Tivoli software

IBM Tivoli Federated Identity Manager

Highlights

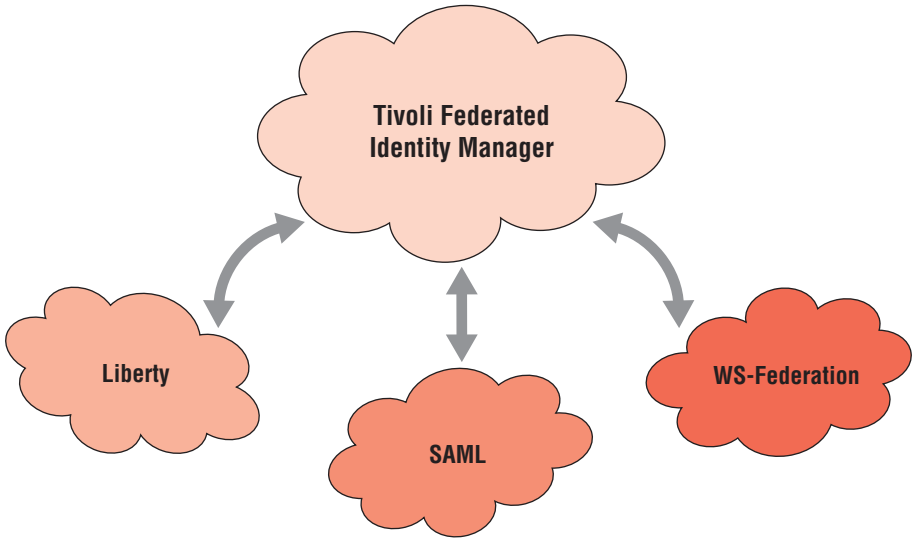
- Helps facilitate secure services transactions across mainframe and distributed environments
- Supports federated single sign-on (SSO) capabilities to help optimize user satisfaction and costs
- Supports a wide number of open standards and specifications, including Security Assertion Markup Language (SAML) 1.x and 2.0, Liberty Alliance Identity Federation Framework (ID-FF 1.x) and Web Services Security specifications (including WS-Federation, WS-Security and WS-Trust)
- Provides integrated audit data collection and reporting capabilities to help facilitate compliance with regulatory and business policies
- Helps optimize identity infrastructure investment and operational costs through federated drop-in capabilities

Businesses are increasingly challenged to extend critical information and data across company boundaries. Partners, customers, clients, distributors, agencies and suppliers require access to data sprawled across corporate human resources, customer relationship management (CRM), enterprise resource planning (ERP) and legacy mainframe systems.

As these integration and access needs grow, redundancies in processes often crop up — such as the proliferation of multiple logins — which can impact both productivity and user satisfaction. For example, customers who log on to the brokerage site of a full-service financial services company using one identity and password must use a different identity and password to log on to the credit card subsidiary of the very same financial services company. The company must then manage twice the infrastructure at twice the cost, while customers and employees are burdened with multiple logins.

To help manage the challenges of cross-enterprise information exchange, many organizations are moving beyond the traditional model of inflexible business processes to a more flexible, more accessible and reusable approach known as Web services. In contrast to a rip-and-replace approach, a service oriented architecture (SOA) is designed to make maximum use of new and existing IT assets.

Federated identity management can help you integrate and extend services across your business ecosystem while helping to minimize the risks associated with sharing identities and services. IBM Tivoli® Federated Identity Manager enables users to SSO to the sites of multiple businesses, while helping to preserve the confidentiality of their user data. Designed to minimize the



impact on business applications, Tivoli Federated Identity Manager can help you reduce costs and speed deployment timeframes for integrating applications within your collaboration infrastructure.

Handle a variety of standards with a single solution

One of the biggest challenges that companies face as they adopt federated identity management is the number of different federation standards. For example, the SAML, Liberty Alliance and WS-Federation standards utilize similar technologies but rely on different protocols and deliver different capabilities. By relying on open standards, you can simplify the integration of cross-domain services and limit redundancies across user accounts. And from an economic standpoint, you can leverage the security data of partners and benefit from a simplified operational model for authentication and authorization across your entire partner ecosystem — without superfluous investment. With very little additional investment on your part, you can greatly extend the content, corresponding business value and user attraction to your Web sites. Tivoli Federated Identity Manager can help provide a seamless, security-rich SSO experience for your users.

