Tivoli software

IBM Tivoli Federated Identity Manager

Highlights

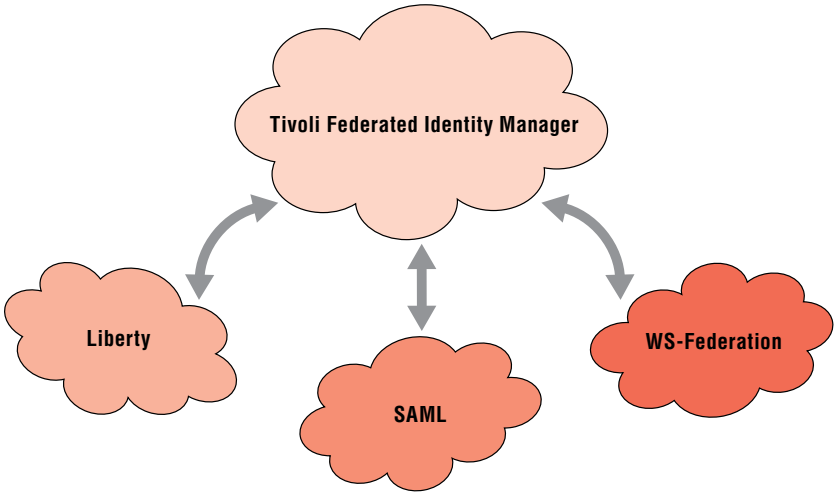
- Ermöglicht sichere Servicetransaktionen in Mainframe- und verteilten Umgebungen
- Unterstützt Single Sign-on (SSO) für eine höhere Benutzerzufriedenheit und niedrigere Kosten
- Unterstützt eine breite Palette offener Standards, einschließlich Security Assertion Markup Language (SAML) 1.x und 2.0, Liberty Alliance Identity Federation Framework (ID-FF 1.x) und Sicherheitsspezifikationen für Web-Services (darunter WS-Federation, WS-Security und WS-Trust)
- Ermöglicht die integrierte Sammlung von Prüfdaten und verfügt über Berichtsfunktionen, die Sie dabei unterstützen, gesetzliche und unternehmensinterne Richtlinien einzuhalten
- Hilft bei der Optimierung von Investitionen in die Identitätsinfrastruktur und senkt Kosten durch föderierte Drop-in-Funktionen

Unternehmen werden mehr und mehr dazu gezwungen, kritische Informationen und Daten auch über Firmengrenzen hinweg auszutauschen. Partner, Kunden, Auftraggeber, Distributoren, Agenturen und Lieferanten benötigen Zugriff auf Daten, die sich bei Mitarbeitern, in Customer-Relationship-Management- und Enterprise-Resource-Planning-Systemen oder auf traditionellen Mainframesystemen verteilt befinden.

Die zunehmenden Anforderungen an Integration und Zugriffsmöglichkeiten bringen oft Redundanzen bei Prozessen mit sich, wie etwa die Verbreitung mehrfacher Log-ins, die die Produktivität und die Zufriedenheit der Benutzer beeinträchtigen können. So zum Beispiel Kunden, die sich auf der Brokerage-Website eines Finanzdienstleisters mit einer Identität und einem Kennwort anmelden, eine andere Identität und ein anderes Kennwort verwenden, wenn sie sich bei der Kreditkartenabteilung desselben Finanzdienstleisters anmelden möchten. Das Unternehmen muss dann die doppelte Infrastruktur zu den doppelten Kosten verwalten, während Kunden und Mitarbeiter mit mehrfachen Log-ins belastet werden.

Zur besseren Bewältigung der Herausforderung des Austauschs von Informationen zwischen verschiedenen Firmen gehen viele Unternehmen über das traditionelle Modell unflexibler Geschäftsprozesse hinaus und verfolgen ein zugänglicheres und an Wiederverwendbarkeit orientiertes Konzept, das unter der Bezeichnung „Web-Services“ bekannt ist. Anders als bei einem Ansatz, der auf vollständige Ersetzungen mit hohem Aufwand setzt, geht es bei einer serviceorientierten Architektur (SOA) darum, neue und vorhandene IT-Ressourcen optimal zu nutzen.

Federated Identity Management kann Sie bei der Integration und Erweiterung von Services über die Grenze Ihres direkten Geschäftsumfelds hinaus unterstützen und gleichzeitig dabei helfen, die Risiken zu minimieren, die sich aus der gemeinsamen Nutzung von Identitäten und Services ergeben. IBM Tivoli Federated Identity Manager ermöglicht Benutzern die einmalige Anmeldung bei den Websites mehrerer Unternehmen und bewahrt gleichzeitig die Vertraulichkeit der Benutzerdaten. Tivoli Federated Identity Manager wurde entwickelt, um die Auswirkungen auf Geschäftsanwendungen zu minimieren und kann Ihnen dabei helfen, Kosten zu senken und Bereitstellungszeiten bei der Integration von Anwendungen innerhalb Ihrer Collaboration-Infrastruktur zu verkürzen.



