PartnerWorld

IBM
Developer
News

Developer Directions

IBM

Developers

Editorial

Welcome to this new edition of IBM Developer Directions, which reflects the continuing commitment of PartnerWorld for Developers to provide our partners with an integrated look and feel in our communications.

With the increase in e-commerce and Internet usage, companies have realised that security is absolutely vital in their internal and external processes as they transform into e-businesses .

The acronym, PAIN, seems to be an ironic description of the four risks associated with Web security. However, in our lead article, our authors show you how these elements can be dealt with.

One of the benefits of open source development is that any security deficiencies can be detected and fixed quickly. Find out how IBM Netfinity* servers running Linux provide a reliable foundation for all aspects of e-business on page 5.

Our regular technical sections are packed with articles for you. Our DB2* section, in particular, contains an excellent article by John Rodriguez on the IBM Enterprise Information Portal which can benefit companies by reducing the cost of locating information and increase user productivity.

Finally I would like to draw your attention to our new e-mail address for feedback – **developernews@uk.ibm.com**. I would be very interested to hear if you have any comments or suggestions regarding this edition.

Regards

Eileen

Eileen Soriton, Editor-in-chief

December 1999/January 2000

PartnerWorld for Developers

IBM Developer News

Developer Directions

Issue 22

e-business: safety by dealing with PAIN

Web security for Netfinity servers running Linux

Security systems leaving you irked and plagued?

e-business: safety by dealing with PAIN

by Stacy Cannady and Thomas H. Stockton

e-business is based on a flow of information between businesses over the Internet. The value of e-business is reduction in costs or increase in revenue that comes as a product of exchanging business information over the Internet. The danger of e-business is the risk of information being lost, stolen, fabricated or corrupted as it passes over the Internet. Therefore, what can be done to mitigate the risks of e-business?

The risks

There are four security risks that must be addressed to assure the safety of e-business transactions and associated data. These four risks can be remembered with the abbreviation PAIN:

Privacy: e-business transactions are protected against access by attackers who seek to make copies of them or insert fraudulent data into the process.

Authentication: Access to e-business applications and data is restricted to those who can provide the appropriate proofs of identity.

Integrity: e-business data and applications are protected in such a way that any effort to change them is detected and prevented.

Non-repudiation: The flow of data through an e-business application and the flow of transactions that drive the data are logged and reported in such a way that should a dispute arise about any transaction, proof of what actually happened can be produced.

The solution

Public Key Infrastructure (PKI) **[www.ibm.com/security/technologies/techpki.html]** provides a solution to the risks of e-business. Elements of PKI technology can be used to solve each of the risks individually, or PKI technology as a whole can be used as a complete security solution for e-business applications. The remainder of this article provides examples of how PKI can be used to address each of the PAIN risks.

Privacy means that a transaction between businesses cannot be viewed or interfered with by an outside party. PKI uses encryption to ensure that transactions are kept private. PKI technology can use encryption to protect the privacy of data in *transit* and in *storage*. Many businesses today think that Virtual Private Networks (VPNs), Extranets or Secure Sockets Layer (SSL) are sufficient to ensure the privacy of e-business. In fact, many of these solutions use PKI encryption technology to provide privacy. However, these solutions can provide privacy for the actual exchange of data across the Internet, and that is all. They do *not* provide privacy for data stored on e-business servers that are connected to the Internet.

There have been many news reports of the theft of e-business data stored on e-business servers. In these cases, the e-business data is stored with limited protection on the e-business server. A hacker who successfully breaks in to the server will almost certainly be able to find and steal that data. If the data is stored in an encrypted format, then the threat of theft is significantly reduced.
Even if the data is stolen, the thief must break the encryption before it can be of any use to him.

While the value of this privacy is obvious, the cost of privacy is less obvious. Encryption is a wonderful tool to protect valuable information, but there is a performance cost associated with the use of encryption. e-business applications that rely on encryption for privacy must be placed on larger servers that are able to provide the additional computing resources that will be needed by the encryption programs.

Authentication means that access to an e-business system is limited to those who can provide the proper identity credentials. Authentication is commonly handled through the use of a logon ID and password. This technology is considered a very low level of authentication and is often easy to break. PKI uses a _digital certificate_ as the identity credential. The idea of a digital certificate is similar to the idea of a passport. Nations require that people travelling across international borders must be able to produce an identity credential called a passport. People get passports by proving who they are to their national government. All governments accept a passport as evidence that the issuing national government believes that this person is who they claim to be.

A digital certificate is very similar. A person must prove his identity to a _Certificate Authority_ or CA. If the CA can verify the claim of identity, it will issue a digital certificate that states that the issuing CA trusts the identity of this individual. Programs that require a digital certificate as an identity credential also specify what CA or CAs they accept certificates from. This is an additional level of security. It prevents a person from starting his own CA and issuing fraudulent certificates. It is also a way for a company to specify who it trusts by defining which CAs it trusts.

In the physical world, we keep our ID in a wallet. In the electronic world, there are two common places to store a digital certificate. The most common is in a Web browser. You may not be aware of it, but you likely already have several digital certificates stored in the browser and used to access various sites on the Internet.

The next most common place to store a digital certificate is on a Smart Card. In this case, the Smart Card is inserted into a special reader in order to access a secured system. The secured system reads the digital certificate stored on the card and decides whether to permit you access.

Some technologies make extensive use of certificates "under the covers," hidden from the view of a user. For example, Virtual Private Networks (VPNs) often rely on certificates to prove identity of network devices. Secure Sockets Layer (SSL), a widely used tool for securing e-business transactions on the Web, also uses certificates built into Web browsers and servers.

Integrity means two things. One meaning of integrity is that the data received is the same as the data sent. That means that the data was not changed in transit either by mistake or on purpose. The other meaning is that at any time in the future, it is possible to undeniably prove whether different copies of the same document are in fact identical or not.

PKI uses a technology called "message digest" or "hashing" to ensure data integrity. It is possible to view any data object as a string of numbers, even if people view it as a text document. Message digest programs do exactly that, they view all data objects as strings of numbers. A message digest program adds up the numbers in a data object using a special technique. The result is a single number called the message digest or hash value of the data object. Because of the mathematical technique used in the calculation, the hash value of a data object is unique – no other data object can produce the same hash value. If so much as one character is changed, added or deleted in a data object (even a blank at the right end of a line), the calculated hash value will be different and the loss of integrity will be detected.

The message digest is a common way of verifying data integrity in transmission. The sender calculates the message digest and sends that value with the file he is transmitting. The recipient calculates the message digest of the received file and compares it to the value that the sender calculated. If they are the same, then the file sent is the same as the file received.

Non-repudiation means that if a discrepancy or dispute arises over an e-business transaction, there is incontrovertible evidence present within the e-business system that can be used to prove beyond reasonable doubt just what exactly occurred and why.

The most common way to provide non-repudiation through the use of _digital signatures._ A digital signature is the electronic equivalent of a hand written signature. Many nations and most of the states in the United States now have laws that define how and where digital signatures can be used in the conduct of business. Most nations will have digital signature laws on the books within two years.

Developer profile

Stacy Cannady has 20 years experience in systems and network support and in data security. Stacy currently works for IBM in PKI security products. He can be reached at *scannady@us.ibm.com*

Thomas H. Stockton has over 12 years experience in the areas of EDI, e-commerce and Internet security, specifically with PKI. Tom currently works in IBM's PKI marketing group, holds an MBA and has contributed several articles to Electronic Commerce World. He can be reached at *tstock@us.ibm.com*

PKI technology is based on a cryptological technique that can create a unique pair of numbers. These numbers are used as keys by special encryption programs. If a file is encrypted with one key in a given pair, only the other key can decrypt it, and vice versa. PKI specifies that when a person receives a key pair, one member of the pair will be kept private and the other will be published as the public key. Here is an example to illustrate how the key pairs are used.

Alice and Bob each have PKI key pairs. They each have access to the other's public key. If Alice wants to send Bob a private message, she can encrypt the message with Bob's public key and send it. Only Bob's private key can decrypt the message, so Alice has confidence that only Bob can read the message, even if a million people were to receive the message.

Now consider another example. Bob and Alice want to digitally sign an electronic contract and they want to be sure that the contract can't be changed later and that neither can dispute that they signed it. Bob will do the following:

Bob and Alice agree to the terms of the contract

Bob calculates a message digest or hash value of the electronic contract

Bob encrypts the hash value with his private key

Bob provides the contract and the encrypted hash value of that contract to Alice

Alice can prove that the hash value is from Bob because Bob's public key can decrypt it. Since no other key in existence can decrypt this hash value, it must have been encrypted using Bob's private key. Alice can tie the decrypted hash

value to the contract by calculating a hash value of the contract herself. Since each document produces a unique hash value, if the value she calculates is the same as the value Bob provided, then the contract she has is the same as the one he sent. Now Alice will encrypt the hash value she calculated with *her* private key. Both parties have digitally signed the contract. The proof of this consists of the following:

The contract

The hash value of the contract, encrypted by Bob's private key
The hash value of the contract, encrypted by Alice's private key

If there is doubt about the contents of the contract, the parties can calculate a hash value of the contract and compare it to the original values calculated by Bob and Alice.

If there is doubt about the keys, can Bob's public key decrypt his version of the hash value? Can Alice's decrypt hers? If the answers are "yes," then the only possible argument that can be made is that a private key has been stolen. If this argument is made, then *all* documents that have been signed or encrypted by the compromised person can be said to be legally void, since the date of theft is probably not known.

Conclusion

Business data has value and so must be protected. Some business data has more value, some less value. This means that an important consideration in the design of any e-business application is "how valuable is this data?" The greater the value, the more must be done to protect it. This measure of value is used to justify a budget for security software and security specialists that will be used to protect the e-business application once it is deployed.

There are four main risks associated with e-business. They are: **p**rivacy of transactions, **a**uthentication of individuals who have rights to access e-business systems, **i**ntegrity of data in transit and in storage, and **n**on-repudiability of transacted business. These four risks can be remembered with the acronym PAIN. PKI technology offers solutions to each of the elements of PAIN in e-business.

