

Lawson Technology: Implementation Considerations

Table of Contents

Introduction.....	3
Lawson Security Highlights.....	3
Role-Based Security	5
Lawson Single Sign-On.....	6
Security and Self-Service Applications	7
LDAP Synchronization.....	7
Dynamic Security by Lookups	8
Securing Decentralized Security.....	9
Maintenance and Lawson Security.....	9
Auditing and Reporting with Lawson Security (Sarbanes-Oxley Compliance)..	10
Scalability and Performance	11
Vertical Scaling	12
Horizontal Scaling.....	13
Remoting.....	14
Advantages and Disadvantages	14
Load Balancing.....	14
Distributed Batch Processing.....	15
Process Integration and Automated Workflows	16
ProcessFlow Offerings.....	16
Using ProcessFlow	18
Integrating Lawson and Non-Lawson Applications to Create Automated Workflows.....	18
Using Lawson ProcessFlow Integrator	19

Introduction

This white paper answers some of the questions organizations have about Lawson™ Technology when it comes to meeting real business needs in three areas:

- 1) Securing data and applications and meeting auditing and compliance requirements.
- 2) Vertical and horizontal scaling of Lawson applications to maximize hardware investments while meeting changing performance and throughput needs.
- 3) Automating Lawson processes and workflows and integrating Lawson and non-Lawson applications.

While not an exhaustive attempt to answer all user questions, this white paper highlights key features of Lawson Technology that help organizations meet these challenges and provides a number of scenarios that show how easily these features are implemented. Readers will see how the Lawson Technology infrastructure can help organizations in their efforts to become compliant with regulatory requirements, to get the best possible return on IT investments by configuring their software applications in a manner that will help streamline and automate business processes, and to meet changing performance and scalability requirements for years to come.

Lawson Security Highlights

Lawson Security is based on a simple yet powerfully flexible premise. Security is driven by user information contained in an LDAP directory. Lawson calls its security model rules- and roles-based security, both of which are described below. Lawson Security ships to customers with role templates that can easily be used to help meet the security needs of many organizations. New roles and additional attributes to roles can be easily created to match virtually any information policy strategy.

Some of the terms and concepts discussed below include:

- **Resources** — In Lawson Security, a resource is a “People” or “Thing” entry that is being maintained in Resource Management. You will add People and Thing resources to the Resource Management directory. People resources are, typically, employees including Lawson users. Thing resources are non-person resources that you need to secure access to (printers and job queues, for example).
- **Attributes** — Attributes are descriptive properties of resources. This can be a name, a location, a Yes/No flag, or whatever information is applicable to the resource.
- **Resource Management** — Resource Management is the Lawson repository for globally interesting data. Globally interesting data is typically user records and other information that is needed by many Lawson components and does not change frequently. The data is stored in an LDAP directory, an industry-standard, protocol-based repository.
- **Rules** — A rule describes a specific access right to the system. Rules apply to all Lawson objects including individual screen form fields. Some examples:
 - Access to the Vendor form (API0) is granted with no restrictions.
 - Access to API0 is granted for viewing but not updating.
 - Access to API0 is granted for viewing and updating.
 - Access to API0 is granted for viewing and updating but no ability to access drill-down fields.

- **Security Class** — A security class is a group of rules that provides access to a specific task. For example, you might create a security class called Pay Vendor Invoices. This class would give access to the data source, forms, reports, and drill fields that a user needs to successfully perform this task. This security class would, in turn, be assigned to all roles that needed to be able to pay vendor invoices (AP Clerk and AP Manager, for example).
- **Roles** — In the Resource Management system, a role is a set of access rights that a user has to the system. You create roles based on the jobs that users perform at your site. You assign security classes (containers of rules) to roles and then assign roles to users. This is an extremely efficient way to assign access rights to users, particularly in systems with many users. Significant cost savings are achieved by assigning multiple roles to multi-tasked employees. This alleviates the need to build custom roles for multi-tasked employees.
- **Structures** — Structures are a specialized feature of the Lawson Security/Resource Management system. You can create a hierarchical view of your organization that you can then use to write specialized security rules. When you create a structure, you use a point-and-click interface to create nodes for each position in your company. You then link a position to a valid Resource Management ID for a user. The end result is a graphical representation, similar to an organizational chart, of your company. The data contained in the structure can then be used to write rules. In short, you can create your organizational structure in Lawson Security and have it drive your security structure.
- **Groups** — In Lawson Resource Management, a group is any assortment of people resources that you want to view as a unit. This would typically be a work group or department within your company. You can use the Resource Management repository to store all employees in your company, organized into departments, whether the employees are Lawson users or not. Groups are not the same as roles. Roles are groups of tasks; groups are groups of people. You can assign resources to groups. You can write rules for groups.

Role-Based Security

After you define your security classes and the rules they contain, you assign security classes to roles. The result is that rules within security classes govern the security for users with those roles. Any users with the role will then have the rules in those security classes applied by the security system when they attempt to access an object.

Some highlights of this approach include:

Lawson ships with a number of role templates that enable you to start using Lawson Security features right away. Users can make many types of inquires, for example, as soon as Lawson is enabled.

