Technical Overview, Appliance Requirements and Technical Flowcharts

Transaction Auditing, Activity Monitor (Listener), Segregation of Duties and Security Reporting

Author: Mike Nitka

Contents

Appliance Overview

Kinsey recommends the installation of a virtual server (appliance) to host the Kinsey applications, Tomcat, Java and a MySQL database. The MySQL database contains 3 types of tables; system parameters, Lawson metadata and client data. The system parameters are required for Kinsey's WebSphere application. That application will send transactions from the Lawson server to the appliance. This is only the case for customers running Transaction Auditing, Activity Monitor or Listener. All security migration projects will run the listener for a period of time, so if your company has engaged Kinsey for security work then the Listener is probably running.

The Lawson metadata is used strictly for Kinsey reports. This includes information like form 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 is collected real time. There is not a scheduled task for these processes.

Virtual Server System Settings

1. JVM Memory (relates to LAUA Reporting and SOD Reporting only)

    - This setting depends on how much memory has been allocated to the virtual server and whether the server is running Windows or Linux. For a Windows OS JVM cannot be set to use more than ½ the memory available, for Linux its variable. We base the setting on the number of LAUA classes defined. Generally 1.5GB will handle up to 100 LAUA Security Classes. However, this parameter can be a moving target depending on the OS and the amount of total memory allocated to the virtual appliance. If we over allocate JVM memory we run the risk of stealing resources from the server, however if we under allocate memory the LAUA reporting applications could hang the appliance. Proper system settings can only be obtained by running test setting in a test environment.