Web security for Netfinity servers running Linux

by Julie Briddon

According to the Netcraft Web Server Survey **[www.netcraft.co.uk/ survey/]**, more than 55 per cent of all Web sites currently use the open source Web server Apache **[www.apache.org]**, many in combination with the Linux operating system.

IBM Netfinity servers running Linux **[www.pc.ibm.com/ww/netfinity/ linux]** offer a reliable foundation for e-business computing, Internet communication, collaboration, Web application development, e-commerce and Web serving. Based on open, industry standards, Netfinity servers provide outstanding performance, reliability, manageability and security for core business applications.

As part of IBM's commitment to open standards, IBM works closely with major industry operating system vendors to optimise and deliver the most robust solutions possible on a Netfinity platform. With input from the development team at SuSE **[www.suse.com]**, this article is meant to help you identify key areas to focus on when implementing a Linux-based Web Server.

The Advantage of Open Source Development
Linux's best advantage: the source code to the operating system and most applications (including the Apache Web server) is freely available and open to everyone. This unique feature makes it easy to adjust and extend the software to your needs.

It also makes the software highly secure. The availability of the source code minimises backdoors or similar security leaks. Security holes or serious bugs will usually be detected and fixed quickly.

Linux Web Server Implementation Tips and Techniques
Since Linux is a "child of the Internet", acting as a Internet server is one of its greatest strengths. If you plan to run a Web server on the Internet using Linux, make sure that you apply all available security fixes.

Most Linux distributions are already pretty secure in their default configuration. However, it is advisable to deactivate all services and daemons that are not necessarily needed for the operation as a Web server, eg. Telnet, ftp or sendmail.

If the service is running as a stand-alone process, disable it.

If it is started using inetd, have a close look at the configuration file /etc/inetd.conf and comment out all services that you do not need.
Even better: disable inetd too.

Linux can also be used as a very flexible packet filtering firewall. This functionality is integrated in the Linux kernel and is called "ipchains". In addition to rule-based packet filtering, ipchains can also be used for Network Address Translation (NAT) or as a transparent proxy server.

If you want to test the security of your Linux server, you can use one of the several security testing tools that are freely available: nmap, Saint or Nessus can be used to scan a single host or an entire network for security holes. These tools can also be used to test any other operating system for security holes.

Conclusion

With momentum derived from the open source model of development, Linux has experienced phenomenal rates of growth and is changing every rule in the IT market. Combined with the open platform design and industry standards of award-winning Netfinity servers, you can build a solid foundation for serving your customers on the Internet.

IBM PartnerWorld for Developers **[www.developer.ibm.com/welcome/ netfinity]** enables you to leverage your current application, data and operating system skills and experience so you can provide a solution your customers can trust for e-business.

> Note: The Linux information in this article was provided by Lenz Grimmer, an engineer on the Linux distribution development team with SuSE Germany. Lenz is currently working with the IBM International Technical Support Organization to produce a SuSE Linux Integration Guide for Netfinity servers. The completed redbook is available at **www.redbooks.ibm.com**
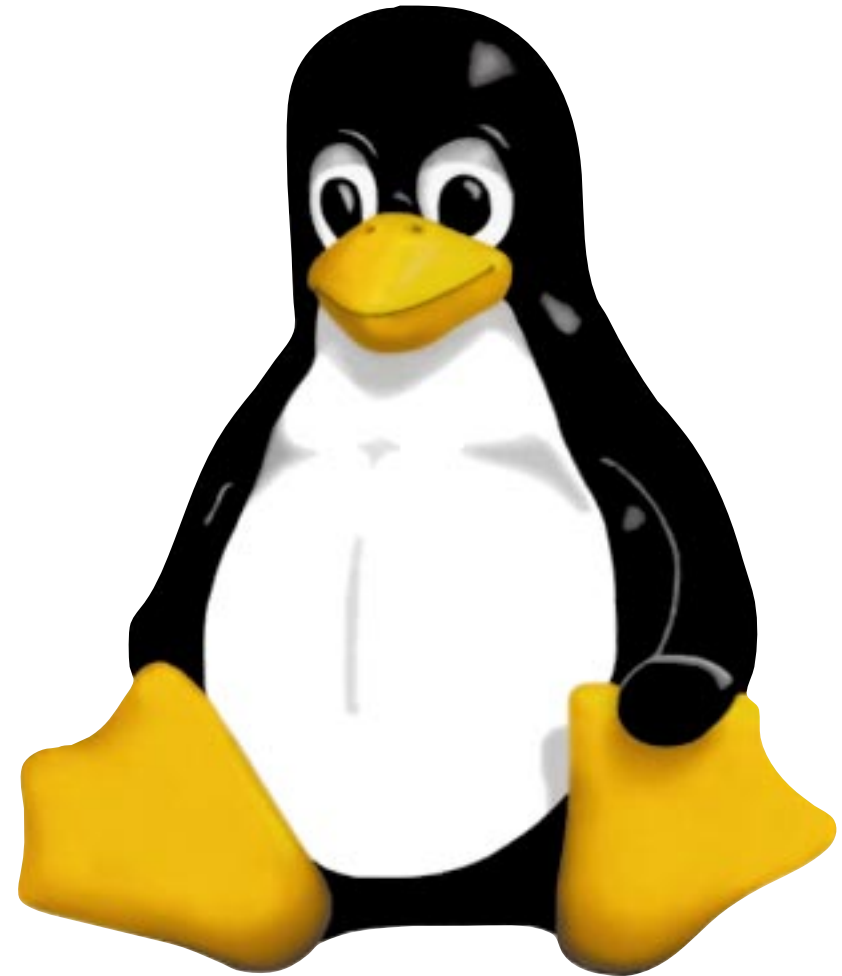
Security systems leaving you irked and plagued?

Finally, a solution that's open for trusted e-business

IBM SecureWay FirstSecure, Version 2

In July 1999, the Aberdeen Group reported that IS managers are "irked by the cost of maintaining security solutions across dispersed computing systems" and "plagued by increasing rates of viral infections, deluges of junk mail and worse."[1]
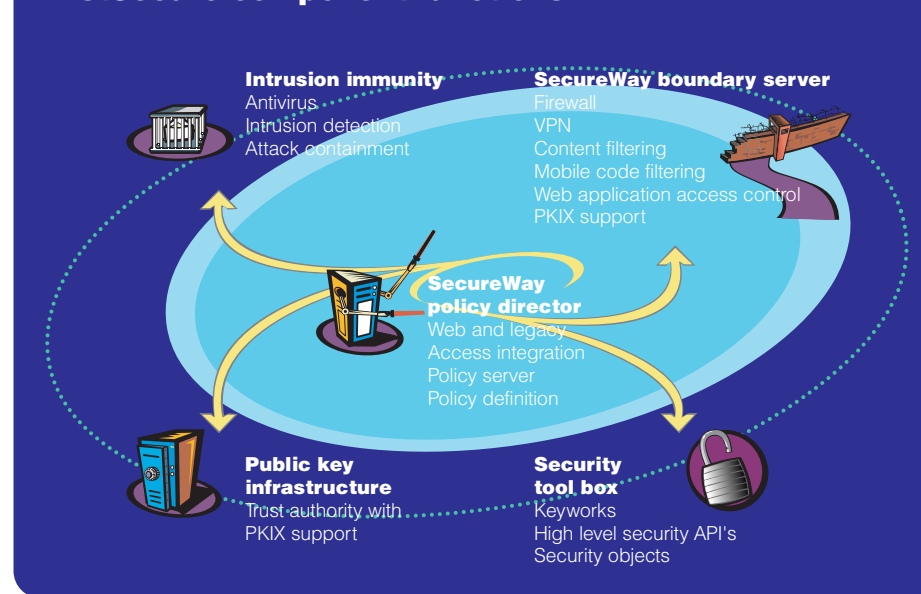
The report further states that IS managers are calling for a security solution that is "more integrated, easier to deploy, less costly and simpler to manage."

With the recent announcement of IBM SecureWay* FirstSecure, Version 2 **[www.ibm.com/software/security/firstsecure/developer]**, IS managers now can rest assured that the technology and the vision of centralised, integrated security is a practical reality. FirstSecure's integrated components powerfully combine authorisation and authentication for security that is easy to manage – opening the doors to conduct trusted e-business with customers, suppliers and partners on the Web.

Integration, control and functionality

"Easy-to-manage security is a critical step toward expanding e-business, enabling companies to build customer relationships as never before," says Mark N Greene, Vice President, IBM SecureWay Software. "FirstSecure helps you put technical issues backstage and focus on developing e-business to its full potential."

FirstSecure component functions

Intrusion immunity
Antivirus
Intrusion detection
Attack containment

SecureWay boundary server
Firewall
VPN
Content filtering
Mobile code filtering
Web application access control
PKIX support

SecureWay policy director
Web and legacy
Access integration
Policy server
Policy definition

Public key infrastructure
Trust authority with
PKIX support

Security tool box
Keyworks
High level security API's
Security objects

"IS decision-makers charged with exploiting new e-business relationships across the Internet will want to talk with IBM," says Jim Hurley, Managing Director of Security at Aberdeen Group. "IBM is one of the few suppliers that understands what is needed to safely and flexibly exploit the new electronic economy.

Moreover, with FirstSecure, the company possesses the capability of delivering against the customer requirements."

Centralised security for Web-based and existing applications

The 'brains' of FirstSecure are in its authorisation component, SecureWay Policy Director. From a central point, Policy Director can authorise and authenticate the individuals who are using your company extranet or Internet applications. Central control simplifies the implementation of security policy, to ensure that the right information reaches the right individuals – whether they be suppliers, customers or business partners.

IBM SecureWay Trust Authority, the FirstSecure authentication component, fully interoperates with Policy Director, allowing positive identification of people logged on to the network.

With a centralised, integrated approach to policy management, FirstSecure lets IS managers create a comprehensive shield against security exposures, while minimising the disruptions and costs commonly associated with incompatible components. The solution addresses key concerns of IS managers:

- Complexity – avoid having to make changes to many different security points when your company alters the security policy: You can make the changes in the FirstSecure central directory, and enforce those changes across distributed security points.