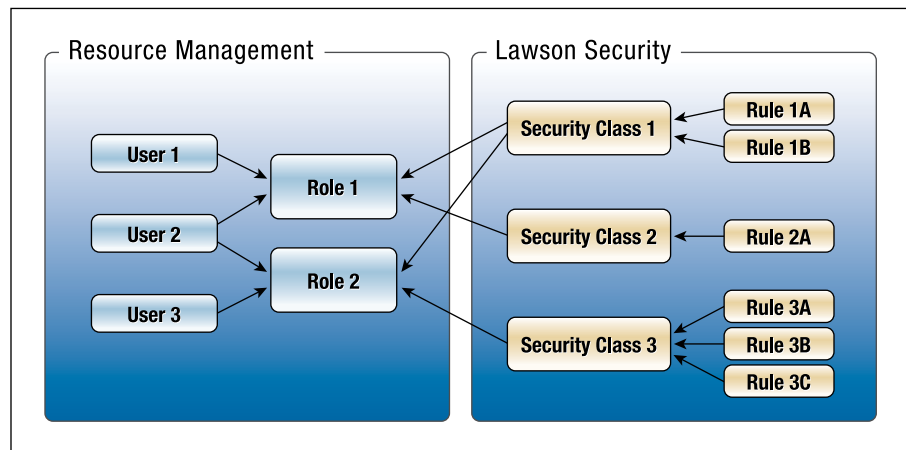
Users can, and typically do, have multiple roles.

Roles and rules can be date-and time-driven, so roles (and the access rights they contain) can be turned on and off certain times. Users, for example, can be authorized to make certain types of approvals only on certain dates and times.

Roles and rules can be unconditional or conditional. This type of access can provide:

- Unconditional access.
- Unconditional access for one or more form actions. This includes standard form actions as add, change, delete, and inquire, as well as any special actions defined for the form.
- Total denial of access.
- Conditional access based on user properties, form properties, and time and date. Conditional statements have "if" or "else" clauses associated with them. For example, the user can access this form during work hours, or on a specific date.

Security Classes, Rules, Roles, and Users



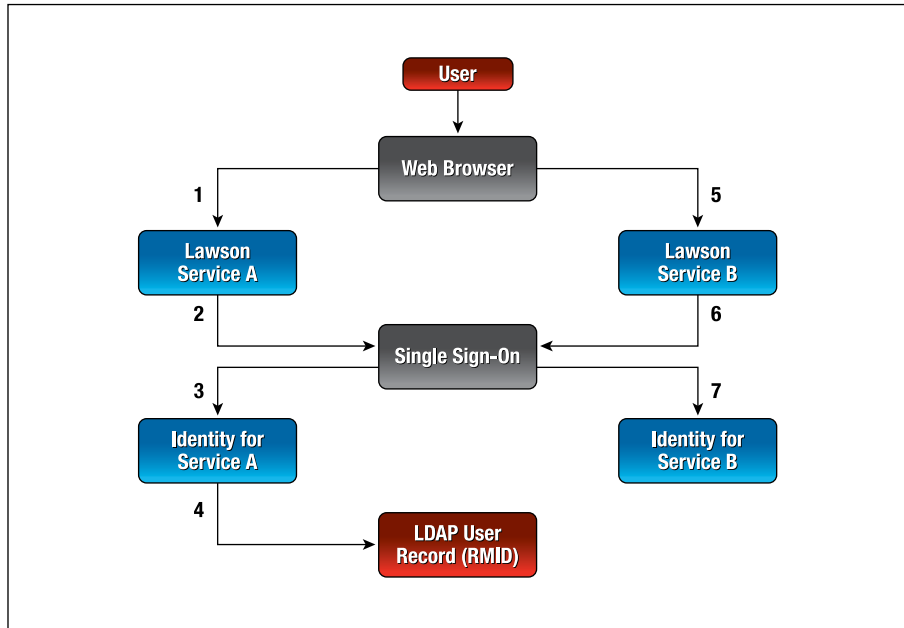
Lawson Single Sign-On

Older versions of Lawson Security, LAUA, could require numerous sign-ons, since the security model Lawson employed could require a sign on for the web server, a sign on for the application server, a sign on for Lawson Employee and Manager Self-Service, and in some cases, a sign on as a application user.

Lawson Security now enables a single sign-on for all Lawson web-based applications, thanks to the new Lawson role-based security model. Single Sign-On provides a consistent authentication interface to the user; no matter what Lawson application or service a user is attempting to access. It also enables a user to be authenticated for one Lawson service and then not need to sign in separately to other Lawson services when the user attempts to access those other services.

Can employees using Lawson Sign-On sign on to non-Lawson applications? Employees can connect to any web-based site you want through the Lawson Single Sign-On Solution. You do this by creating a service for that site. A service is a custom connection you create between Lawson applications and a third-party application.

Single Sign-On Flow



Security and Self-Service Applications

Role-based security makes securing Lawson self-service applications easy and fool-proof. You simply assign an employee a self-service role. Some are shipped with Lawson Security. Others can easily be created.

How it Works

Setting up security for the Lawson Employee and Manager Self-Service application has two main parts. The first part is to set up the agent identities for the Lawson Employee and Manager Self-Service application. These identities link a company and employee to a Resource Management ID and enable the Lawson Employee and Manager Self-Service application to limit employees to their own employee records. The second part is to use Lawson Security to grant the appropriate level of access to the forms and files needed by the Lawson Employee and Manager Self-Service application.

When you do this, you can also restrict users' access to the forms and files used by the Lawson Employee and Manager Self-Service application, depending on your data security needs. You can also set up managers who need to access their own employee records, as well as those of their direct reports, but not the employee records of any other employees.