Bewältigen Sie mehrere Standards mit einer Lösung

Eine der größten Herausforderungen, denen Unternehmen bei der Einführung einer Federated Identity Management-Lösung gegenüberstehen, ist die Anzahl unterschiedlicher Föderationsstandards. So verwenden beispielsweise die Standards SAML, Liberty Alliance und WS-Federation ähnliche Technologien, basieren aber auf unterschiedlichen Protokollen und stellen unterschiedliche Leistungsmerkmale bereit. Bei einer auf offenen Standards basierenden Lösung können Sie die Integration domänenübergreifender Services vereinfachen und Redundanzen für verschiedene Benutzerkonten begrenzen. Und aus wirtschaftlicher Sicht ist interessant, dass Sie die Sicherheitsdaten Ihrer Partner nutzen und von einem vereinfachten Betriebsmodell für die Authentifizierung und Autorisierung in Ihrer gesamten Geschäftsumgebung profitieren können – ohne überflüssige Investitionen. Mit nur sehr geringen Investitionen Ihrerseits können Sie den Inhalt, den geschäftlichen Nutzen und die Benutzerfreundlichkeit Ihrer Websites verbessern. Tivoli Federated Identity Manager kann Ihnen dabei helfen, Ihren Benutzern eine nahtlose und sichere Single Sign-on-Erfahrung zu ermöglichen.

Tivoli Federated Identity Manager kann mit der breiten Palette von Föderationsstandards arbeiten, die Ihre vorhandenen und potenziellen Partner möglicherweise verwenden. Wenn Sie den IBM Tivoli Federated Identity Manager verwenden, nutzen Sie eine Lösung, die Ihnen Folgendes ermöglicht:

- *Unterstützt umfassende Föderationsfunktionen mit Single Sign-on, funktionsreicher Sicherheitsanpassung und Web-Services-Sicherheit durch die Standards SAML 1.1.x und 2.0, Liberty ID-FF und WS-Federation.*
- *Ermöglicht die Unterstützung des Identitätsmanagements im Rahmen einer SOA durch die Verwendung von WS-Trust beim Austausch und bei der Übertragung von Identitäten und Eigenschaften.*
- *Vereinfacht die Integration von Identität und Sicherheit - einschließlich von Vertrauensbeziehungen zwischen Anwendungsplattformen, die WS-Security und WS-Trust verwenden.*
- *Übermittelt Authentifizierungs- und Identifikationsinformationen über Geschäftspartner durch verbesserte Unterstützung verschiedener Sicherheitstokens – darunter PassTickets, x.509-Zertifikate und Kerberos-Tokens.*
- *Automatisiert die Verteilung von Benutzerkonten und Berechtigungen mithilfe von WS-Provisioning.*

Single Sign-on in Ihrem direkten Geschäftsumfeld

Als einer der ersten Schritte zur Nutzung der Vorteile einer SOA können föderierte Single-Sign-on-Funktionen Ihnen dabei helfen, Realisierungszeiten dadurch zu verkürzen, dass Informationen aus mehreren Domänen auf der Ebene der Benutzeroberfläche integriert werden. Föderierte SSO-Protokolle wie SAML und WS-Federation bieten mehreren föderierten Geschäftspartnern standardisierte und interoperable Möglichkeiten, sich über das Vorweisen von Berechtigungsnachweisen zwischen einem Identitätsprovider und einem anerkannten Föderationsprovider zu einigen. Mit Single Sign-on können Benutzer mit einer Anmeldungsidentität nahtlos durch Websites navigieren und zusammengefasste Ansichten nutzen, die kritische Informationen im Kontext des Geschäftsprozesses liefern.

Die Vorteile einer einmaligen Anmeldung (SSO), wie etwa gesteigerte Produktivität, höhere Benutzerzufriedenheit und niedrigere Kosten, können schnell verspielt werden, wenn die SSO-Funktionen nicht in kosteneffizienter Weise mit Ihren Geschäftsanwendungen integriert sind. Wenn Sie zum Beispiel proprietäte Anwendungsprogrammierschnittstellen (APIs) verwenden, werden möglicherweise umfangreichende Modifikationen Ihrer Anwendungen erforderlich, die viel Zeit und Geld kosten können. Gleichzeitig kann dies Ihre Flexibilität bei der Hinzufügung von Föderationsbeziehungen und Protokollen zur Erfüllung stets neu auftretender geschäftlicher Anforderungen beeinträchtigen.