- Cost – sidestep writing extensive new security code for each e-business application you deploy: FirstSecure will extend and enforce access control at the level of your existing applications – independent of operating systems and Web environments.

- Implementation – management of security policy for multiple Web servers is simple: SecureWay Policy Director can manage the entire e-business infrastructure as if it were a single entity.

FirstSecure: Delivering the vision

FirstSecure is ideal for companies eager to overcome the IT hurdles of moving into advanced e-business by deploying an affordable, centrally managed security system based on integrated components. A few highlights:

- The authorisation component, SecureWay Policy Director, implements the latest standards of LDAP, aznAPI[2] and Public Key Infrastructure(PKI)[3] including PKIX, which lets one company's certificate authority recognise and work with digital certificates from other companies.

- The authentication component, Trust Authority, integrates functions that help to apply, issue and manage digital certificates. It has an advanced registration facility to automate certificate management, ensuring scalability, interoperability and investment protection.

- The firewall component uses the LDAP directory to store data, an important milestone for the security industry. When you define a user to the SecureWay Policy Director, that user ID is automatically defined for the firewall – it's not only clean, but a performance booster.

The intrusion-immunity component includes regular attack-signature updates from IBM's renowned research experts in the IBM Global Security Analysis Lab, so customers essentially have IBM's researcher working for them full-time.

The SecureWay Toolbox is enhanced to include practical examples to help you deploy FirstSecure, and support for LDAP, aznAPI, PKIX and Secure Sockets Layer (SSL).

Extending integration to the desktop level, FirstSecure also communicates with the recently announced IBM SecureClient, which provides security on a PC chip. When you set policies with SecureWay Policy Director, IBM systems with the SecureClient embedded security chip will enforce those rules.

IBM's strategic vision includes expanded application interoperability, such as the FirstSecure upcoming support for CORBA and IBM WebSphere* Application Server Enterprise Edition. IBM's recent acquisition of DASCOM, Inc., an industry leader in authorisation and access-control technology, further strengthens IBM's position to deliver a vision of centralised, integrated security.

Open for trusted e-business

IBM FirstSecure Version 2 helps IS managers transform security concerns into an asset: an enterprise that is truly open for trusted e-business.

For the entire solution, comprehensive FirstSecure Implementation Services are available, including an architecture and design workshop, strategic planning, installation and non-production testing.

Be among the first to reap the full competitive advantage of integrated security.

[1] *Aberdeen Group, Inc., The New Internet Guardians: Integrated Coverage, Better ROI. Boston, MA: June 1999.*

[2] *Formerly known as AUTHZ API*

[3] *Public Key Infrastructure for X.509 V3 (PKIX) is the most widely supported Internet standard for certificate authority interoperability.*

New edition of WebSphere supports EJB model

by Deb Smith, Team Leader, Java and e-business Enterprise Integration

WebSphere 3.0 now supports Enterprise JavaBeans, making it possible for developers to use EJB technology to develop exciting new applications. It's time to get your development teams working with EJBs now! Investments in building your skills now will pay off at deployment time in 2000.
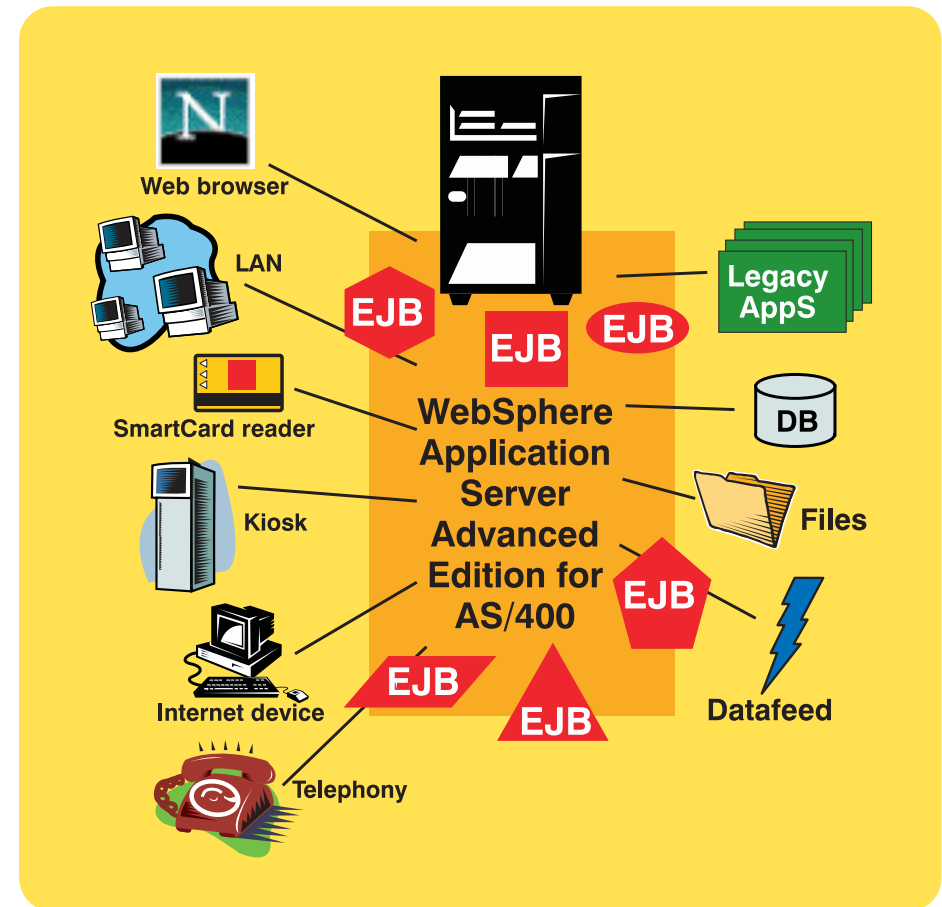
EJB and WebSphere defined

As you know from past issues of this newsletter, Enterprise Java Beans (EJB) are reusable, pre-packaged pieces of application code that can be combined with other components to create customised applications.

The EJB specification is emerging as the standard component model for application servers and the foundation of the e-business framework.

WebSphere is IBM's strategic Java Web application server. It "sits" on top of the HTTP server to provide an environment for running dynamic Web applications linked to DB2 Universal Database* for AS/400. The IBM WebSphere Application Server was created to allow developers to take advantage of the portability and extensibility of Java as they enable applications for intranets, extranets and the Internet.

WebSphere today

Available at no cost as part of the OS/400* license, WebSphere Application Server, Standard Edition V2.02 can be incorporated into e-business solutions today. WebSphere supports and executes Java servlets and Java Server Pages. It also includes application services for session and state management, enhanced administration and XML document Structure Services.

Web browser · LAN · SmartCard reader · Kiosk · Internet device · Telephony · EJB · WebSphere Application Server Advanced Edition for AS/400 · Legacy AppS · DB · Files · Datafeed

For added security, the *IBM WebSphere Application Server for AS/400* **[link to www.ibm.com/as400/websphere]** can be configured to run under a specific AS/400 user profile.

A native AS/400 user registry is provided for WebSphere-enforced security, which ties to AS/400 user profiles.

New with Advanced Edition

Starting January 2000, AS/400 application developers can use IBM WebSphere Application Server, Advanced Edition V3.0 to develop applications using EJB.

The new product, to be priced and packaged separately, will include support for Enterprise JavaBeans, compliant with the Sun EJB specification. Advanced Edition will provide a portable Java-based Web application deployment environment that supports and executes everything the Standard Edition does plus EJB 1.0 specification support for:

• Stateless and stateful session beans

• Bean-managed persistence

• Container-managed persistence

• Remote Method Invocation (RMI) client support

• XML, both as a development modelling standard and as a runtime data interchange standard.

Advanced Edition can host EJB components in a container which provides transaction, security and persistence support that makes development of server-side business logic considerably easier.

Session beans and entity beans are supported with container-managed persistence to DB2 UDB for AS/400 databases. It provides connectors for back-end support and is built on a CORBA 2.0 compliant IIOP infrastructure. With EJB, CORBA compliance is part of the package!

EJB specification supported

As previously mentioned, the EJB specification is the standard component model for application servers. EJB components are the building blocks of customised applications – all have complete access to data and applications. SunMicrosystems released the 1.0 specification for EJB in March 1998. Based on this specification, IBM will deliver support for the industry standard EJB programming model through WebSphere Application Server 3.0, Advanced Edition for AS/400.

A look into the future

WebSphere technology is fast becoming the strategic programming model for IBM and for AS/400. EJB technology is in its infancy right now, but we expect to see it mature quite rapidly.

At time of print, SunMicrosystems Enterprise JavaBeans Specification Version 1.1, draft 3, was in public review. (The next release is expected to feature connectors to existing systems and is tentatively scheduled for six to nine months after Version 1.1 is released.)

WebSphere's objective is to implement all of the Enterprise Java standards and comply with J2EE as it develops.

As it does, you'll be able to take advantage of the frameworks that IBM and key partners are building rather than reinventing those frameworks yourself. You can focus your programming efforts on business problems and finding that "killer app" for the Web.

The bottom line

EJB technology is becoming an indispensable model in application architecture design.

Now is the time to start developing using the WebSphere Application Server, Advanced Edition 3.0 for AS/400. When it matures in 2000, your business will be ready to deploy your application, giving you the competitive advantage in the next millennium.

Newest versions of WebSphere Application Server, Studio, Performance Pack and Performance Pack Cache Manager now available

Don't miss the new versions of IBM WebSphere **[www.ibm.com/software/ WebSphere]** software now available:

IBM WebSphere Studio, V3.0 is the most complete Web development product available today for developing and deploying your interactive Web sites, and recently won "Best of Show" for Web application development at Fall Internet World '99 – the largest event for e-business and Internet technology.

IBM WebSphere Performance Pack, V3.0 allows your Internet service provider (ISP) business or corporate enterprise to confidently host mission-critical Internet applications for its high-volume Web sites. It improves the scalability, availability and performance of your site.