LDAP Synchronization

Do I have to Continually Synchronize the Lawson LDAP Directory with our Existing LDAP Directory? Lawson is now LDAP compliant with existing LDAP repositories that contain information on your employees, thanks to a technique called LDAP binding. Lawson uses its own LDAP database, but when users sign-on to a Lawson application, Lawson can connect to existing LDAP databases to authenticate user passwords.

How it Works

By default, passwords are encrypted and stored in the Resource Management repository in your LDAP directory server and user authentication is handled by Lawson. Lawson also supports the ability to authenticate web access based on LDAP entries stored in a customer-specified location instead of in the Lawson default location. When you use this method to store passwords, you configure Lawson to look in your location when it authenticates a user. Some reasons you might want to do this are:

- You already store password data in an LDAP directory and you want Lawson to reuse the data.
- You want to manage passwords yourself using a tool outside of Lawson.
- You might do this, for example, if your LDAP directory supports password expiration and you want to make use of this feature.
- You use systems in addition to Lawson that require authentication and you want them all to look in the same location for passwords.

Dynamic Security by Lookups

User security is no longer created and maintained by hardcoding data about individual users pertaining to specific access rights. Rather, Lawson maintains security by imposing data level restrictions within roles. Role templates come predefined within Lawson and are also created by companies to meet specific needs. Since each employee is assigned a role or roles, they automatically receive the access rights contained in those roles. When a user role changes, their access rights dynamically reflect the change. All of this is managed with Lawson Resource Management, which is based on user data contained in an LDAP directory.

In effect, Lawson knows all it needs to know about a user's access privileges when the user signs in to the Lawson portal and is looked up in the LDAP directory. When user information in the LDAP directory changes as a result of HR changes to a user's job, their roles (and associated access rights) may be adjusted accordingly.

Rules and roles can be defined by a large number of different attributes. These attributes can be used to tailor Lawson Security to conform to the driving forces that define an organization's particular data security requirements. For some businesses, this may be territories and locations; for others, specific sites, such as a hospital or store; for others, operating units or functional departments.

A scenario:

- A financial services organization is divided into four territories (East, West, North, South). User access rights to sales accounting data are based on, among other things, territory.
- Territories are reorganized. Some states in the East are moved into the West. Some states in the South are moved into a new territory called Mid-Atlantic.
- HR changes are made to employee information to reflect the changes and the LDAP directory may be updated.
- Without a system like Lawson Security, employee access privileges would also have to be changed to reflect their reassignments (employees who moved to a different territory would have to have access privileges removed from their former territories, which could involve manually hard coding data). If a large number of employees are involved, the process can take a lot of time and effort, and employees may temporarily retain inappropriate access levels. In complex organizations, or organizations that change frequently, the effort can lead to an excessive and unmanageable number of security classes that leaves the organization less secure the more it grows or changes.
- With Lawson Security, security is dynamically driven by user information, so the moment employees are reassigned, their access rights dynamically change.

Securing Decentralized Security

The ability to “secure” security is particularly useful for larger organizations that want to give security administrators the ability to control certain aspects of user access at certain facilities or sites or within functions such as payroll, but limit their ability to administer security in other parts of the organization.

For example, a large hospital chain uses Lawson Security to allow administrators at its hundreds of sites to perform certain functions related to access for personnel at only their facility. In this example, onsite sub-administrators can assign employees to roles that include certain access privileges such as Lawson Employee and Manager Self-Service, but they have no power to create or maintain access for employees in other facilities — a privilege limited to “super-administrators” at regional and corporate headquarters. This eliminates any possibility that security sub-administrators can compromise access privileges or security policies beyond their limited areas of authority. It also reduces the number of super-administrators needed by larger organizations in centralized security departments. The following are some of the types of Lawson Security administrators you can create:

- Super-administrators with access to the entire Lawson system. It is necessary to have at least one person with access to the entire Lawson system.
- Sub-administrators who only need access to the Lawson Security Resource Management Administrator. For example, you might have an administrator whose only administrative job is to add new users to the system but who can't create or assign security classes and write rules.
- Schema Editor administrator. If you choose to change the Lawson-delivered schema (metadata) for Lawson Resource Management (for example, you may want to add your own attribute or hide a Lawson-delivered attribute that you don't use), you must have at least one user who has access to the Schema Editor. However, you might want to have an additional special administrator for this purpose. Sites that do not change the Lawson schema do not need to make use of this tool.
- Lawson Portal Administrator. A Portal Administrator is responsible for assigning access to what users can do and see in the Portal and for assigning Portal bookmarks. A Portal Administrator does not need administrator status in Lawson Security. However, if you want a Portal Administrator to be able to manage Portal attributes that are stored in Resource Management, you could (for example) set them as Resource Management administrators.

Maintenance and Lawson Security

Regardless of the size and complexity of your business, Lawson Security contains a number of features that make assigning and maintaining security access more efficient and more easily maintained, even for a large numbers of users.

When attributes, structures, and groups are used to write access rules and drive roles, it's easy to recreate your existing organizational structure within the Lawson Security framework. This can make developing and implementing an enterprise security strategy relatively easy, not to mention easily maintained.

Attributes makes it easy to use factors that are important to your business to drive security. Location is a good example. (Regions and operating units are other good examples.) If your business consists of many locations and you want to drive your security model by these locations, you can create roles within Lawson Security based on location. When an employee changes location, their role(s) and particular access privileges automatically change to match the new location.

