Service oriented architecture solutions
White paper

Tivoli software

Security and management for SOA environments.

August 2006

Contents

Overview

With increased demands for collaboration, integration and Internet-based services, today's organizations need to evolve their IT environments beyond silos of technical function and subject matter expertise. Specifically, each organization needs an IT infrastructure that enables people who are responsible for managing systems, databases and applications to work together efficiently, reliably and cost-effectively.

To meet these needs, many organizations are beginning to look at an infrastructure strategy based on service oriented architecture (SOA). Already used as an application integration strategy by organizations across a wide variety of industries, SOA provides an approach for integration – based on loose coupling, code reuse and standards-based interfaces – that effectively overcomes monolithic architectures and allows for more flexibility and change with less disruption. Functions that in the past were considered part of a business application or process, such as access control, can be exposed as services in an SOA environment – thus lowering the cost of developing new applications and, more importantly, of managing those environments in the future.

However, the open, diverse and heterogeneous nature of an SOA environment presents unique challenges in terms of security, ease of use and application management. To fully address these issues, a solution is required that spans all aspects of SOA, including federated identity management, message-level security, single sign-on (SSO), and service monitoring and management.

One of the first aspects where security is introduced is within the messaging middleware. Previously, a point-to-point security approach such as network security protocols like Secure Sockets Layer (SSL) or Transport Layer Security (TLS) was deemed sufficient. In today's SOA environments, end-to-end security techniques – including message-level security – are required, based on services spanning corporate and organizational boundaries. Securing the messages in SOA – as well as ensuring consistent application of message security policy – is of paramount concern.

Security concerns do not stop at the network or message level. A wide variety of not only security end points, but also security tokens, credentials and IDs must be managed as well. For example, a company may want to integrate with a number of business partners, but they use different identity credentials, including format, content and protection of credentials. Federated identity management provides secure integration, service delivery and data sharing among trusted providers of information and services without forcing one company to change its identity infrastructure in order to integrate with another. Single sign-on – a well-known benefit of federated identity management – enables users or service requestors to easily traverse among various Web sites and service domains – an important requirement for heterogeneous SOA environments. Federated Audit – the ability to reconcile user audits between applications and processes – is also an essential from an SOA compliance standpoint.

IBM products and services support end-to-end SOA solutions that provide the hardened security, ease of use and superior performance required for today's SOA environments.

Leverage the benefits of SOA

For today's organizations, "working better" means "working together." Mergers and acquisitions, increased cross-business and government collaboration, more outsourced services for users and greater user demand for online services are requiring that organizations find new ways to integrate applications, reuse existing assets, share information and exchange services across the Internet with partners, associates, suppliers and other organizations.

Properly implemented and managed, SOA environments enable organizations to:

- Collaborate with other organizations efficiently.
- Reduce the implementation and operational costs of adding or changing business services.
- Respond rapidly to dynamic business needs.
- Comply with government regulations.

Bridge the SOA security gap

Despite the obvious benefits of SOA, implementing an SOA environment can involve a number of challenges. First and foremost is the critical need for security. The very openness of an SOA environment – integrating formerly separate domains of authorization and control – requires management and protection of information across networks, security domains, services, components, platforms and business entities.

For companies, partners and suppliers connected across an SOA environment, SOA security must provide solid answers to questions such as the following:

- How do we identify and authenticate the service requester?
- How do we identify and authenticate the source of the message?
- Is the client authorized to send this message?
- Can we ensure message integrity and confidentiality?
- How can we audit access to Web services?
- How can we address all of the above — while still ensuring fast, easy service delivery for users?

In more specific terms, XML Web services can easily expose back-end systems to entities outside the firewall, but traditional security devices do not secure XML or Simple Object Access Protocol (SOAP) messages. For example, a SOAP request transmitted via HTTP tunneling bypasses the firewall, by design. XML Web services can also pose a high security risk because of the very fact that they occur in large volumes in many different places across the SOA environment, making them hard to track and monitor.

To provide adequate SOA security without sacrificing ease of use, organizations need a multilayer security solution that includes both federated identity management and message-layer security.

Highlights

Federated identity management

Federation can be defined as a business process that helps to simplify the integration and sharing of data between trusted providers of information and services. A federated identity is like a passport – a unique user identity that is recognized and honored among business partners.

A federated identity allows a user from one federation partner to seamlessly access resources from another partner in a secure and trustworthy manner. A federated identity system also enables an organization to share identity data about their users with trusted partners. Sharing identity data enables a partner organization to obtain information about a third-party identity (such as a customer, supplier or client employee) from that user's home organization. This helps to eliminate the cost and burden to the partner organization to create and manage identity data for the third-party user. It also accelerates the ability for partners to integrate.

