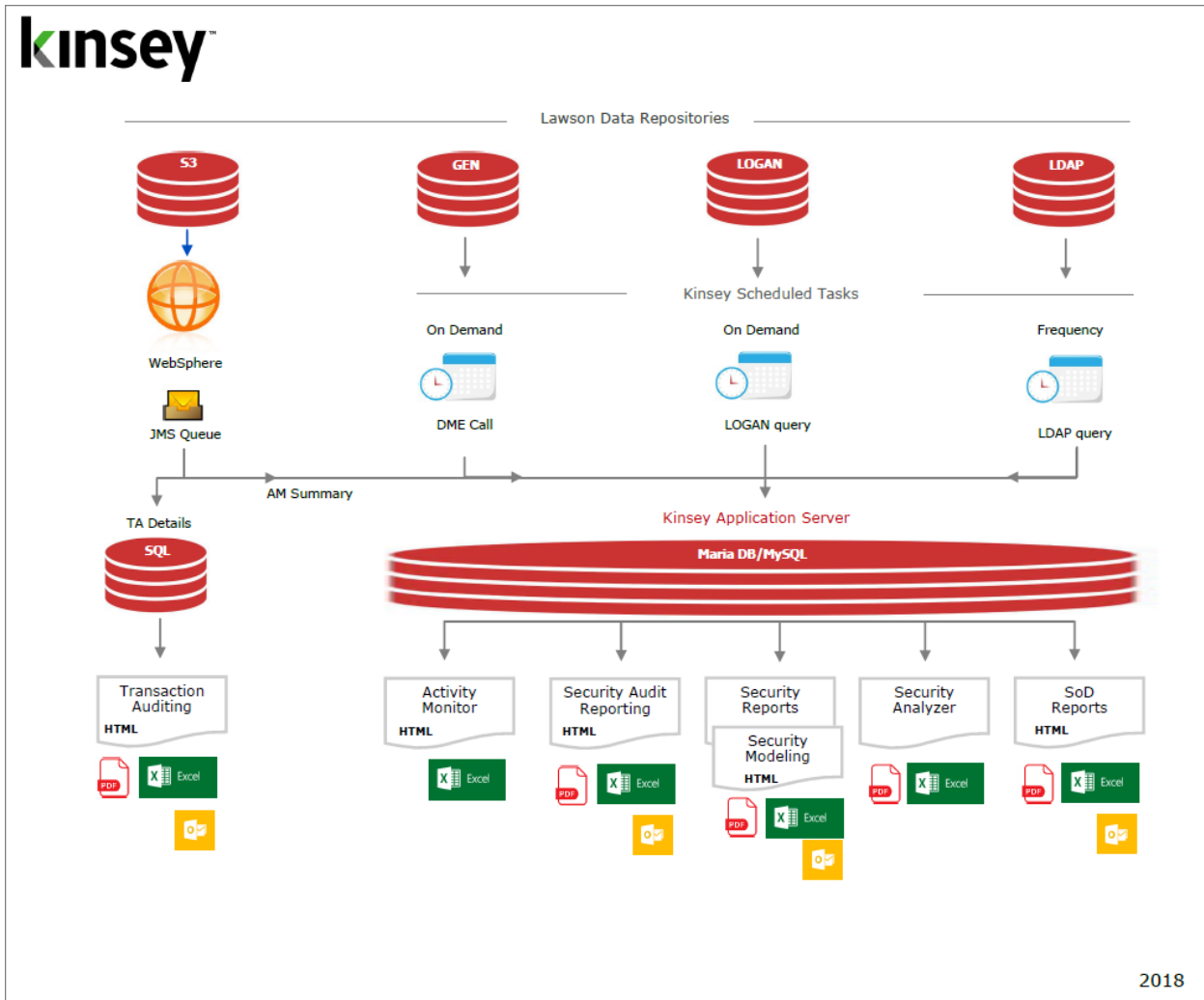
Standard Kinsey Appliance Installation
Jan. 2010



Lawson Portal Listener/Auditor Overview



Application Flowchart



Hardware Requirements

Kinsey Application Server (VMware or Hyper-V)

- Dual Core allocation (64bit hardware)
- Quad Core allocation (64bit hardware for Windows 2012 or 2012R2)
- 8 GB RAM
- 50 GB Hard Drive (variable depending operating system, applications and retention policies)
- Single Ethernet

Server Operating System Options

Linux Servers

- Cent OS - Version 7.0 (Community Enterprise RedHat v7.0)
- Similar version of Linux

Microsoft Windows Servers

- 2000/2003/2008/2008R2/2012/2012R2

For Windows 2012R2 see hardware requirements above

Server Software (to be installed by Kinsey)