Attributes that define roles can also be made conditional. If an employee works in two different locations, for example, access privileges for their two different roles can be limited to certain dates and times.

Roles can be assigned or changed in a group (see above). For example, if you want to add a role to a corporate finance group or delete a previously assigned role, you can perform this maintenance at the group level instead of at the individual user level.

You can do generic role assignments. This can be very useful if employees frequently move from one part of the organization to another. For example, employees in a sales unit could be assigned a blanket "sales" role, which grants them access to certain types of sales data through the Lawson Portal, regardless of their location at any particular time. If an employee is transferred out of sales, as soon as his or her HR record is changed, he/she no longer has sales-role access rights.

Auditing and Reporting with Lawson Security (Sarbanes-Oxley Compliance)

One important question for any potential Lawson customer is how Lawson Security auditing and reporting features help organizations comply with Sarbanes-Oxley and other legal and regulatory requirements. The answer is simple: Lawson Security can help provide auditors and others the answers to virtually any security-related question in real-time. This comes by way of reports built-in to Lawson Security and also by the ability of users to load Lawson data logs into report writers to create custom reports.

Auditors can also be given a "role" with certain access rights as Lawson users and query the database directly. This eliminates any questions about the independence and impartiality of data and produces real-time answers. For example, an auditor might want to see all users with access to five different Lawson forms. Instead of requesting reports on users for each form from a security administrator — a process that could take a few days or more — and then comparing five different forms manually, the auditor is given a limited role that allows him or her to query through the Lawson Portal and run reports without the ability to change or enter data.

Lawson Security also has a number of fairly simple yet profoundly important provisions for meeting compliance requirements and audits, including workstation control and password management. For example, the Lawson Security session management feature allows businesses to close down a user's session after a certain specified period of inactivity — meeting auditors' demands to shield sensitive data on unattended workstations from viewing by unauthorized personnel. The same feature can be used on the Lawson Employee and Manager Self-Service application running on kiosks.

The types of reports available with Lawson Security include:

- User security reports. Simply enter a user ID to see what individual users have access to, including both forms and data.
- All users who have access to specific Lawson applications or features. For example, if an auditor wants to see every employee who can access and/or add information about something as sensitive as garnishments, he or she can enter the related garnishment form within Lawson and see who those employees are.
- Segregation of duties. Lawson Security makes it easy to see or report on users who have a combination of roles that may potentially violate the concept of segregation of duties mandated by Sarbanes-Oxley.
- With Lawson Security you can also view logs of single user activity.
- With Lawson Security you can control user access to forms and data in virtually any way — from the basic access level needed by users of the Lawson Portal (without access to any forms in the main Lawson application product line) to allowing users access to application forms and data, to giving users the ability to run batch jobs and view reports.

Scalability and Performance

Lawson Technology provides organizations with two important options to scale (run multiple instances of Lawson software in parallel) their Lawson environments to whatever extent they need while maximizing performance and throughput. The options organizations select will be influenced by several factors, including what type of hardware on which they prefer to run their applications (i.e. high performance UNIX[®] servers or low-cost Windows servers) and their failover and redundancy requirements.

Key concepts discussed below include:

- Vertical scaling (distributing the Lawson workload among one or a small number of high-end servers)
- Horizontal scaling (distributing the Lawson workload among low-cost Windows servers)
- Remoting (running different components of the Lawson environment on different servers)
- Load balancing (distributing the Lawson workload among vertically or horizontally scaled servers)
- Clustered file systems (which allow you to perform remotely in a horizontally scaled environment but only have to maintain one Lawson environment)
- Distributed batch processing (distributing background processing among different servers in a horizontally scaled environment)

Vertical Scaling

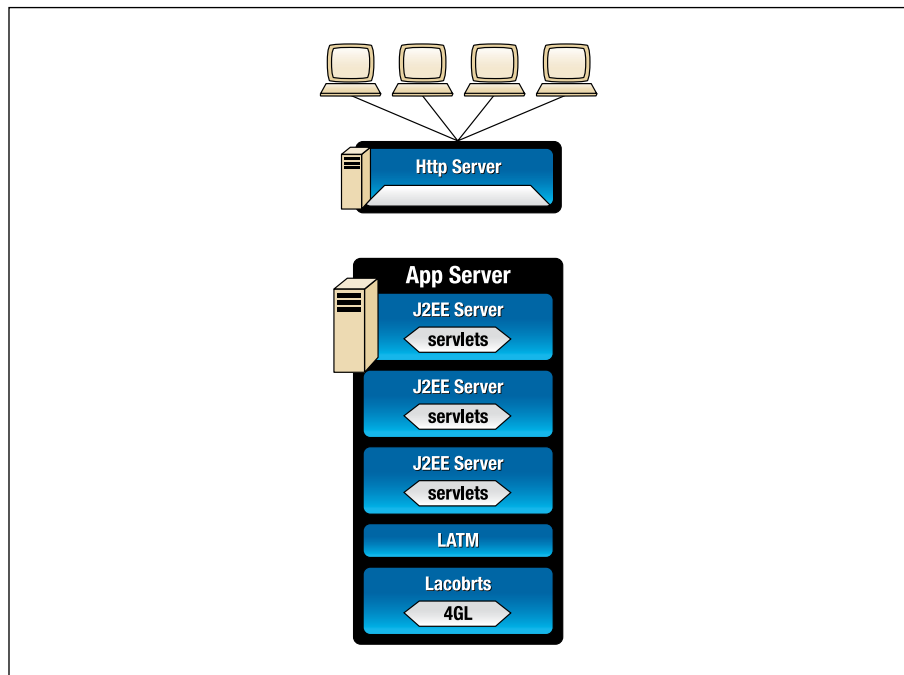
Vertical scaling refers to the ability to run multiple Java virtual machine (JVM) server instances of Lawson components and applications on one machine. The chief benefits of vertical scaling include:

- Increased throughput
- Better use of symmetric multiprocessing (SMP) resources
- Increased redundancy against software failures

Here are examples of why organizations might want to take this approach.