2. Appliance Memory (8 MB 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.

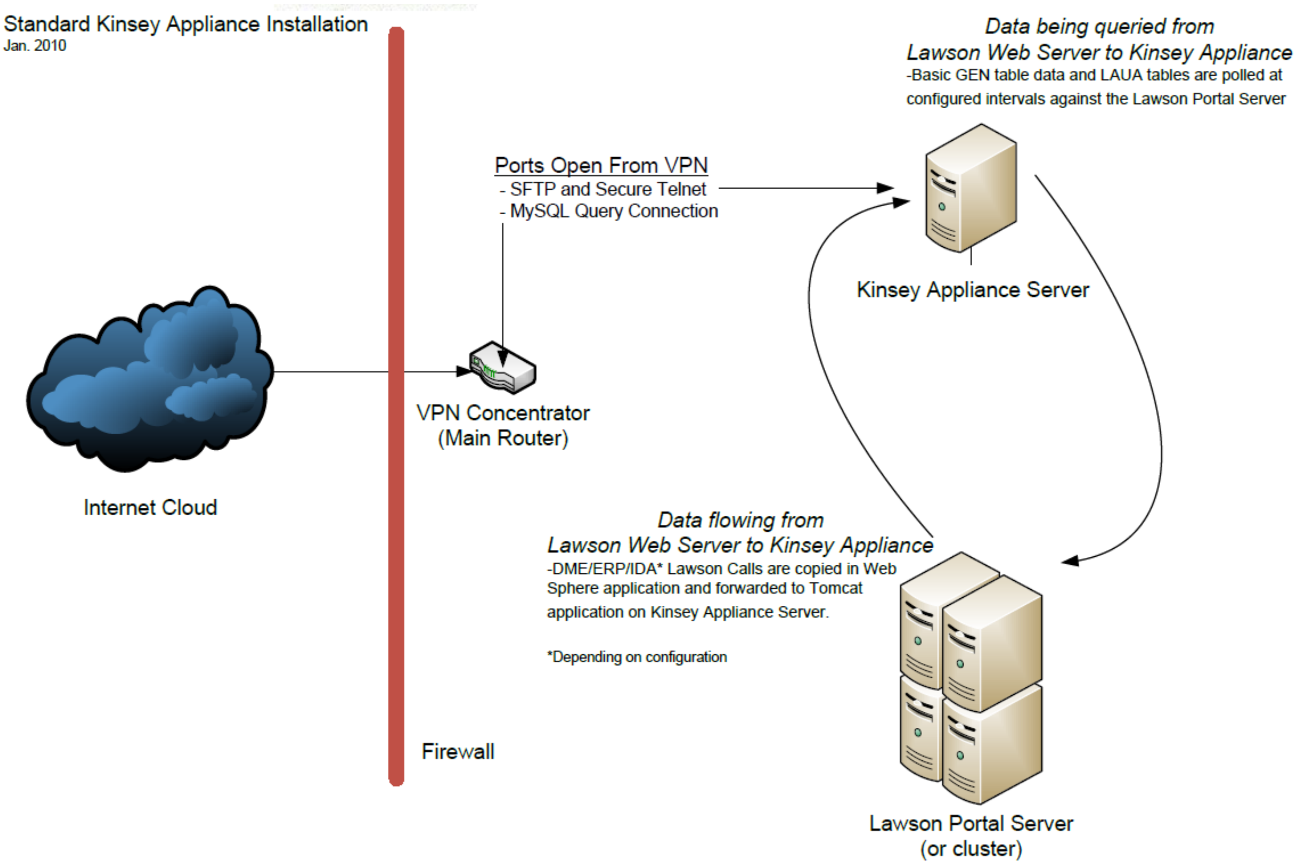
3. If LDAP Paging is used by Lawson

    - ADAM and Tivoli page sizes are based on how Lawson is set. Kinsey does not make a change to these settings.

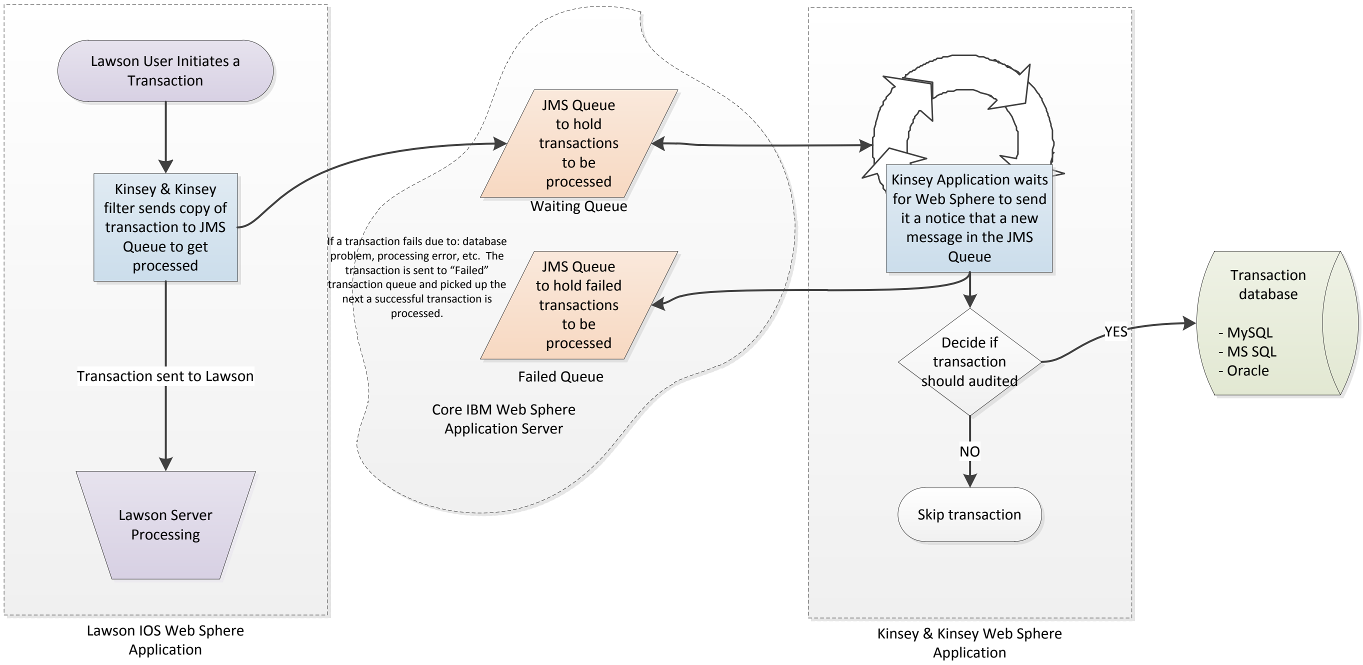
4. If LDAP Paging ***is not*** used by Lawson

    - If using Tivoli then the maximum records has to be set to (Users x Identities available).

Kinsey Appliance Installation


Standard Kinsey Appliance Installation
Jan. 2010
Data being queried from
Lawson Web Server to Kinsey Appliance
-Basic GEN table data and LAUA tables are polled at configured intervals against the Lawson Portal Server
Ports Open From VPN
- SFTP and Secure Telnet
- MySQL Query Connection
Kinsey Appliance Server
Internet Cloud
VPN Concentrator
(Main Router)
Data flowing from
Lawson Web Server to Kinsey Appliance
-DME/ERP/IDA* Lawson Calls are copied in Web Sphere application and forwarded to Tomcat application on Kinsey Appliance Server.
*Depending on configuration
Firewall
Lawson Portal Server
(or cluster)