Tivoli Federated Identity Manager is designed to interoperate with the wide variety of federation standards that your partners and potential partners may employ. When you use Tivoli Federated Identity Manager, you deploy a solution that enables you to:

- Support the broadest federation functionality by enabling SSO, rich security customization and Web services security through SAML 1.1.x and 2.0, Liberty ID-FF and WS-Federation standards.
- Enable support for identity management across an SOA through the use of WS-Trust for identity and attribute exchange and transformation.
- Help simplify the integration of identity and security — including trust relationships between application platforms using WS-Security and WS-Trust.
- Communicate authentication and identification information about business partners through increased support for multiple security tokens — including PassTickets, x.509 certificates and Kerberos tokens.
- Automate the provisioning of user accounts and entitlements, using WS-Provisioning.

Enable SSO across your business ecosystem

As one of the first steps toward realizing the benefits of an SOA, federated SSO capabilities can help you speed time to value by integrating information from multiple domains at the user interface layer. Federated SSO protocols like SAML and WS-Federation provide standard,

interoperable means for multiple federation business partners to negotiate the presentation of credentials about a user from an identity provider to a trusted federation provider. Through SSO, users can navigate seamlessly among Web sites while maintaining a single logon identity and leverage aggregated views that deliver critical information in the context of the business process.

The benefits of SSO, such as increased productivity, improved satisfaction and lowered costs, can quickly be eroded if the SSO capabilities are not integrated with your business applications cost-effectively. For example, using proprietary application programming interfaces (APIs) can require extensive modifications to your applications that require a significant amount of time and money. At the same time, it can limit the flexibility you have to add federation relationships and protocols to meet evolving business requirements.

By leveraging the market-leading reverse proxy from IBM Tivoli Access Manager for e-business, Tivoli Federated Identity Manager lets you integrate a Web application through an HTTP/HTTPS connection. The loose coupling between the application layer and federated SSO functionality eliminates the need to use proprietary APIs — enabling you to connect a wide variety of Web applications into your federated environment with little to no change to your applications. Moreover, applications and their associated middleware and servers can be upgraded without any changes to the integration with the federated SSO services. Similarly, new federation relationships and protocols can be added with virtually no impact on the applications.

Hardware and software requirements

Supported platforms

- IBM AIX® 5.2 and 5.3
- Sun Solaris 9 and 10 SPARC
- Red Hat Enterprise Linux® Advanced Server (IA32) 3.0 and 4.0 for IBM System z™ and Intel® Architecture, 32-bit
- SUSE Linux Enterprise Server 9 for System z and Intel Architecture, 32-bit
- z/OS, Version 1, Release 6 and Release 7 (for WSSM component only)
- Microsoft Windows® Server 2003

Supported standards

- SSO and identity federation between identity providers and service providers using:
  - SAML 1.0, 1.1, 2.0
  - Liberty ID-FF 1.1, 1.2
  - WS-Federation
- Security token services using WS-Trust
- The following standard token types are supported in WS-Security headers of SOAP messages:
  - SAML tokens
  - Username tokens
  - X.509 tokens
  - Kerberos tokens
  - Binary tokens
- WS-Security token integrity using XML digital signatures
- WS-Security token confidentiality using XML encryption
- Federated provisioning support using WS-Provisioning
- Java™ Authorization Contract for Containers (JACC) for Java authorization
- Java 2 security support
- Open Authentication Reference Architecture (OATH)

Deploy policy-based access control

To enable you to fully leverage the user identities that you manage with Tivoli Federated Identity Manager, the software includes the same policy server as the award-winning Tivoli Access Manager for e-business. In addition to supporting your SSO initiatives, this policy server helps you define and administer security policies across your Web services as easily and consistently as for your enterprise's Web applications and portals.

Because the Tivoli Federated Identity Manager architecture enables you to evaluate business rules at run time — outside of a resource or application — you can modify parameters that influence access without rewriting and recompiling applications. In this way, the software helps you simplify management and respond quickly to changes in your business requirements and in your relationships with business partners and third-party users.