- Your business wants to make intensive use of a Lawson Human Resources or Lawson General Ledger application, supporting thousands of concurrent users on a single application server with multiple processors.
- You want to leverage the complete amount of processing power available on the machine.
- You prefer the stability of the 'big box' server.
- You want user access to be through remote web servers.
- You want to maintain only one Lawson environment but run multiple instances of Lawson components and applications.
- Your preferred redundancy strategy is to have a single back-up server.

Example Supported Vertical Configuration



Vertical Scaling with Lawson

Multiple server instances on one machine for increased throughput, better utilization of SMP resources, increased redundancy against software failures.

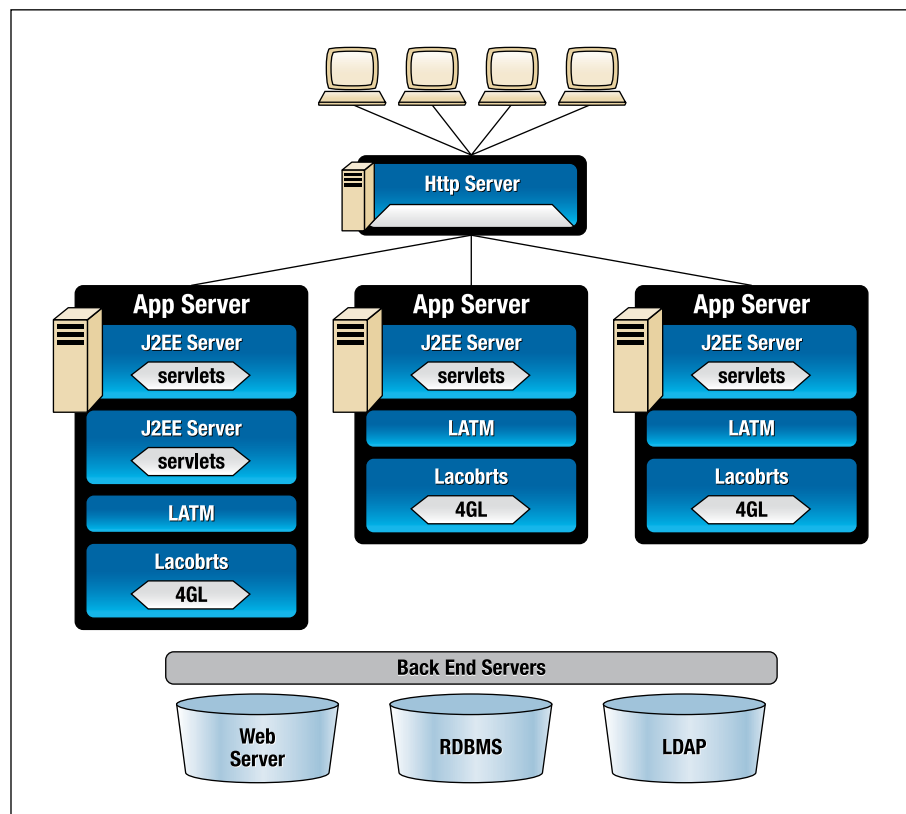
Horizontal Scaling

Horizontal scaling refers to the ability to run Lawson on multiple machines, with user requests load balanced among the various machines.

Your organization might want to take this approach if:

- Your organization prefers lower cost Windows servers. With this approach, Lawson can be up and running for as little as the cost of three smaller servers. For organizations whose key consideration is hardware costs, this is an important benefit.
- When the numbers of users grow and you need more throughput, you prefer to simply add as many Windows servers as you need.
- You prefer the failover capabilities of this type of environment. If a particular machine fails, user requests can be redirected to a different machine.

Example Supported Horizontal Configurations



Horizontal Scaling with Lawson

Multiple servers on multiple machines for lower hardware costs, increased throughput, better failover.

Remoting

A key feature of Lawson Technology is a type of horizontal scaling called remoting, which provides maximum flexibility in the use of distributed platforms. With remoting, you can run each component of the Lawson environment (web server, LDAP server, application server, database server) on separate physical servers over a network, or any combination of components on the same server.

Besides making horizontal scaling possible, remoting is also a benefit for organizations that want to maximize the use of hardware in a more vertical set up. For example, say your organization has a 16-way server that supports 1,000 concurrent Lawson users. This uses only half the capacity of the machine. With remoting, you can run other components of the Lawson environment, such as the LDAP server, on the same server and make greater use of device capacity.

Advantages and Disadvantages

The Lawson approach to scalability has both advantages and disadvantages. The latter, however, are largely mitigated by other features of Lawson Technology.