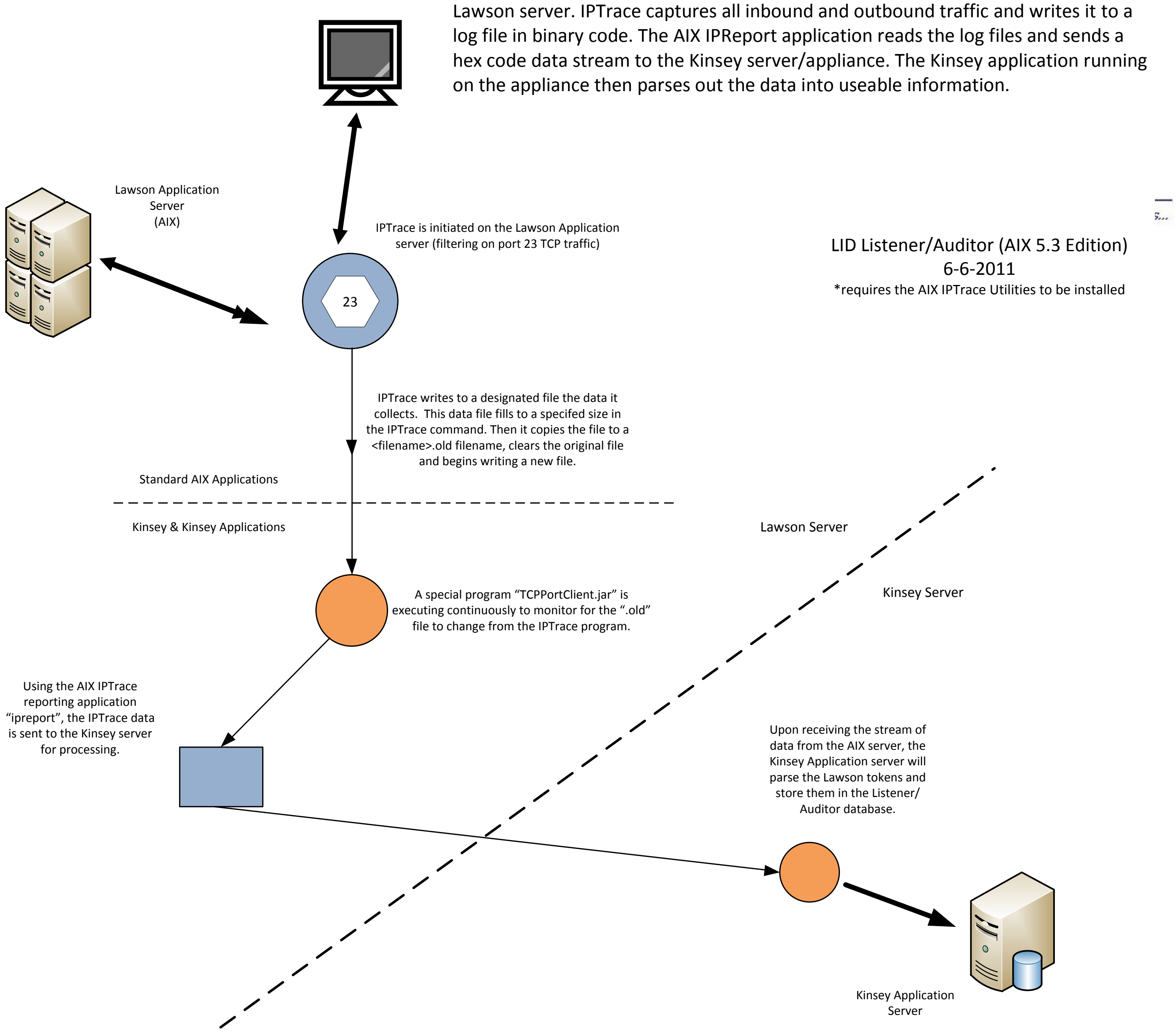
Lawson Portal Listener/Auditor Overview


Lawson User Initiates a Transaction
Kinsey & Kinsey filter sends copy of transaction to JMS Queue to get processed
Transaction sent to Lawson
Lawson Server Processing
Lawson IOS Web Sphere Application
JMS Queue to hold transactions to be processed
Waiting Queue
JMS Queue to hold failed transactions to be processed
Failed Queue
Core IBM Web Sphere Application Server
Kinsey Application waits for Web Sphere to send it a notice that a new message in the JMS Queue
Decide if transaction should audited
YES
NO
Skip transaction
Transaction database
- MySQL
- MS SQL
- Oracle
Kinsey & Kinsey Web Sphere Application

If a transaction fails due to: database problem, processing error, etc. The transaction is sent to “Failed” transaction queue and picked up the next a successful transaction is processed.