IBM WebSphere Performance Pack Cache Manager, V3.0 is a standalone, proxy caching solution scaled to meet the caching needs of locations that support ten to fifty concurrent users.
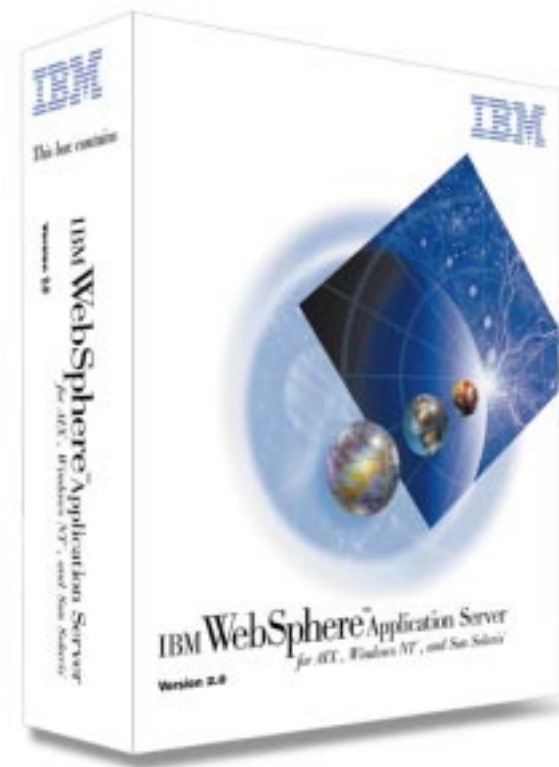
InstantQA Services: a proven methodology for enhancing software reliability

By Steven Angelo, Senior Vice President, Reasoning, Inc.

System downtime resulting from undetected software defects costs organisations over $85 billion a year, despite the billions of dollars spent on software testing and maintenance. To help enterprises and commercial software developers avoid the problems caused by software defects, Reasoning, Inc. **[www.reasoning.com]** offers *InstantQA* Services.

The InstantQA methodology combines automated code inspection technology, defect-database analysis, and Independent Verification & Validation (IV&V) by Reasoning's software quality specialists. An InstantQA service engagement produces a prioritised list of hard-to-find defects that can significantly impact the reliability of software applications.

Combining InstantQA Services and Traditional Testing

The most rigorous software testing has been proven to find only 85 per cent of all software defects. In many organisations, the percentage of defects found is much lower. The reasons for this shortcoming include the following:

• QA resources and schedules are limited

• Testing achieves limited code coverage

• Keeping test data and scripts current is difficult

These shortcomings are inherent to any quality assurance process that relies heavily on traditional black box testing. A better solution is to combine black box testing – which focuses on application functionality, with white box testing – which focuses on application structure – to obtain new levels of software quality and reliability.

InstantQA provides industry-leading white box testing through independent automated source code inspection services and offers the following benefits:

• Finds defects early

• Reduces development costs

• Lowers business risk

• Improves quality without taxing in-house resources

• Performs repeatable, automated quality control

• Finds the source of defects for faster repair.

The InstantQA Methodology

InstantQA is a flexible and repeatable service that has been developed using over 14 years of experience in the software quality and reliability marketplace.

InstantQA Improves software reliability by combining:

• Advanced Automated Source code Inspection (ASI) Technology

• Highly skilled software quality specialists

• Independent Verification and Validation (IV&V)

• Unique defect-tracking database analysis

• Flexible, client-focused inspections

• Automated, periodic re-inspections

• Identification of a wide range of software defects.

Using static analysis techniques, InstantQA is able to uncover defects that may be impossible to find through traditional testing methods. InstantQA identifies these defects in C, C++ and COBOL, including IBM VisualAge* COBOL applications. For example, InstantQA checks for Interface errors in COBOL applications that use CICS* extensions (for example, checking inconsistency between the actual length of a data area being passed and the length specified in the parameter list). InstantQA is offered as a service because it is flexible enough to incorporate additional client-specific and CICS-specific defect types during software inspection.

InstantQA identifies a wide range of software defects:

Defect Type	Examples
Assignment	Size truncations Loss of precision
Arithmetic	Divide by zero Data overflow
Client-specific	Currency conversion errors Failure to check Return-codes
Control flow	Empty while or if statements Misuse of boolean values
Dead code	Unused functions Unused files
Fragility	Deeply nested if statements Highly unstructured code
Initialisation	Use of uninitialised or partially initialised variables
Interface	Function parameter mismatches in size, number
Memory management	Memory leaks Accessing null pointers
Pointer management	Dereferencing invalid pointers Use of negative subscripts
Standard violations	Violations of naming or documentation rules

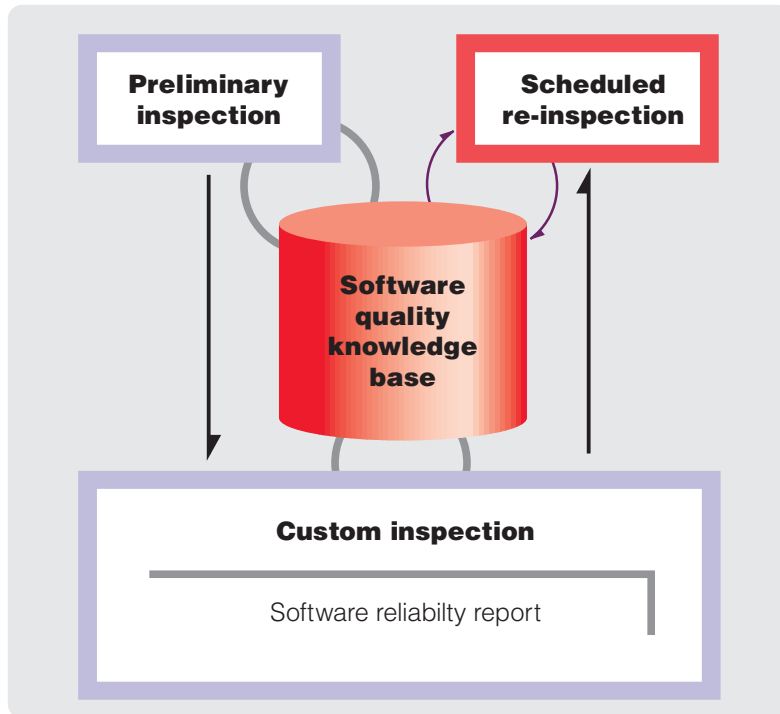## InstantQA at work

The InstantQA service engagement follows a three-phase methodology (see model below):

Phase 1: preliminary inspection
The inspection process starts with a source code analysis to identify occurrences of relevant defect classes that could cause application failure, data corruption, incorrect behaviour, or unpredictable results. If the client has a defect tracking database, then that is also reviewed using industry-standard Orthogonal Defect Classification (ODC) defect types, to determine problematic application behaviour and gain insight into potential defect classes to inspect.

Results from the preliminary inspection are presented in a summarised report form and provide a high-level software quality assessment of the entire application source code.

Phase 2: custom inspection
Reasoning's software quality specialists collaborate with the client's staff to identify and prioritise focus areas for the custom inspection. Areas of focus may include specific types of defects, compliance to corporate coding standards, and process improvements. Once agreement on the focus areas is reached, an iterative automated inspection of the client's source code is performed.

The goal of each iteration is to uncover and refine the defects most important to the client's organisation, while eliminating irrelevant defect information. A comprehensive Software Reliability Report is published at the conclusion of the custom inspection phase. The report provides recommendations for improving software reliability and reducing the risk of application failure.

Phase 3: scheduled re-inspection
Periodic re-inspections leverage the investment and knowledge gained in the initial inspection process to ensure applications remain defect-free during redevelopment and maintenance. Also, general software quality experience gathered by other Reasoning InstantQA engagements can be incorporated into the re-inspection process.

Summary

Reasoning offers InstantQA Services to help software development organizations produce highly reliable software faster and at a lower cost – without placing new demands on in-house IT departments. These services complement testing and are more accurate and scalable than manual or product-based software inspections.

OS/390 Web security:
latest features, functions, and development tools

by Ray Yatko

Today enterprises around the world are taking notice of e-business **[www.ibm.com/e-business/]**. In addition, many of these enterprises have begun to transform the way they do business to take advantage of e-business opportunities. One of the key elements that most enterprises look for when planning an e-business transformation is security. With OS/390* Web Security, enterprises and the developers **[www.ibm.com/developer/security/]** who create e-business applications have the opportunity to implement the robust security required in today's dynamic e-business environments. Technical Support from PartnerWorld for Developers **[www.developer.ibm.com/welcome/technical1.html]** is pleased to support OS/390 Web Security.

The latest S/390* and OS/390 **[www.s390.ibm.com/security/]** features, functions and tools that address Web Security provide strong hardware isolation functions and system integrity, system-level security, network-level security, and transaction-level security. These features, functions, and tools are made available to developers through both OS/390 Release 8 [Generally Available (GA) in September 1999] and OS/390 Release 9 [scheduled to be GA the end of March 2000].

The OS/390 security related products, services, and development tools available to developers in OS/390 Release 8 and Release 9 include support for Internet Key Exchange (IKE) and Protected User IDs, along with improvements to Server Digital Certificates, Client Digital Certificates, User-identity mapping, Directory Services, and a more secure Java** for OS/390 (part of the WebSphere Application Server Enterprise Edition for OS/390).

Another key update for OS/390 Web Security is the SecureWay branding of two key servers to align with the IBM SecureWay brand of products. The eNetwork Communications Server for OS/390 is now known as SecureWay Communications Server for OS/390 and the OS/390 Security Server is now known as the SecureWay Security Server for OS/390. IBM SecureWay software **[www.software.ibm.com/security/]** provides integrated directory, connectivity and security between users and applications for e-business in a networked world. IBM SecureWay software is supported on multiple platforms including OS/390.

The core enabling technology for secure e-business is digital certificates, which provide a basis for establishing secure sessions between partners in an e-business transaction. A crucial part of implementing digital certificates is managing the certificates used by server applications, and ensuring there is an uncompromised chain of trust. The SecureWay Security Server for OS/390 (in Release 8) provides functions to help manage server certificates and to help protect server private keys in a uniform way.