Federate Web services across heterogeneous application platforms

Just as Tivoli Federated Identity Manager provides a platform to simplify sign-on for user identities, the software also enables you to use the same platform to provide access to the Web services your company provides and consumes. Just as federated SSO protocols (such as SAML or WS-Federation) target browser-based passive-client approaches, Tivoli Federated Identity Manager enables the federation of Web services without requiring the tight coupling across identity repositories of partners and customers. Using the Tivoli Federated Identity Manager Security Token Service, you can provide the identity and attribute management required to expose a legacy application to a customer or partner without requiring changes to your application's internal user registry. For example, you can extend the security functionality across Web services platforms such as IBM WebSphere® Application Server, Microsoft® .NET and SAP NetWeaver. You can also:

- Rely on a single point of administration and management for internal and external Web services.
- Simplify the development of Web services that service heterogeneous application platforms.
- Rapidly and cost-effectively develop Web services by "delegating" the Web services security layer to Tivoli Federated Identity Manager.

From the Tivoli Federated Identity Manager console, you can configure the federation policies to enable capabilities that include partner enrollment, authentication and authorization credentials and policy mapping.

Manage identity flows across services

Reusing existing assets to lower costs and increase flexibility is one of the main benefits realized through an SOA environment. But as services are linked together into business processes, inconsistencies in user identities and their implementations can quickly derail an SOA initiative. Successfully dealing with these different user identities and identity exchange formats is critical to the success of an SOA.

Tivoli Federated Identity Manager provides a Security Token Service (STS) to help manage the complexities of passing user identities between services. Based on the WS-Trust standard, the STS can be invoked directly from applications or other middleware through the protocol defined by the WS-Trust standard. Through the STS, the security credentials of one partner or domain are transformed and exchanged in real time with the identity infrastructure of another partner

or domain. This allows you to simplify identity management and quickly integrate Web sites and application platforms — without needing to rip and replace an existing infrastructure.

As an additional layer of security, the security tokens, including PassTicket, x.509 certificates and Kerberos tickets, are themselves protected through digital signatures and encryption. The STS functionality can also be accessed from leading XML firewalls/gateways, including DataPower XS40 XML Security Gateway — one of the most widely deployed XML security gateways in the industry.

Help improve your ability to demonstrate business compliance

One of the key impediments to passing an audit and achieving compliance is the lack of accountability for granting user rights and permissions to access business systems. To aid compliance with regulatory requirements and corporate governance standards, Tivoli Federated Identity Manager provides an integrated audit data collection and reporting component.

Extend the value of your IBM System z investments

Tivoli Federated Identity Manager can help you derive greater value from extending legacy applications without sacrificing the ability to control access privileges — a critical element for both security and auditing purposes. To help companies verify that the right information is delivered to the right person, Tivoli Federated Identity Manager enables you to correlate an IBM z/OS® transaction to the user identity that initiated the transaction — which can help ease the burden of compliance with relevant regulations such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA) and Control Objectives for Information and related Technology (COBIT), along with other regulations and industry best practices.

The Tivoli Federated Identity Manager Security Token Service can also be used to map distributed user IDs to z/OS Security Server Remote Access Control Facility (RACF) user IDs and associated RACF PassTickets (one-time passwords for authentication to RACF). The RACF ID and PassTicket can then be used to connect to z/OS hosted resources using individual user identities. This enables fuller and more robust auditing of z/OS users and applications, ensuring that access to an organization's most expensive IT asset — its System z — is always safely monitored. The availability of Tivoli Federated Identity Manager component support on z/OS enables rich token support for Web services in environments involving WebSphere on z/OS.

Leverage open standards to consistently and securely provision users

Tivoli Federated Identity Manager enables you to provision identity accounts and entitlements across identity domains in a security-rich fashion, using WS-Provisioning. The software enables you to:

- Transmit and receive WS-Provisioning messages to and from partner identity management systems for user account provisioning.
- Verify security on WS-Provisioning messages you receive.

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage information technology (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 how Tivoli Federated Identity Manager helps you simplify user account management and optimize security by leveraging relationships with your trusted business partners, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/security

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

Produced in the United States of America
7-06

G507-1137-01