HPUX/AIX Lawson LID Listener/Auditor Overview

All telnet activity, including logins, is sent through port 23 as clear text to the Lawson server. IPTrace captures all inbound and outbound traffic and writes it to a log file in binary code. The AIX IPReport application reads the log files and sends a hex code data stream to the Kinsey server/appliance. The Kinsey application running on the appliance then parses out the data into useable information.



IPTrace is initiated on the Lawson Application server (filtering on port 23 TCP traffic)

LID Listener/Auditor (AIX 5.3 Edition)
6-6-2011
*requires the AIX IPTrace Utilities to be installed

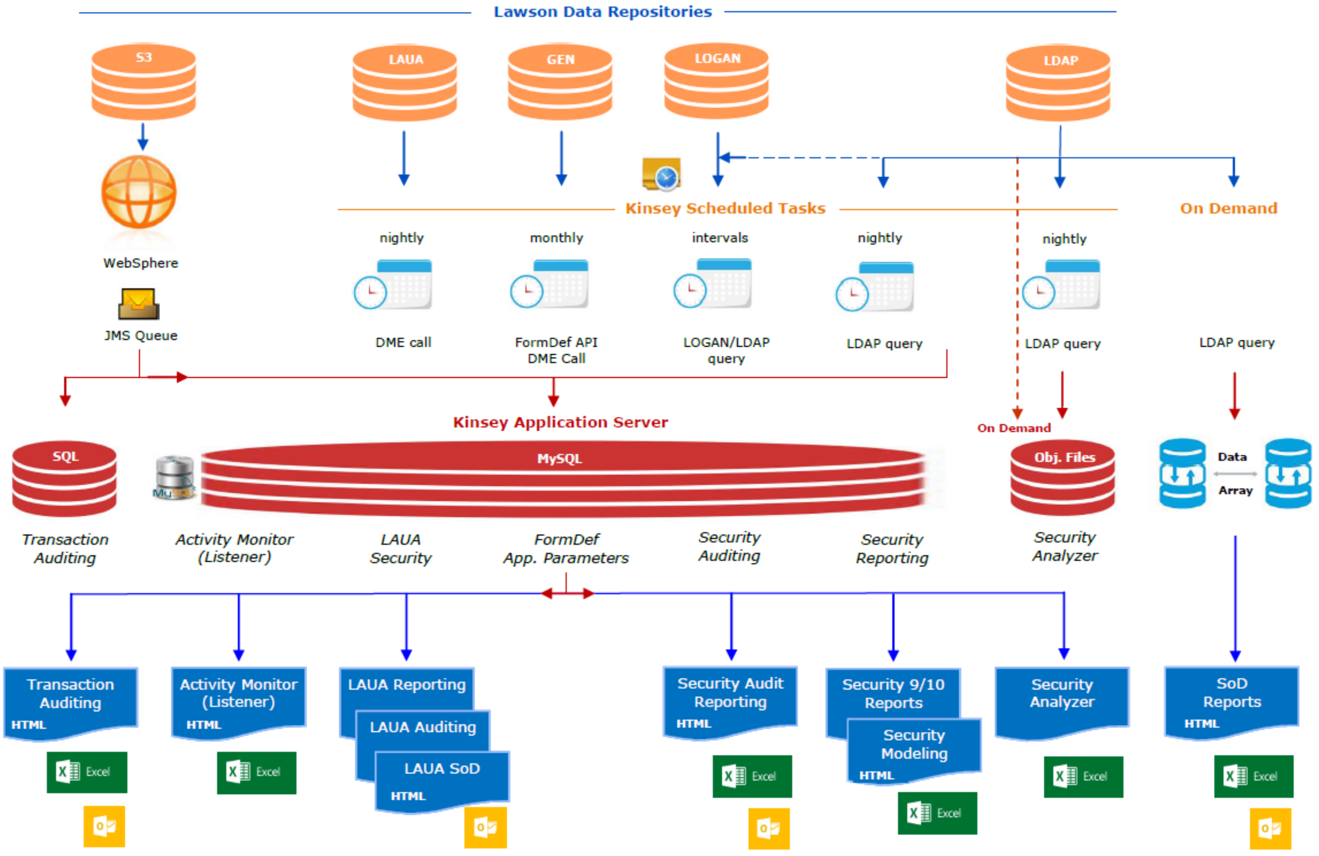
IPTrace writes to a designated file the data it collects. This data file fills to a specifed size in the IPTrace command. Then it copies the file to a <filename>.old filename, clears the original file and begins writing a new file.