For true redundancy with horizontal scaling — distributing the Lawson environment among multiple servers — you need a backup duplicate server for each distributed server.

Horizontal scaling also requires the use of a clustered file system, which you must purchase from a separate software vendor. This enables Lawson to share volumes, file systems and individual files among applications running on multiple servers as though they are running on a single server. No matter how many servers you use in your Lawson environment, you only have to install and maintain a single Lawson environment. In terms of simplifying the administration of the Lawson environment and Lawson applications, this can be a huge benefit for many organizations. But it requires what some may see as the additional burden of supporting another layer of software — in this case, a clustered file system application that can perform well in a high volume transaction environment.

The drawbacks to remoting will be far outweighed for many organizations by the savings that come from using as many low-cost Windows servers as needed to support a large base of Lawson users while only have to maintain (including patching and upgrading) the Lawson environment on a single server. The administrator's workload, in other words, will be nearly the same as if Lawson was running on only one server.

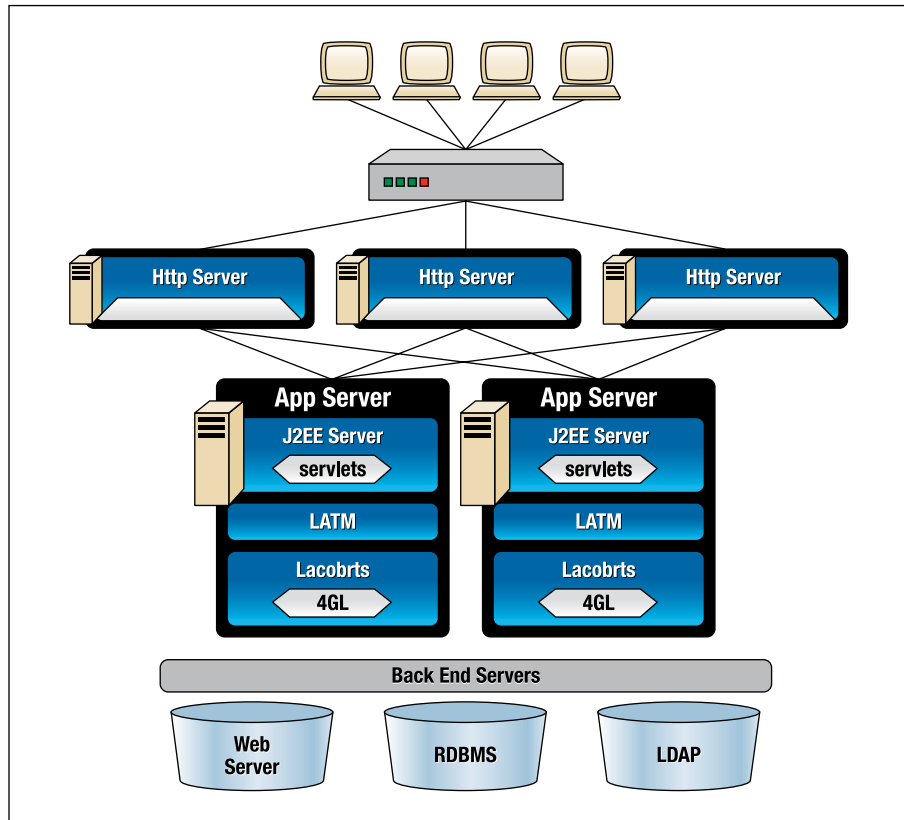
Load Balancing

Another feature of Lawson Technology allows scalability at the web-server level. With hardware-based load balancing, organizations can have any number of web servers connected to their Lawson environment. This is provided by a hardware load balancer made by Cisco® and other manufacturers. If one or more web servers fail, the user load is automatically shifted to the remaining web servers, resulting in no interruption to users accessing Lawson applications through the Lawson Portal.

Weighted load balancing provides organizations with the ability to balance their Lawson workload among different servers of different capacity. This helps them use their hardware installations more efficiently. For example, you may want to support 3,000 concurrent users. You have an eight-way server capable of supporting 2,000

users, but you don't want to purchase another eight-way server to support the remaining 1,000 users, since this represents more capacity than you need. Weighted load balancing allows you to balance the workload between different-sized servers. In this example, you could put the remaining 1,000 users on a much less expensive four-way server, with the workload balanced between the two machines. In other words, you can divide the workload among servers of differing capacities and ensure that you don't have to buy more hardware than you need.

Hardware Load Balancing



Hardware Load Balancing with Lawson

Provides virtual IP addresses for all web servers for greater flexibility in configuration.

Distributed Batch Processing

One question organizations may have about a horizontally scaled Lawson installation is how to handle batch processing (jobs that run in the background and are managed by a queue) in such an environment. Lawson installations also support distributed batch processing in horizontally scaled environments, with communication between servers via TCP/IP sockets. This can be an important way to improve system performance and another way Lawson Technology supports organizations that prefer the cost and failover benefits of a horizontally scaled environment.

Process Integration and Automated Workflows

ProcessFlow Offerings

Lawson Technology provides a number of features that make it easy to create simple-to-complex automated workflows involving not only Lawson applications but other non-Lawson applications as well. With these features, organizations can integrate a wide variety of enterprise applications into sophisticated workflow processes and achieve a level of seamless enterprise application integration.