The primary application interface to these new functions is provided by Open Cryptographic Enhanced Plug-ins (OCEP), a new component of Security Server. The functions are incorporated into two plug-ins, one for data library services, and one for a trust policy manager. OCEP functions are to be used by applications complying with Common Data Security Architecture (CDSA) standard interfaces, which will help make it easier for developers to develop and port applications to the S/390 platform. It will also help customers apply consistent security rules to e-business applications that use digital certificates. For client certificates, OS/390 Release 8 gives users the ability to map groups of certificates to a RACF user ID based on criteria such as an application or system variable.

For User-identity mapping improvements in OS/390 Release 8, the Security Server provides the ability to associate RACF user IDs to Lotus Domino user IDs, which is used in the OS/390 WebSphere HTTP Connector to Domino function of Lotus Domino* for S/390. This improvement allows a Web user who has been authenticated with a certificate or RACF user ID by IBM HTTP Server for OS/390 to access Lotus Domino for S/390 without the need for a separate logon to Lotus Domino.

Also in Release 8, for Directory Services, the LDAP client and server will be distributed as fully enabled (no charge) portions of the Security Server. LDAP is a fast-growing technology for new network application development. It is a standards-based directory capability implemented with both LDAP Client and LDAP Server components on OS/390. In Release 8, the LDAP Server is being enhanced to support the LDAP Version 3 protocol. The OS/390 Release 8 LDAP Server is able to interoperate with LDAP clients on OS/390 and other platforms which support the V3 protocol.

Java for OS/390 (part of the WebSphere Application Server Enterprise Edition for OS/390) is now available at the JDK 1.1.8 level and contains significant performance and security enhancements over the product at the JDK 1.1.6 level. In addition to improvements in base Java performance, Java for OS/390 at the JDK 1.1.8 level offers enhanced scalability for multi-threaded applications. Like Java for OS/390 at the 1.1.6. level, the 1.1.8 level of the product provides native support for the IEEE floating-point hardware shipping with S/390 G5 and G6 machines. Using this support, some Java floating-point-intensive applications on OS/390 could run 100 times faster.

Security enhancements provide support for Java resource access authorisation checking through the OS/390 System Authorisation Facility (SAF) interfaces. They are designed to work with the Security Server (RACF) or equivalent. These enhancements, described on the Java for OS/390 Web site, are the first instalment of support that integrates Java security with our existing base system security. Java for OS/390 at the JDK 1.1.6 level continues to be supported for a limited time.

The OS/390 operating system is a dependable and secure operating system for e-business applications. OS/390 offers the required security and flexibility to move traditional applications into the next millennium and to grow new applications on a solid and secure infrastructure. Technical Support from PartnerWorld for Developers encourages developers to take advantage of OS/390 Web Security to get their e-business applications to market faster.

IBM Enterprise Information Portal : the window into your data and multimedia objects

By John A. Rodriguez

Web-based applications have become a standard way of transacting business and locating information. The Web is responsible for the explosive growth of many companies and industries, and the exponential growth of information. Many companies now manage a diverse number of transaction and warehouse data sites to support and accommodate their e-business applications. These companies have many other information and content data stores that cannot be accessed from existing Web-based applications.
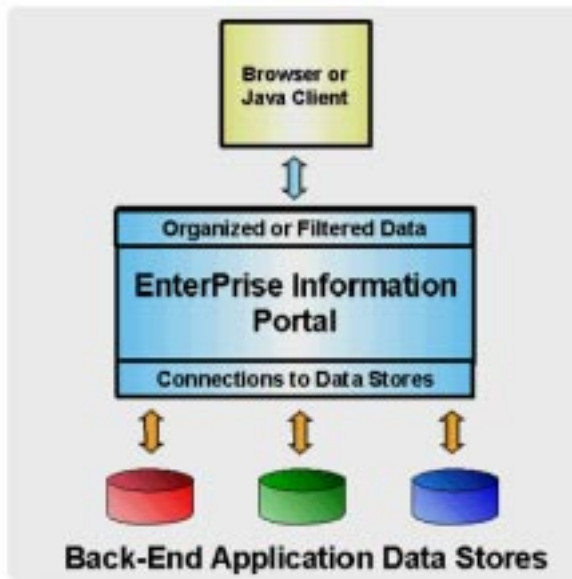
Click on image to view full screen version

With limited information technology resources, companies need a way to deliver the vast information stored in databases and content servers without having to write specific Web-based applications. How does an IT Manager respond quickly to the escalating demands for Web access to data generated over many years from dedicated applications and processes? For most the answer will come with the implementation of an EnterPrise Information Portal.

An EnterPrise Information Portal is a way of centralising access to numerous disparate data stores, categorising information, and delivering that information through a Web browser or Web-based applications. By implementing a portal, IT managers can provide an Internet gateway to any corporate database or data store used by dedicated applications. The portal addresses the demands of a Web user who requires a common access to application databases and unstructured data such as documents, images, and media objects. A company benefits by reducing the cost of locating information and the increased user productivity. Taking advantage of a portal that simultaneously searches many datastores and presents a consolidated list to the end user, provides end users with information they need, when they need it, to do their job.

The IBM portal solution
IBM's newly announced Enterprise Information Portal **[www.developer.ibm.com/pid_db2/eip.html]** builds on the strength IBM has in managing and accessing information. With the industries leading database, DB2 **[www.developer.ibm.com/pid_db2/index.html]**, and the top Content Management solutions in the EDMSuite (Enterprise Document Management Suite) **[www.developer.ibm.com/pid_edm/index.html]** and Digital Library **[www.developer.ibm.com/pid_db2/mam.html]**, the IBM Enterprise Information Portal provides a robust and flexible portal for accessing multiple data stores (also called content servers) containing structured and unstructured data.

Built on the concept of a federated data store, the IBM Enterprise Information Portal provides independent connectors for accessing and retrieving data from back-end content servers. Retrieved data is sorted and categorised, using schema mappings from the federated data store and then delivered to user based object oriented applications. An extensive set of Object Oriented (OO) Application Programming Interfaces (APIs) provided at the client service layer, gives the application developer the ability to build applications using C++, Java, or ActiveX. IBM Enterprise Information Portal also includes a number of visual and non-visual JavaBeans that gives an application provider facilities to quickly build a portal based application using the visual builder in a Java Integrated Development Environment (IDE). In fact, IBM Enterprise Information Portal ships a Java client built with the customisable JavaBeans. A "Thin Client" enabler that uses the non-visual JavaBeans is included to deliver content through an http server to a browser application.
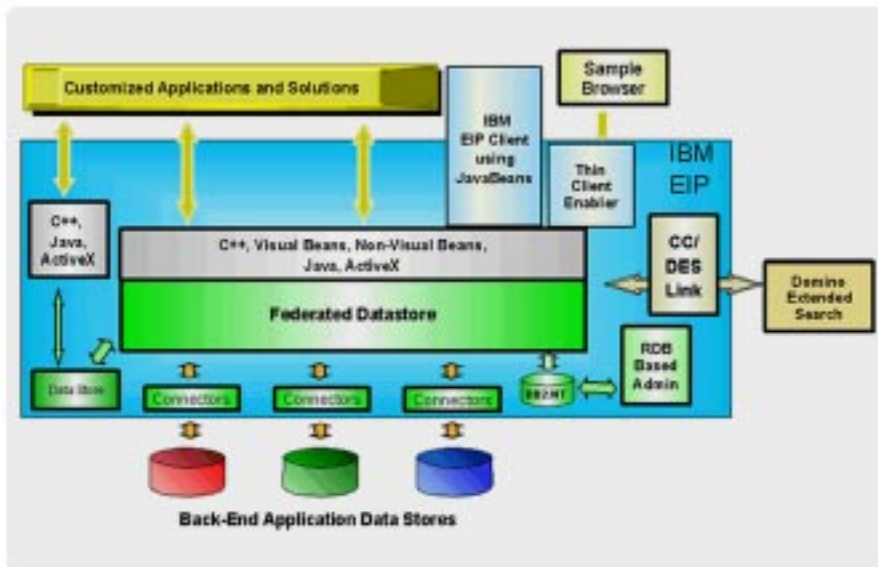
Click on image to view full screen version

IBM Enterprise Information Portal includes support for querying the vast install base of Lotus Domino servers. By linking to Domino Extended Search, queries can be performed against Domino servers at the same time queries are being performed against other data stores. The results (hit lists) are combined by the federated layer and made available to the end user application as a single list of entities. The user selects the items they would like to work with and the IBM Enterprise Information Portal retrieves the data and/or objects from the various data stores or content servers. The objects are delivered to the end-user application for processing.

The federated service layer

IBM Enterprise Information Portal uses the resources of DB2 databases for storing schema mapping information. The IBM Enterprise Information Portal System Administration program is used to define content servers, along with their available search fields or attributes. The System Administration program is used to create search templates containing federated attributes that map to each of the native attributes or indexes in the targeted content servers. The federated search templates provide a single set of searchable attributes to end user applications. The end user application retrieves search templates from the federated data store so users can formulate search requests. The user selects their search criteria and once submitted, the federated layer uses the mapping criteria to formulate simultaneous searches against the different content servers with the attributes required for that data store.