In an SOA environment, federated identities simplify the linkage of services to users. This allows services in an SOA to have a unified view of the user accessing the service and use that information for role-based access control and audit. For users, federated identity provides them with SSO so they only have to sign on once to navigate among various Web sites, thereby improving their experience and streamlining the request and delivery of Web services.

Federated identity management enables large numbers of users and identities to be efficiently managed and provides a common way to network identities among different companies or applications

For organizations, a federated identity management system enables them to manage even very large numbers of users and identities in a secure, efficient and cost-effective manner. Federated identity management also provides organizations with a common way to network identities among different companies or applications, simplifying service integration, improving service and helping to reduce costs.

Reusing and extending legacy applications to support new business services is a key strategic objective of SOA. Today many clients are integrating their mainframe applications, including IBM CICS® and IBM DB2®, into an SOA using Web services. These applications are being used and reused in ways not previously imagined, including widespread connectivity to Internet-based clients. This brings with it a change in securing these applications. Mainframe security systems boast the time-proven IBM RACF® and IBM z/OS® security systems. However, these security systems were not intended to handle the multitude of possible access means (beyond the traditional 3270 "green screen"), including those where users provide their identification and authentication credentials to other entities and expect single sign-on to the mainframe security system. As federated identity management techniques are employed in these types of environments, it is imperative to achieve the appropriate balance between end-user usability and user administration usability. Federated Identity and Federated Audit techniques enable user authentication and access control at various points in a message flow and improve accountability by implementing identity propagation, with the appropriate audit recording, from the portal to the distributed application tier to the mainframe.

Message-level security

Message-level security ensures that the body of a message – where the data/request information is located – is protected throughout transit of the message, regardless of its routing, including routing through untrusted points such as routers or switches. Federated identity management supports trusted identities across disparate security domains, including message-layer protection. An additional layer of security is required that can parse, validate schema, encrypt and decrypt messages, and provide digital signatures for XML Web service transactions. This is often provided with a dedicated SOA appliance inside the firewall, ideally one capable of providing the wirespeed performance needed for real-world applications.

In short, the right SOA appliance should be able to:

- Simplify SOA deployments with minimal configuration, customization and management.
- Accelerate SOA transactions with faster XML throughput.
- Help protect SOA traffic by providing XML threat protection, Web services security functions, and integration with security and identity management software.

Ensure proper application management

SOA Web services are usually enabled by composite applications, which are deployed as partitioned business logic and data that span Web servers, Java™ 2 Enterprise Edition (J2EE™) application servers, integration middleware and mainframe systems.

Traditional tools only monitor individual processes, so they cannot handle problems involving composite applications. Organizations need SOA-specific tools that can identify and resolve performance bottlenecks in composite applications. These tools should also provide detailed analysis, complete application life-cycle management and integration support for other SOA tools and applications.

Take advantage of IBM security and management solutions

IBM is redefining the boundaries of SOA with a comprehensive portfolio of solutions to support hardened security, ease of use and superior performance for SOA environments.

IBM Tivoli® Federated Identity Manager supports the management of identities and provides users with simplified access to information and services.

IBM Tivoli Federated Identity Manager for z/OS is designed to enable mainframe applications to participate securely in an SOA. It provides a strong security bridge for distributed applications and mainframe applications by integrating with RACF to enable end-to-end identity propagation and secure

access to mainframe applications. As part of this support, the federated audit solutions provided by Tivoli Federated Identity Manager for z/OS support the auditing of identity mapping functionality used to provide the bridge between RACF and distributed identity management systems.

IBM WebSphere® DataPower® SOA appliances – a variety of easy-to-deploy network devices – help simplify, secure and accelerate XML and Web services.

IBM Tivoli Composite Application Manager for SOA facilitates the management of services through the environment by discovering, monitoring and managing the message flows.

IBM Tivoli Composite Application Manager for WebSphere – an application management solution – helps deliver high availability and performance across servers in an SOA environment.

A composite application is an application whose business logic and components span a variety of resources. Things like a Web server, application server, messaging backbone, a process server, a presentation server, legacy resources, applications and more are all types of components that a composite application may leverage in delivering business value.

These resources may also span across corporate or internal organizational boundaries. In some cases, it is necessary to traverse a variety of security domains in an efficient and secure fashion. When a message needs to traverse a variety of security domains, each of which may have different policies implemented for authentication, network security and so on, message-level security is required.

Support real-world SOA environments with IBM solutions

To better understand the real-world benefits of a security-rich SOA environment, we can consider a typical scenario in which an organization uses SOA and IBM solutions to deliver services to their customers in a protected, efficient and cost-effective manner.