ProcessFlow is a Lawson process automation utility that allows users to graphically define a process (activities that need to be executed in a particular sequence). In ProcessFlow, a process that moves work from one defined activity to another defined activity is called a flow. A flow transfers information and/or work from one user to the next until the work is completed. A flow can also perform work that does not involve users, such as taking information from one Lawson form and adding or changing the same information on another Lawson form automatically. For example, when a new employee is added on an HR Employee form, that employee could also automatically (by means of a flow) be set up as a Vendor for Employee Expenses.

ProcessFlow Standard is delivered with Lawson Technology and includes pre-built workflow processes covering various functional areas. ProcessFlow Standard allows you to make a limited number of changes to pre-built workflows, using ProcessFlow Designer, which provides a graphical interface that allows you to use icons to represent the activities of a process and the relationship of those activities to each other.

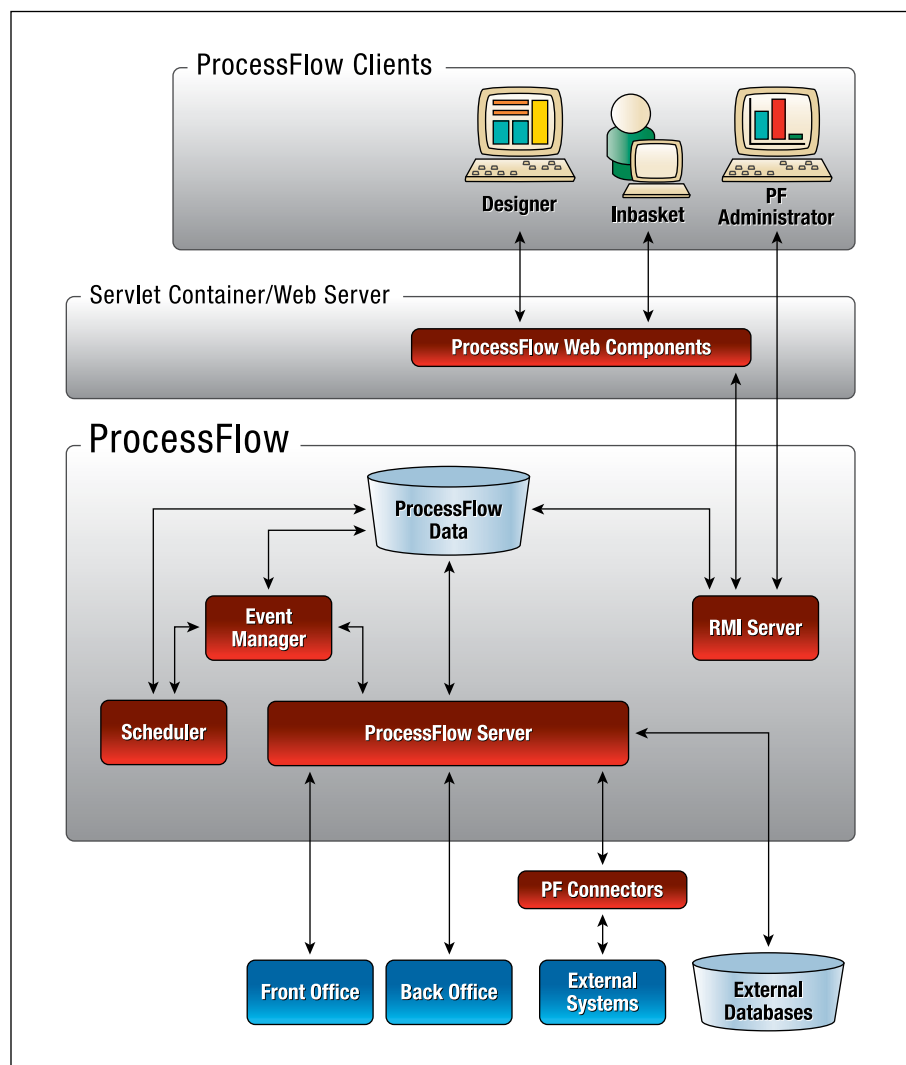
ProcessFlow Professional is an option to ProcessFlow that allows you to make more extensive changes to pre-built workflows or create new workflows.

ProcessFlow Integrator is an option to ProcessFlow that combines the functionality of ProcessFlow Professional with the ability to link any non-Lawson application(s) to Lawson applications so that data flows between them. ProcessFlow Integrator enables high-volume, real-time transactions into and out of Lawson applications. ProcessFlow Integrator also links non-Lawson applications to the Lawson applications where real-time is not a requirement but easy sharing of data via batch mode is required.

ProcessFlow Integrator helps customers integrate their business operation systems with Lawson business management system and database. With ProcessFlow Integrator, Lawson applications can communicate with non-Lawson applications. It can update the LDAP security repository to reflect changes in the ERP data in security, inactivating security for terminated employees. ProcessFlow Integrator can also reach out to Web Services within Lawson and beyond Lawson to your enterprise. ProcessFlow Integrator:

- Validates transaction data by executing Lawson business logic.
- Transforms data to a form that is recognized by Lawson applications.
- Transforms data to a form recognized by a foreign system.
- Performs complete business processes with supplied APIs.
- Transmits data into Lawson applications from a foreign system.
- Enables inquiry on and change of Lawson data from a foreign system.
- Transmits data from Lawson to a foreign system using Lawson ProcessFlow workflow triggers.