When the search requests have been serviced by each of the targeted content servers, the federated layer presents the list of items to the end user application, with the retrieved disparate attribute data mapped to the federated attributes. What the user sees is a list of items that appear to have come from the same content server.
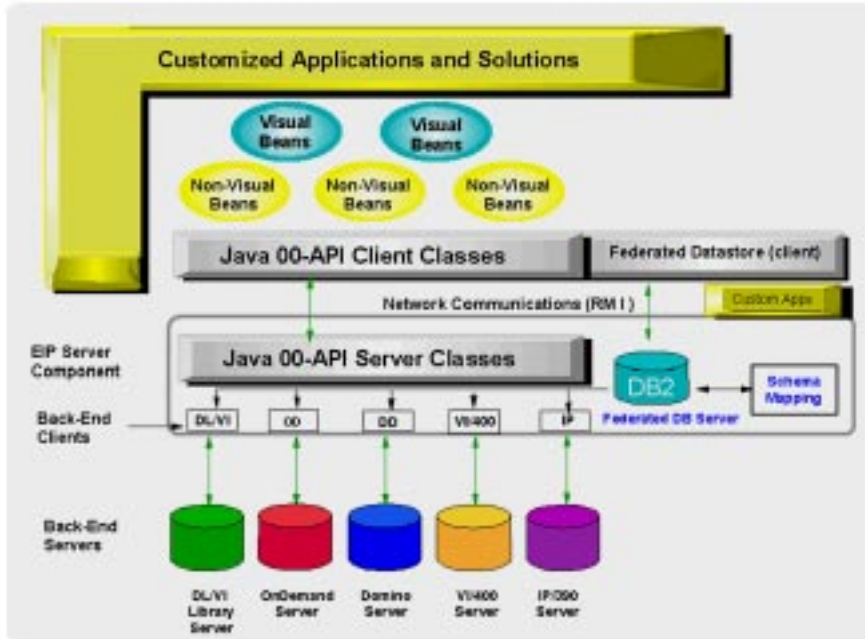
Click on image to view full screen version

Federated search connectors

In order for the federated search to work against a content server or back-end data store, a connector must be defined. The connector acts as a specific client class allowing access to the content server. In fact, a connector is also used to give applications access to the search templates stored in the federated data store.

With a defined connector, a query issued by a Web-based end user application can be performed against the native system. The connector handles interfacing with the native data store, mapping the interfaces required to perform a query, and returning the desired hit list. In EIP the connectors are contained in the runtimes for each of the defined Content Servers.

The initial release of the IBM Enterprise Information Portal provides connectors for the following content servers:

- IBM EDMSuite VisualInfo and DB2 Digital Library
- IBM EDMSuite VisualInfo for OS400
- IBM EDMSuite OnDemand
- IBM ImagePlus for OS/390
- Lotus Domino.Doc
- Lotus Domino Extended Search.

Additional content server connectors and runtimes can be defined by application providers.

Object Oriented API Service Layer

IBM Enterprise Information Portal provides a complete set of Object-Oriented (OO) Application Programming Interfaces (APIs) based on the open-object model. Application developers can use C++, Java (including javabeans), or ActiveX to implement IBM Enterprise Information Portal based query applications. IBM Enterprise Information Portal provides an implementation of the Dynamic Data Object (DDO) and its extension, the eXtended Data Object (XDO), which are part of the Object Management Group's (OMG) CORBA Persistent Data Services (PDS) protocols. IBM Enterprise Information Portal persistent software objects are called datastores and represent back-end content servers. IBM Enterprise Information Portal datastores provide user sessions, connections, transactions, cursors, and queries for accessing and manipulating data in the content servers.
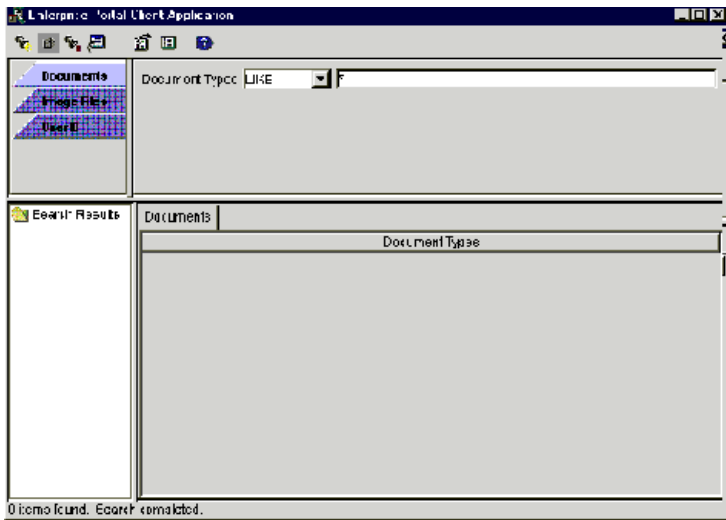
Although C++ and ActiveX can be used to build applications, application developers wanting to provide remote Web-based applications that access the federated capabilities of the portal will look to the Java OO-APIs or Java Beans. As the following picture shows using the Java interfaces allows one to use the Remote Method Invocation (RMI) interface so the client classes in the Java API can communicate with the server classes for manipulating data through the network. This means the runtimes for the content servers, containing the connectors, are stored and shared on an RMI server. The remote clients can call the runtimes on the RMI Server for accessing back-end content servers. This method simplifies the implementation for a Web-based application and reduces the overhead required for an IBM Enterprise Information Portal based end user application client.

JavaBeans and the IBM Enterprise Information Portal client

The IBM Enterprise Information Portal client was prepared using the Enterprise Portal non-visual and visual JavaBeans. JavaBeans are portable, platform-independent, reusable software components that provide models for how objects can be manipulated. EIP beans provide connection, data modelling, and a simple programming interface to Java OO-API client classes. EIP JavaBeans are Java Swing 1.1 compliant components allowing them to be used and customised within any Swing 1.1 compliant visual builder. Application developers can use the Java IDE visual builders to quickly build a Web-based query application.

The IBM Enterprise Information Portal non-visual beans provide the programming interface (more methods and properties) for applications, and are used for connection, data modelling, and service through the Enterprise Portal OO-API Classes to the federated service layer. The visual beans provide graphical user interface components for organising and displaying information returned by the IBM Enterprise Information Portal federated service layer through the non-visual beans. The following is a sample EIP application using the Java Beans.

Summary

IBM's EnterPrise Information Portal provides the query, consolidator, connectors, and object oriented application programming interfaces needed for implementing an Internet portal. When used in conjunction with IBM's Content Management products (EDMSuite VisualInfo, EDMSuite OnDemand, Domino.doc, and Digital Library) and IBM's DB2 Warehouse Manager, IBM Enterprise Information Portal provides an end-to-end solution for managing structured and unstructured information, and making it readily available to e-business applications.

Domino R5 embraces Java

by Jon Rush , Senior Software Engineer

If you like to use Java to develop your Lotus Notes applications, it's a lot easier with Domino R5!

With the new release 5.0 of Domino, the Designer **[www.lotus.com/ home.nsf/welcome/dominodesigner]** has been segregated out of the Notes client, allowing you to create Domino Java agents in one place. Building on past Domino Java enhancements, creating Java classes is now just another function of creating a Lotus Notes application.

Two development environments "under one roof"
Until now, the AS/400 programmer was required to utilise a program like VisualAge for Java to create and compile the Java class, and then use the Domino 4.6.x Designer to import this class file into the Domino database and application.

The programmer would have to know exactly what package of the Lotus Domino Object Model classes to import as well as what base class to extend and which methods to implement. Now, with Domino R5, Domino Designer controls the integration of Java classes within Domino applications — all the programmer has to focus on is creating the Java class.

New Designer screen
The top portion of the Designer screen (see screen capture below) is the section where we name our agent, define when it will run, and on what Domino objects it should operate. (You should recognise this from previous Domino 4.6.x releases.) The bottom two panels represent new functions with Domino R5.
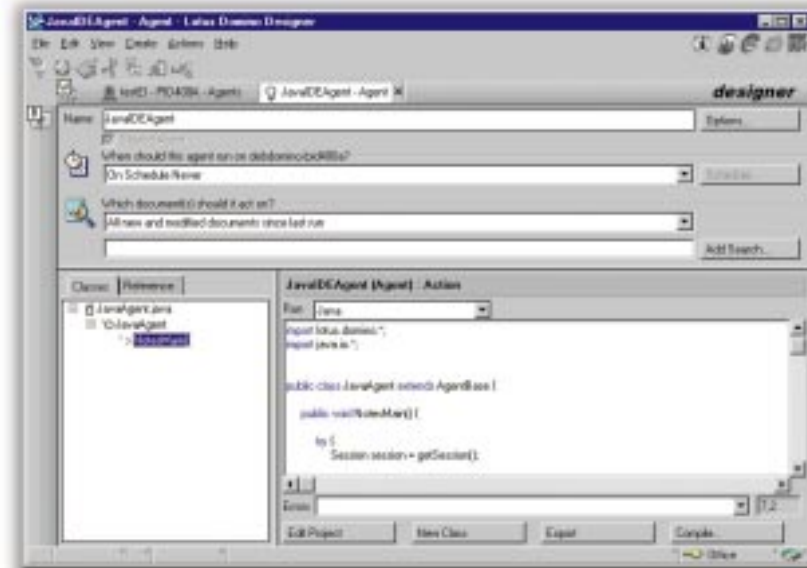
The new Java development environment with Domino R5

On the left...
The left panel shows the tree structure of the Java agent. You can click on the Reference tab and get context-sensitive information for each recognised programming language – including Java.

You select the desired topic from the Reference list and either:

• See the syntax for an event, method, or property, or

• Paste information from the Reference tab into the Script area.

For Java you will be able to view and paste core Java constructs and the Domino Object Model class constructs.

And on the right...
The right panel is the script panel where the Java source code is entered. When creating a new Java agent, Domino Designer provides a skeleton class (that extends the Domino Agent Base class and the Notes Main method that you will have to implement) and creates the logic the agent will execute.

The buttons at the bottom right allow you to Compile the Java agent you just created and edit if errors occur. The Export button will output the Java code into a .java ASCII file. The New Class button will create a new Java class skeleton in the script area, and the Edit Project button will allow you to add other class files or .jar files to this agent's project.

In summary, these enhancements to Domino R5 Designer significantly improve the processand capabilities for creating Domino Java agents and applications. For more informationsee the Help documentation that comes with the Domino R5 Designer tool.

Providing application hosting services on AS/400 white paper

The concept of delivering applications online as a service is growing at a phenomenal rate. Application Service Providers (ASPs) will provide these services to their customers through data centers with banks of servers connected to a variety of network access methods such as ISDN, dial up and Frame Relay; however, the most common connection will become the Internet. This white paper, _Providing Application Hosting Services on AS/400_ **[www.as400.ibm.com/developer/asp/papers.html]**, discusses some of the particular functional attributes of a server that make it most effective for serving in this market.