A special program "TCPPortClient.jar" is executing continuously to monitor for the ".old" file to change from the IPTrace program.

Using the AIX IPTrace reporting application "ipreport", the IPTrace data is sent to the Kinsey server for processing.

Upon receiving the stream of data from the AIX server, the Kinsey Application server will parse the Lawson tokens and store them in the Listener/ Auditor database.

Kinsey Application Flowchart



Hardware Requirements

Kinsey Application Server (VMware, 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

- Cent OS - Version 5.5 (Community Enterprise RedHat v5.5)   *Kinsey preferred OS
- Similar version of Linux

OR

Microsoft Windows

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

For Windows 2012R2 see hardware requirements above

Server Software (to be installed by Kinsey)

- MariaDB v10 or greater
- Tomcat v8.0 or greater
- Java v1.8 or greater

These are minimum hardware and software requirements for the following products:

- Kinsey LAUA Auditor and Reporting
- Kinsey Activity Monitor (Listener)
- Kinsey Transaction Auditing
- Kinsey LS9 Dashboard
- Kinsey Segregation of Duties
- Kinsey SMP Applications

Application Software, Connection and User Requirements

Supported Software Versions

Supported Applications	Excel 2003	Excel 2007>	Adobe	MSAccess 2003*	MS Access 2007>	MS IE (Minimum Version)	Chrome
LAUA Reporting/Auditing	Yes	Yes	Yes	NA	NA	9.x	29.0
LS9 MS Access Reporting	Yes	Yes	Yes	Yes	Yes	NA	NA
LS9 Browser Reporting	Yes	Yes	Yes	NA	NA	9.x	29.0
LS9 Security Analyzer	No	Yes	Yes	NA	NA	9.x	29.0
LS9 Auditing	Yes	Yes	Yes	NA	NA	9.x	29.0
Segregation of Duties	NA	NA	NA	NA	NA	9.x	29.0
Listener Reporting	Yes	Yes	NA	NA	NA	9.x	29.0
Transaction Auditing	Yes	Yes	Yes	NA	NA	9.x	29.0

Connection Requirements

- Appliance Server must be able to connect to: All Products
  - Lawson Server via HTTP(S) (using DME calls)
- Lawson server must be able to connect to: Listener/TA
  - Appliance Server via HTTP(S)
- Computer that Kinsey consultant runs SMP Build on must be able to connect to: SMP Projects
  - Appliance Server via HTTP(S)
  - Appliance Server via MySQL port 3306
  - Lawson Server via HTTP(S) (using DME calls)

Minimum VPN Connection Requirements

- Port 80 (web) and 3306 (MySQL) 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

- LS9 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 LS9 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 LS9 security reporting, LS9 security auditing and Segregation of Duties reporting.

- LS9 System Admin User/Password (for TEST and PRODUCTION server) (SMP Projects only)
  This user ID is required to build and maintain Lawson Security 9

  - This user needs to have full Lawson security access to the Lawson Security Administrator application.

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

User Requirements Grid

Application	Portal Admin User	LS9 User(Read only)	LS9 Admin User
LAUA Reporting/Auditing	X		
LS9 Reporting/Auditing	X	X	
Activity Monitor (Listener)	X		
Transaction Auditing	X	X	
Segregation of Duties	X	X	
Security Migration Process	X	X	X

Installation steps for Kinsey WebSphere app

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

Note: The Kinsey appliance can be restarted anytime without stopping Lawson. When the Kinsey appliance 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 appliance is running, if not start the appliance and validate that you can access the Kinsey portal page.
2. Restart MySQL and Tomcat on the appliance in that sequence and validate that you can access the Kinsey portal page.
3. If Lawson still won't start then reboot the appliance 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 Listener needs to be deactivated please schedule time with Kinsey to evaluate the condition of the appliance prior to reactivating the application. Possible problems include hardware failure, network configuration changes (i.e. Lawson or application server IP address changes), MySQL 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 appliance. If the Kinsey server is unable to received messages for any reason the JMS queues will hold the transactions until the Kinsey appliance is back online. This is similar to an email message being stuck in the outbox. If the Kinsey appliance 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 appliance is back online all of the messages (transactions) will be sent to the appliance.

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

Virtual Server Monitoring

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

PORT CHECK:

MySQL – Port 3306

Should return something similar to:

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

TOMCAT – Port 80

(This will not return anything for a GOOD)

SERVICE CHECK (if possible):

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

Tomcat - (ps -ef | grep tomcat)

PING:

Kinsey Server (for network connection check)