- MariaDB
- Tomcat
- Java

Note: MySQL Enterprise version 5.7 is also a supported database

Application Software and Connection Requirements

Supported Software Versions

Supported Applications	MS Excel 2003	MS Excel 2007-2016	Adobe	MS IE (Minimum Version)	Chrome
LS Reporting	Yes	Yes	Yes	9.x	29.0
LS Analyzer	No	Yes	Yes	9.x	29.0
LS Auditing	Yes	Yes	Yes	9.x	29.0
LS Modeling	Yes	Yes	Yes	9.x	29.0
LS Segregation of Duties	Yes	Yes	NA	9.x	29.0
Activity Monitor (Listener)	Yes	Yes	Yes	9.x	29.0
Transaction Auditing	Yes	Yes	Yes	9.x	29.0
Landmark Security Reporting	Yes	Yes	Yes	9.x	29.0

Connection Requirements

- Kinsey Server must be able to connect Lawson Server via HTTP(S) (using DME calls)
- Lawson server must be able to connect to Kinsey Application Server via HTTP(S) for Activity Monitor and Transaction Auditing.

Minimum VPN Connection Requirements (Linux Installations only)

- Port 80 (web) and 3306 (MySQL/MariaDB) opened on the VPN tunnel if a VPN connection is allowed.

Lawson & System Users Required

- Lawson Portal User/Password (for both DEV/TEST and PRODUCTION servers)
This user ID is used to pull data from GEN tables for Kinsey reporting.
 - This user needs the same security class that is assigned to the default 'Lawson' user account. This included access rights to GEN databases, all product lines, all forms and all tables.
 - The user must also have the "Security Officer" role in user profile of LAUA

The user should be able to do the following

- Access the GEN database. For example:
http[s]://[LAWSON SERVER]/cgi-lawson/dme.exe?PROD=GEN&FILE=SECCLASS
- Perform formdef.exe calls. For example:
http[s]://[LAWSON SERVER]/cgi-lawson/formdef.exe?_PDL=[PDL]&_TKN=CU01.1&_OUT=XML
- LS LDAP Server 'Read-only' User/Password (for TEST and PRODUCTION server)

“Read-only” is a minimum requirement; the user ID can be full access. This ID is used to pull data from LDAP for Kinsey security reporting and segregation of duties.

- This is not an LS Lawson user, but rather a LDAP structure browser user similar to what you would use to connect with jxplorer or in Lawson’s install.cfg.
- **Note that the user ID and password are entered and stored in clear text in the application configuration file.** This user is only required for LS Security Reporting, LS Security Auditing and Segregation of Duties reporting.

Server Information

- Kinsey Server
 - Name:
 - Remote Desktop User:
 - Remote Desktop Password:

Most of this info will be in the Lawson the install.cfg

- Lawson Portal
 - URL
 - User: (may be Lawson, see above)
 - Password:
- LDAP
 - Server Name:
 - Port:
 - User DN: (this should preferably be read-only, see above)
 - Password
- WebSphere Console URL

Installation steps for Kinsey WebSphere 7.0 application

Note: Applies to Security Migration, Transaction Auditing and Activity Monitor projects.

To be completed after Kinsey applications have been installed on the Virtual Server

1. Install Kinsey app on Lawson app (WebSphere) server in the Test/Dev environment
2. Restart WebSphere – if applicable (some versions of WebSphere do not require a restart)

Result: This will activate JMS Queues on Lawson application server for Test/Dev

3. Modify the WEB.XML file (for Lawson Test server)
4. Restart Lawson IOS (Test/Dev server only)

Result: Kinsey 'Listener' is now active in TEST/DEV. This will cause a slight interruption in Lawson services and should be done after hours whenever possible)

5. Install Kinsey app on Lawson app (WebSphere) server in the Production environment.
6. Restart Web Sphere – if applicable (some versions of WebSphere do not require a restart)

Result: This will activate JMS Queues on Lawson app server for Production

7. Modify the WEB.XML (for Lawson Production server)
8. Restart Lawson IOS (Production server only)

Result: Kinsey 'Listener' is now active in Production. This will cause a slight interruption in Lawson services and should be done after hours whenever possible)

Troubleshooting

Potential Lawson Problems

Portal screens aren't responding.

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 MySQL/MariaDB. 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 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 Listener (refer to page xx of installation guide)

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), MySQL/MariaDB corruption, hard drive is full or JAVA update has changed the settings.

WebSphere hangs

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 (listener data). This will not cause the system to crash but these transactions will be lost. Once the Kinsey application server is back online all of the messages (transactions) 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. In Mercy's case that would be 2.5GB.
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 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)