New redbook – how to replace OfficeVision/400 in your applications

In February 1999, IBM announced that OS/400 Version 4 Release 4 is the last release of the operating system that OfficeVision/400 and OfficeVision JustMail for OS/400 will support. IBM does not plan to enhance OfficeVision/400 or JustMail to support any future versions or releases of OS/400. This redbook **[www.redbooks.ibm.com/abstracts/sg245406.html]** describes Domino for AS/400 and AS/400 alternative services and APIs. It also provides several sample applications, including OfficeVision/400 sample applications, as a starting point. It is intended for use by those AS/400 customers, Business Partners, and software vendors who have developed applications that use the functions included in, or associated with, OfficeVision/400. It is also suitable for those who wish to develop similar new applications without previous experience with OfficeVision/400. You can view this redbook online or order hardcopy at the Web site provided above.

Check out our newest Internet-based Education courses

Register today for the following Internet-based Education courses (IBE) – Digital Certificates, Net.Data, Introduction to XML and more! These courses are intended to help you incorporate the latest technology into your AS/400 applications. For a complete learning experience; IBEs include graphics, speaker notes, audio, quizzes and Frequently Asked Questions. A complete listing of over fory IBEs are available at our Web site **[www.as400.ibm.com/developer/education/ibcs.html]**. Currently, these courses are available as a no charge offering.

Internet-based Presentations (IBPs)

Presentations and labs are now available from the Partners in Education (PIE) Summer School 1999. The presentations and labs range from beginning to advanced topics for people who are new and familar with AS/400. These courses range in topic from _AS/400 Basic Security, AS/400 Integration with Windows NT**, AS/400 Client Access: client administration tips_ and more! A complete listing of Partners in Education courses and other Internet-based Presentations is available at our Web site **[www.as400.ibm.com/developer/education/ibcs.html].**

IBM's Web Integrator Initiative

IBM understands that nobody knows your business like you do. Before building the Web Integrator Initiative **[www.ibm.com/software/webintegrators/emea]**, we surveyed the Web community and asked firms like yours to talk about their critical needs, four key objectives were identified and this initiative addresses them all.

As Business Partners, let's design and deliver world-class customer solutions, based in whole or in part on IBM offerings, to help our customers transform into 21st century e-businesses, which can help grow our profitability.

Please go to our Web site for further details and enrolment information.

The Expert Perspective

The Expert Perspective **[www.developer.ibm.com]** is a new monthly column for developers and software engineers that focuses on key IBM technologies, products and relevant technical topics. Articles include think-pieces, "how-to", future directions, and technology discussions. Our authors are high profileand very respected people within the technical community.

Java 2 Security information from Developer Connection

Looking for technical information on Web security? Recent issues of the IBM Developer Connection Technical Magazine **[www.developer.ibm.com/ devcon/mag.htm]** feature a series of articles on the Java 2 security model. "Applets and Java 2 Security," and "Implementing Custom Security Permissions in Java 2," were published in the June 1999 magazine. "On the trail of certificates in Java 2" was published in the September issue. The January 2000 issue features three articles: "Signing and verifying certificates in Java; The Security Migration Aid: Bringing Java 2 Security to Java 1.1.8"; and "Java Cryptography Part 1: Encryption and decryption."

The authors are application developers on the IBM Java Security project. Additional technical articles on Web security also are published on the Web site.

Accelerate your development efforts with PartnerWorld for Developers!

www.developer.ibm.com

PartnerWorld for Developers provides support and services to commercial software developers worldwide who build solutions using IBM technologies. The program can help you get solutions to market faster, lower your development costs and reach broader business opportunities.

Commercial members of PartnerWorld for Developers can take advantage of amazing benefits at no charge. The offerings include:

Business services to reduce your costs:

- Hardware Mall* discounts and low-cost leases on selected AS/400, RS/6000*, S/390 and Netfinity equipment.

- Software Mall* online ordering system, allowing members to obtain the latest versions of popular IBM software products at exceptionally low prices.

Technical services to accelerate your development efforts:

- Developer Support Online, delivering technical assistance via the Web, 24x7. Resources include FAQs & HATs, sample code, white papers and more.

- Developer Connection, your source for the latest tools and information for building e-business solutions.

  The Developer Connection is available to commercial members on the Web for download at no charge, or by subscription on CDs at media cost plus shipping.

- Worldwide Solution Partnership Centers (SPCs), giving you the resources to port and test your code across various IBM and non-IBM platforms in a single visit, at no charge!

Marketing services to showcase and sell your products: (more details in the next article)

- Listings in the Global Solutions Directory, an extensive online catalogue of applications, tools and services, providing worldwide exposure for your solutions.

- Solution Excellence awards, recognising commercial members who have developed outstanding e-business solutions. Winners in 9 different categories receive up to $30,000 in marketing and technical support!

Information services to keep you ahead of the curve:

- Solution Partnership Center technical briefings and hands-on workshops.

- Bi-weekly electronic newsletter with the latest IBM developer information, program discounts and offers.

- Web broadcasts, chat sessions, tradeshows and more!

  If you're not already a member of PartnerWorld for Developers, join now! There is no charge for membership. Register on the Web at **www.developer.ibm.com**

  * Access to offerings varies by geographic location. Restrictions may apply.

  Consult the Web site for details.

Help

Here are some simple tips which may make viewing and navigating easier.

Navigation
To read the Main Theme articles, just click on the headlines on the front page.

You can also use the toolbar in the top right-hand corner to navigate throughout the issue.

Weblinks
Where URLs appear in the text (highlighted in pale blue), just click on the box and your browser will open onto the relevant Web page.

To use the weblinks, you may need to configure your Acrobat Reader to your browser, this is in File-Preferences-Weblink (and locate your browser).

Legibility
You may have problems when viewing the text on smaller screens, particularly on laptops. To alleviate this, either press Escape and use the zoom icons in Acrobat Reader (pressing "Control+Shift+L" to return to Full Screen Mode), or click on areas of text to be guided through the article at a larger magnification.

Publishers note

IBM Developer News: Management Directions is a bi-monthly information service for commercial software developers, solution providers, system integrators and IT consultants. IBM Developer News: Management Directions is circulated in all major countries in Europe, Middle East, Africa, North America, Asia Pacific and Latin America.

You can submit contributions or comments to the editor at developernews@uk.ibm.com or write to IBM Developer News: Management Directions, PartnerWorld for Developers, Normandy House, PO Box 32, Bunnian Place, Basingstoke, RG21 7EJ, United Kingdom.

All material is copyright, so please contact the editor for approval to copy or quote from IBM Developer News: Management Directions.

Editor-in-Chief: Eileen Soriton
US and LA Editor: Sharnette Mitchell
Asia Pacific: Waqar Hasan

Continue receiving the information you need to develop e-business solutions by subscribing to our new customisable electronic newsletter, IBM Developer News.

Subscribe now at:
www.developer.ibm.com/news/newsletter_ann.html

IBM United Kingdom Limited
EMEA Marketing and Publishing Services
Normandy House
PO Box 32
Bunnian Place, Basingstoke
RG21 7EJ
United Kingdom

The IBM home page can be found on the Internet at www.ibm.com

IBM is a registered trademark of International Business Machines Corporation.

* Netfinity, DB2, SecureWay, WebSphere, DB2 Universal Database, AS/400, OS/400, VisualAge, CICS, OS/390, S/390, Hardware Mall, RS/6000 and Software Mall are trademarks of International Business Machines Corporation.

* Lotus Domino is a trademark of Lotus Development Corporation.

**Java is a trademark of Sun Microsystems, Inc.

**Windows NT is a trademark of Microsoft Corporation.

© International Business Machines Corporation 1999.

This document is the property of IBM and remains exclusively intended to observe IBM rules. No public diffusion authorised. The recipient of this letter is not authorised to diffuse or transmit this letter to whoever, without the express authorisation of IBM.