Form Clip: ProcessFlow Architecture



Using ProcessFlow

Lawson ProcessFlow Standard is designed to make automation of common Lawson workflows easy.

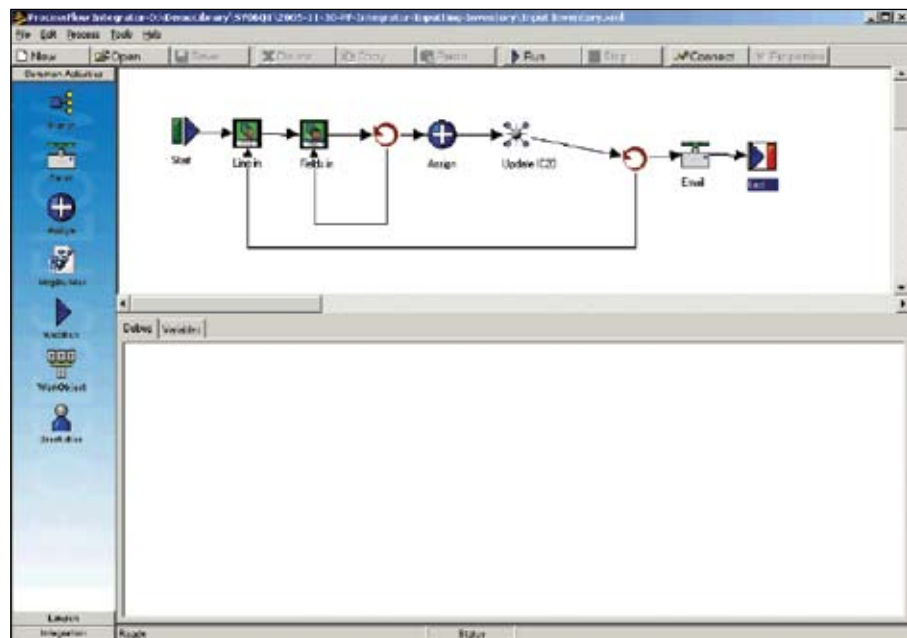
One key to the ease of use of ProcessFlow Standard is a series of Solution Packs that come standard with Lawson applications. Among other functions, these automatically notify via email Lawson users whenever a “downstream” event has occurred in a Lawson application that requires an action on their part. When the action then occurs users “upstream” in the process area similarly automatically notified. These pre-built solutions can be customized to a certain extent through ProcessFlow Designer, although making full use of all ProcessFlow Designer capabilities requires ProcessFlow Integrator.

Integrating Lawson and Non-Lawson Applications to Create Automated Workflows

There are two ways to integrate Lawson and the optional non-Lawson applications into automated workflows. Both ways involve using the optional Lawson ProcessFlow Integrator application.

The first method integrates Lawson and non-Lawson applications at the database level. By using what Lawson calls the SQL node in ProcessFlow Designer, you can link activities within the Lawson environment to changes in a database outside Lawson. This happens by linking a change in a non-Lawson database table to an automated workflow event within a Lawson application. These changes must consist of “Yes/No” database events.

ProcessFlow Designer Workspace



For example, you have a non-Lawson time card system and a time record is added by an employee. You want the Lawson Human Resources application to notify the appropriate manager that the time card needs to be approved. Using ProcessFlow Designer, you can link the change in the non-Lawson database to an automatic email notification within Lawson Human Resources to the manager that the time card needs action.

That's a simple example, but it's easy to chain processes together to create quite sophisticated workflows that launch processes within Lawson-based events in other systems, or processes in other systems based on events within Lawson. For example, non-Lawson Point-of-sale systems that link to non-Lawson inventory management applications can be linked to Lawson Procurement to automatically create purchase orders when inventories for specific products fall below certain levels. Similar workflows that pass back and forth between Lawson and non-Lawson applications can be created through Lawson Human Resources, Lawson Financials and other applications.

Using Lawson ProcessFlow Integrator

So far, we've discussed a level of integration that occurs when a pre-determined "Yes/No" event in one application, Lawson or otherwise, triggers a predetermined event in other applications.

Lawson ProcessFlow Integrator takes it a big step further by dynamically interfacing Lawson and non-Lawson applications to enable high-volume, real-time transactions into and out of Lawson applications. ProcessFlow Integrator also links non-Lawson applications to Lawson applications where real-time is not a requirement but easy sharing of data via batch mode is required. For example, a proprietary application that resides on a mainframe computer can be linked to Lawson applications so that the mainframe application and the Lawson applications share data.

Lawson ProcessFlow Integrator is the newest addition in the Lawson Business Process Management Suite. BPM products automate short-lived transactions between applications/systems, for example, integrating an order transaction from a web site into a procurement application, while also automating long-lived transactions that flow across disparate applications/systems, for example, requiring human review and approval before time records from one application are transferred into another, disparate application.



Headquarters:

Lawson
380 St. Peter Street
St. Paul, MN 55102-1302
USA
Tel +1 651-767-7000

info@lawson.com
www.lawson.com

**For further information about Lawson Technology, call 1-800-477-1357,
direct at +1-651-767-7000, international at +46 8 5552 5000.**

Lawson, Lawson Software and the Lawson logo are trademarks of Lawson Software, Inc. Other products or services names mentioned may be trademarks of Lawson or the respective owners of those trademarks. Copyright ©2007 Lawson Software, Inc. All rights reserved. EEO/AA C-WP460 0107