Need:

A retailer provides its employees with health insurance. The employees need a fast, easy and secure way to check their policy profiles on the insurance provider's Web site. The insurance company needs an efficient way to authenticate employee identifications and respond to service requests in an efficient, secure manner. In addition, compliance reports are required to verify that sensitive insurance information has been provided only to properly authenticated and authorized employees.

Process:

An employee working for a retailer wants to receive a quote for one of the policies provided by her company. She logs in at the retailer's Web portal, entering her unique password and providing biometric identification through a fingerprint reader on a PC or laptop. **Tivoli Federated Identity Manager** authenticates her identity.

Once authenticated, she requests an insurance quote. This request is sent to the retailer's application server. From there, the retailer's identity server issues an authentication token for her to the insurance server through **Tivoli Federated Identity Manager**.

At this point, the retailer's application server sends the insurance company a Web service/SOAP request in a format consistent with the WS-Security standard. Inside the firewall at the insurance company's Web site, **IBM**

WebSphere DataPower XML Security Gateway XS40 intercepts, parses, validates, filters and decrypts the Web service request. The insurance company receives the request and security credentials validating the identity of the user. The insurance company then compares the user and her request against the authorization policy in **Tivoli Federated Identity Manager**, which validates that the user is properly authorized to receive the information requested. That done, the insurer then processes the request and sends the requested information to the retailer. The reply is again parsed, validated and filtered by **WebSphere DataPower XML Security Gateway XS40**, which then encrypts the reply for transmission to the employee.

A record of this service request and reply, along with others from the retailer's Web site, are recorded in compliance reports by **Tivoli Federated Identity Manager**. The reports are delivered to the retailer's chief information security officer (CISO) and auditor, providing a comprehensive audit trail of authentication and authorization as required by government regulations.

While all this is being processed, **Tivoli Composite Application Manager for SOA** monitors the traffic flow – from the initial request through the WebSphere DataPower appliance into the application server – to verify appropriate performance of the Web services, trigger events or situations when the environment is not operating in an optimal fashion, and provide subject matter expert tools to help analyze problems and determine their root causes.

Benefits with IBM solutions and SOA:

- SSO access to multiple Web pages and portals, both inside and outside the organization
- Enhanced end-user experience
- Audit capabilities across heterogeneous environments
- Support for key standards and specifications for federated identity management, such as WS-Security, SAML, Liberty, WS-Federation and WS-Trust
- Monitoring provided for all parts of the message flow

Highlights

IBM offers a variety of real-world SOA solutions to support an organization's security, enable ease of use and enhance performance

About SOA solutions from IBM

IBM is fully committed to providing real-world solutions for SOA environments. That is why IBM offers a variety of SOA software and appliance solutions that work together to support the high levels of security, ease of use and performance demanded by today's organizations.

For organizations that already have Tivoli Federated Identity Manager

WebSphere DataPower SOA appliances can add:

- Content-based routing, service-level management and proxy processing for WS-Trust.
- XML firewall and XML threat protection.
- Increased levels of security assurance such as HSM and packaging.
- Enhanced performance with support for SSL, XML, WS standards and SAML.

For organizations that already have WebSphere DataPower SOA appliances

Tivoli Federated Identity Manager can add:

- A centralized, Web-service, security-policy management server.
- Service to enforcement agents embedded in the application platform.
- Security-token service for use by other enterprise applications.
- The ability to add Java components for token translation or proprietary authentication.
- Proxy processing for WS-Trust, WS-Federation, Liberty Alliance ID-FF and SAML 1.x, 2.0.

Tivoli Composite Application Manager for SOA can add:

- Centralized monitoring and management of services through the environment.
- Integration with WebSphere DataPower SOA appliances for monitoring Web service flows, as well as Simple Network Management Protocol (SNMP) resource information through the Universal Agent.
- Integration with IBM Tivoli Service Level Advisor for the creation of historical service level agreement reporting on Web services.

For organizations that already have IBM SOA solutions

Tivoli Composite Application Manager for WebSphere can add:

- Simplified life-cycle management for applications.
- The ability to detect, analyze and repair performance issues quickly and effectively.
- Improved reporting through deep-dive analysis.
- Support for smooth integration with other IBM SOA products.

Tivoli Composite Application Manager for SOA can add:

- Centralized management of services through the environment.
- Integration of services management with resource and composite application management.

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes in order to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

For more information

To learn more about IBM solutions for SOA security and management, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
8-06

TAKE BACK CONTROL WITH Tivoli.

GC28-8455-00