Browser or Java Client

Organized or Filtered Data

EnterPrise Information Portal

Connections to Data Stores

Back-End Application Data Stores

Back-End Application Data Stores
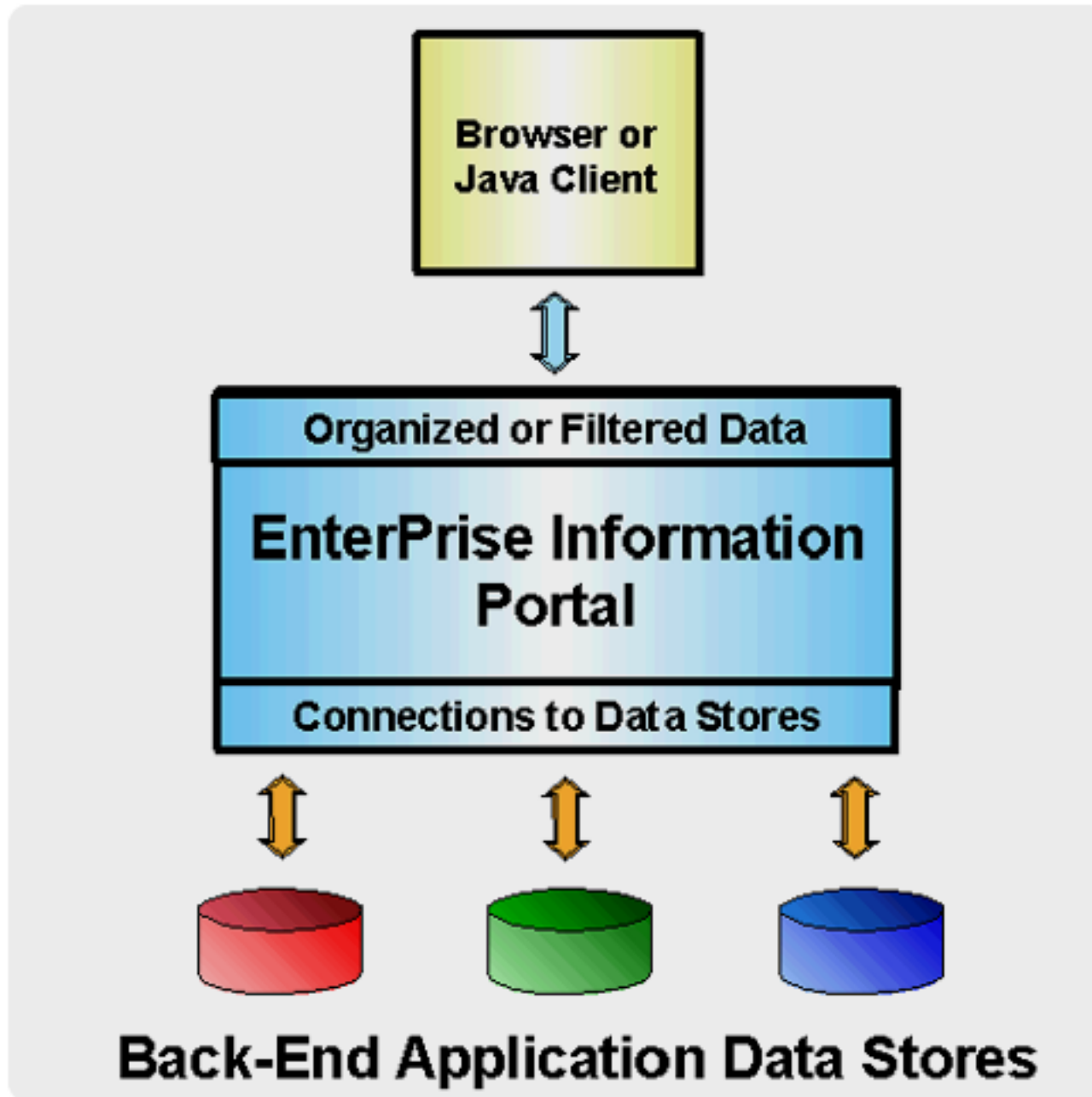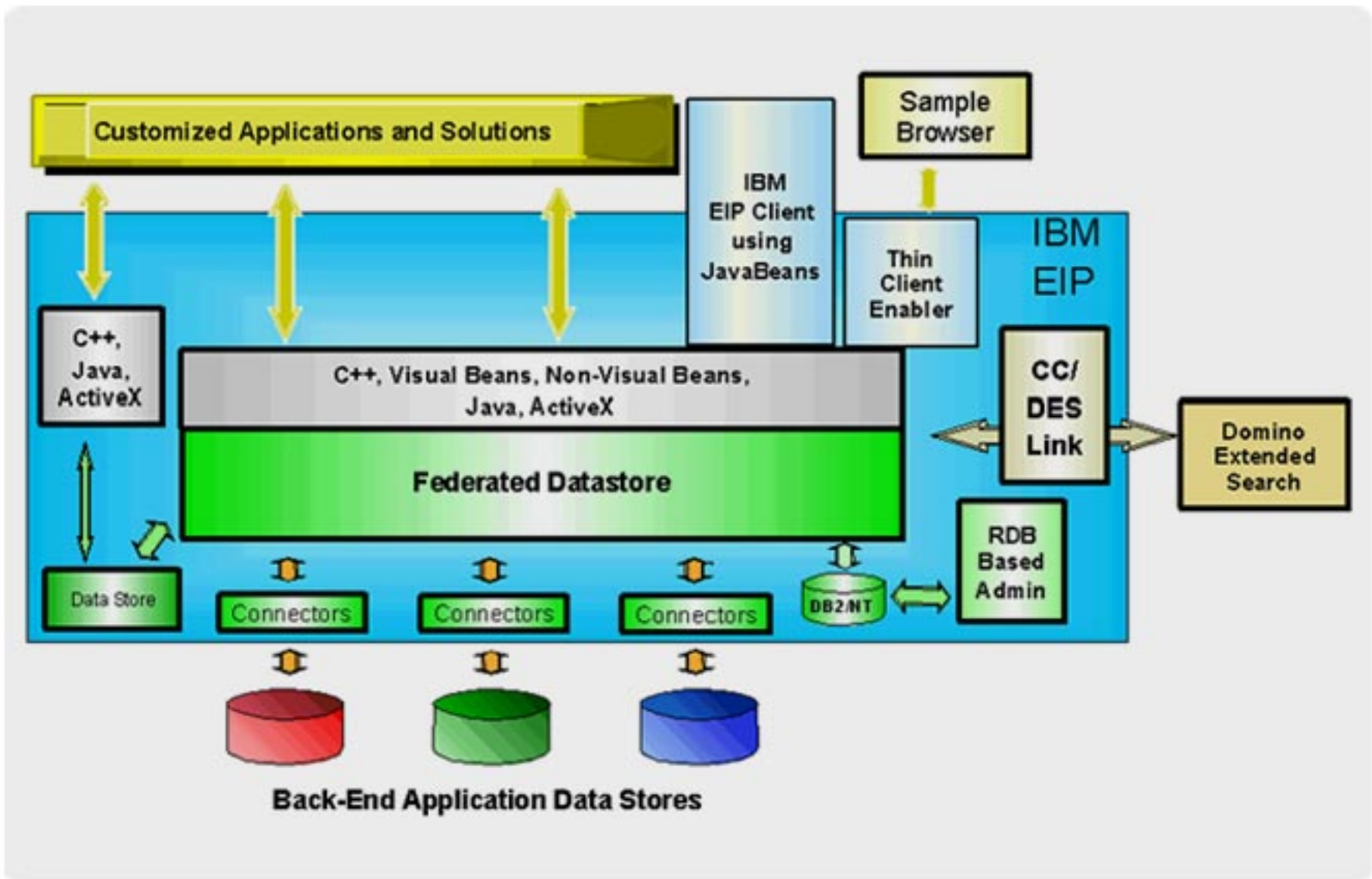
Click on image to return to article
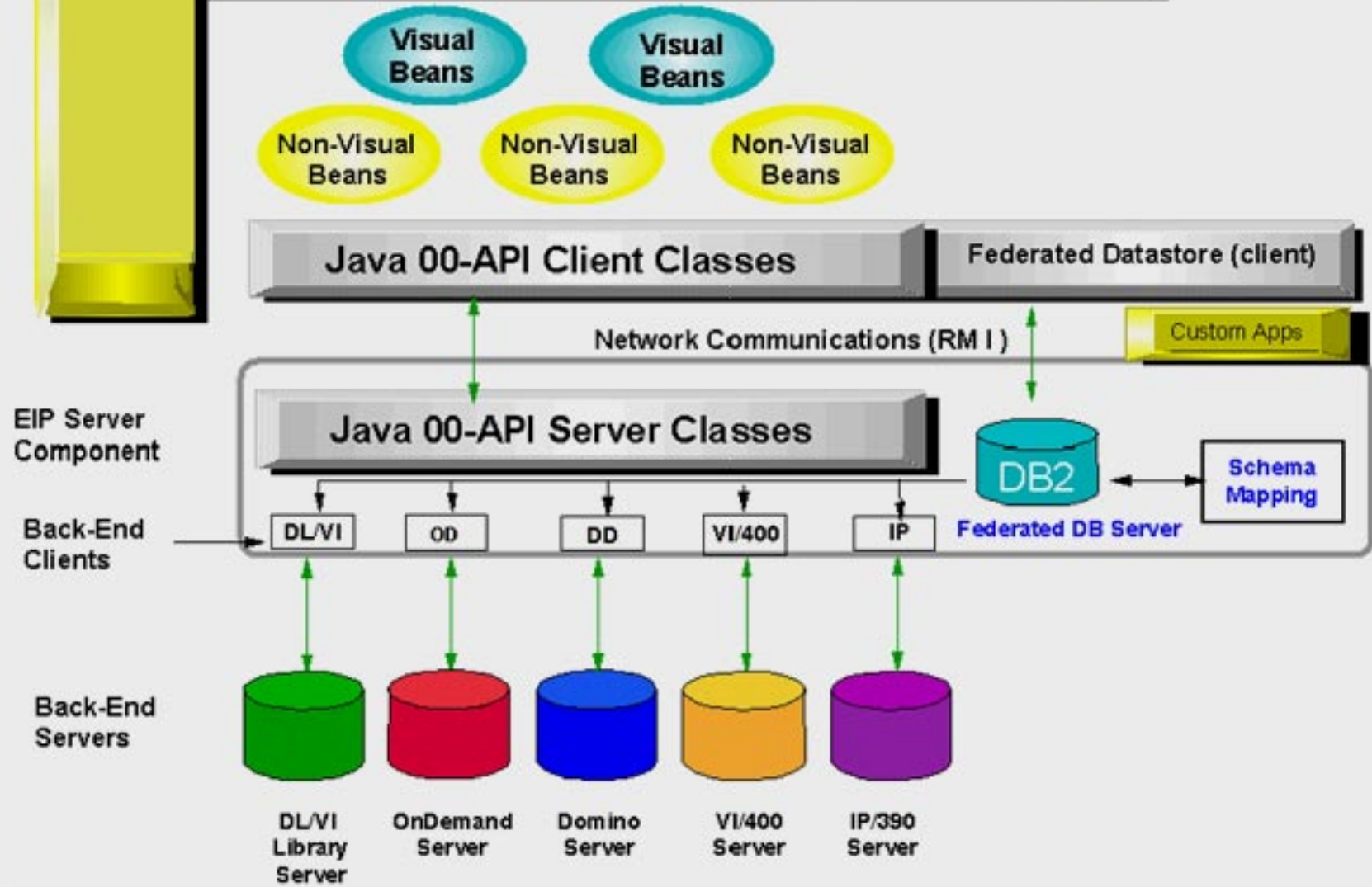
Click on image to return to article

FirstSecure component functions

Intrusion immunity
Antivirus
Intrusion detection
Attack containment

SecureWay boundary server
Firewall
VPN
Content filtering
Mobile code filtering
Web application access control
PKIX support

SecureWay policy director
Web and legacy
Access integration
Policy server
Policy definition

Public key infrastructure
Trust authority with
PKIX support

Security tool box
Keyworks
High level security API's
Security objects

Click on image to return to article