Durch die Nutzung des marktführenden Reverse Proxy von IBM Tivoli Access Manager for e-business ermöglicht Tivoli Federated Identity Manager Ihnen die Integration einer Webanwendung über eine HTTP-/HTTPS-Verbindung. Die lockere Verbindung zwischen der Anwendungsebene und der föderierten SSO-Funktionalität macht die Verwendung proprietärer APIs überflüssig. So können Sie eine breite Palette von Webanwendungen in Ihre föderierte Umgebung integrieren, ohne dabei große Änderungen an Ihren Anwendungen vornehmen zu müssen. Darüber hinaus können Anwendungen und die entsprechende Middleware und Server ohne Änderungen an der Integration mit den föderierten SSO-Services aktualisiert werden. Ebenso können neue Föderationsbeziehungen und Protokolle praktisch ohne Auswirkungen auf die Anwendungen hinzugefügt werden.

Hardware- und Softwarevoraussetzungen

Unterstützte Plattformen

- IBM AIX 5.2 und 5.3
- Sun Solaris 9 und 10 SPARC
- Red Hat Enterprise Linux® Advanced Server (IA32) 3.0 und 4.0 für IBM System z und Intel® Architektur, 32-Bit
- SUSE Linux Enterprise Server 9 für System z und Intel Architektur, 32-Bit
- z/OS, Version 1, Release 6 und Release 7 (nur für WSSM-Komponenten)
- Microsoft® Windows® Server 2003

Unterstützte Standards

- SSO- und Identitätsföderation zwischen Identitäts- und Service-Providern mit:
  - SAML 1.0, 1.1, 2.0
  - Liberty ID-FF 1.1, 1.2
  - WS-Federation
- Sicherheitstokenservices mit WS-Trust
- Die folgenden Standard-Tokenarten werden in WS-Security-Kopfzeilen von SOAP-Nachrichten unterstützt:
  - SAML-Tokens
  - Benutzername-Tokens
  - X.509-Tokens
  - Kerberos-Tokens
  - Binäre Tokens
- WS-Security-Token-Integrität mit digitalen XML-Signaturen
- WS-Security-Vertraulichkeit mit XML-Verschlüsselung
- Föderierte Einrichtungsunterstützung mit WS-Provisioning
- Java™ Authorization Contract for Containers (JACC) für die Java-Autorisierung
- Java 2-Sicherheitsunterstützung
- Offene Authentifizierungsreferenzarchitektur (Open Authentication Reference Architecture, OATH)

Auf Richtlinien basierende Zugriffskontrolle

Damit Sie die Benutzeridentitäten, die Sie mit Tivoli Federated Identity Manager verwalten, vollständig nutzen können, enthält die Software den gleichen Richtlinienserver wie die preisgekrönte Software Tivoli Access Manager for e-business. Zusätzlich zur Unterstützung Ihrer SSO-Initiativen hilft Ihnen dieser Richtlinienserver dabei, so einfach und konsistent Sicherheitsrichtlinien für Ihre Web-Services zu definieren und zu verwalten wie für die Anwendungen und Webportale Ihres Unternehmens.

Da die Architektur von Tivoli Federated Identity Manager es Ihnen ermöglicht, Geschäftsregeln während der Laufzeit zu bewerten – außerhalb von Ressourcen oder Anwendungen –, können Sie die Parameter ändern, die den Zugriff beeinflussen, ohne Anwendungen neu schreiben oder kompilieren zu müssen. So hilft Ihnen die Software bei der Vereinfachung der Verwaltung und bei der schnellen Reaktion auf Änderungen bei Ihren geschäftlichen Anforderungen oder bei Ihren Beziehungen zu Geschäftspartnern und Dritten.

Föderation von Web-Services über heterogene Anwendungsplattformen hinweg

Ebenso wie Tivoli Federated Identity Manager eine Plattform für die vereinfachte Anmeldung von Benutzeridentitäten bereitstellt, ermöglicht die Software Ihnen auch, die gleiche Plattform für den Zugang auf die von Ihrem Unternehmen bereitgestellten und verwendeten Web-Services zu nutzen. Und so wie föderierte SSO-Protokolle (wie etwa SAML oder WS-Federation) für browserbasierte Konzepte mit passiven Clients ausgelegt sind, ermöglicht Tivoli Federated Identity Manager die Föderation von Web-Services, ohne eine enge Verbindung zwischen den Identitätenquellen von Partnern und Kunden vorauszusetzen. Mit dem Sicherheitstokenservice von Tivoli Federated Identity Manager können Sie das Identitäts- und Eigenschaftsmanagement bereitstellen, das erforderlich ist, um einem Kunden oder Partner eine ältere Anwendung zur Verfügung zu stellen, ohne das interne Benutzerregistry Ihrer Anwendung ändern zu müssen. Sie können zum Beispiel die Sicherheitsfunktionalität über Web-Services-Plattformen wie IBM WebSphere Application Server, Microsoft .NET und SAP NetWeaver hinweg ausdehnen. Sie können auch:

- *Für interne und externe Web-Services einen einzigen Administrations- und Verwaltungspunkt nutzen*
- *Die Entwicklung von Web-Services für heterogene Anwendungsplattformen vereinfachen*
- *Web-Services schnell und kosteneffizient entwickeln, indem Sie die Web-Services-Sicherheitsebene an Tivoli Federated Identity Manager „delegieren“*

Von der Konsole von Tivoli Federated Identity Manager aus können Sie die Föderationsrichtlinien konfigurieren, um Funktionen wie die Registrierung von Partnern, die Authentifizierung und die Zuordnung von Autorisierungsnachweisen und Richtlinien zu aktivieren.

Verwaltung von Identitätsflüssen über mehrere Services hinweg

Die Wiederverwendung vorhandener Ressourcen zur Senkung der Kosten und zur Steigerung der Flexibilität ist einer der wichtigsten Vorteile, die eine SOA-Umgebung bietet. Aber da Services miteinander zu Geschäftsprozessen verbunden sind, können Inkonsistenzen bei Benutzeridentitäten und ihren Implementierungen schnell zum Misserfolg einer SOA-Initiative führen. Für den Erfolg einer SOA ist der korrekte Umgang mit den verschiedenen Benutzeridentitäten und den Austauschformaten für Identitäten von entscheidender Bedeutung.

Tivoli Federated Identity Manager bietet einen Security Token Service (STS) zur Unterstützung beim Umgang mit den Komplexitäten, die die Weitergabe von Benutzeridentitäten zwischen Services mit sich bringt. Der STS basiert auf dem Standard WS-Trust und kann direkt aus Anwendungen oder anderer Middleware heraus über das vom WS-Trust-Standard definierte Protokoll aufgerufen werden. Durch den STS werden die Sicherheitsberechtigungsnachweise eines Partners oder einer Domäne umgewandelt und in Echtzeit mit der Identitätsinfrastruktur eines anderen Partners oder einer anderen Domäne ausgetauscht. Dies ermöglicht Ihnen, das Identitätsmanagement zu vereinfachen und die Websites und Anwendungsplattformen schnell zu integrieren – ohne eine vorhandene Infrastruktur vollständig ersetzen zu müssen.

Die Sicherheitstokens, darunter PassTicket, x.509-Zertifikate und Kerberos-Tickets, sind als zusätzliche Sicherheitsebene selbst durch digitale Signaturen und Verschlüsselungen geschützt. Die STS-Funktionalität kann auch aus führenden XML-Firewalls/Gateways heraus aufgerufen werden, darunter DataPower XS40 XML Security Gateway – einem der am häufigsten verwendeten XML-Sicherheitsgateways der Branche.

Verbessern Sie Ihre Fähigkeit, die Einhaltung von Vorschriften zu demonstrieren

Eines der häufigsten Hindernisse beim Bestehen eines Audits und bei der Einhaltung von Vorschriften ist die fehlende Verantwortlichkeit für die Gewährung von Benutzerberechtigungen für den Zugriff auf Geschäftssysteme. Zur Unterstützung der Einhaltung gesetzlicher Vorschriften und unternehmensinternen Führungsstandards bietet Tivoli Federated Identity Manager eine integrierte Komponente zur Sammlung von Prüfdaten und zur Berichterstellung.

Erweitern Sie den Nutzen Ihrer IBM System z-Investitionen

Tivoli Federated Identity Manager kann Ihnen dabei helfen, mehr Nutzen aus der Erweiterung vorhandener Anwendungen zu ziehen, ohne auf die Kontrolle von Zugangsberechtigungen verzichten zu müssen – ein kritisches Element für Sicherheits- und Prüfungszwecke. Damit Unternehmen besser überprüfen können, dass die richtigen Informationen die richtigen Personen erreichen, ermöglicht Tivoli Federated Identity Manager die Korrelierung einer IBM z/OS-Transaktion mit der Benutzeridentität, von der die Transaktion ausgeht – hierdurch wird neben anderen Bestimmungen und bewährten Branchenverfahren die Einhaltung von Vorschriften wie Sarbanes-Oxley, dem Health Insurance Portability and Accountability Act (HIPAA) und den Control Objectives for Information and Related Technology (COBIT), neben anderen Bestimmungen und bewährten Branchenverfahren, beträchtlich erleichtert.

Der Tivoli Federated Identity Manager Security Token Service (STS) kann auch dazu verwendet werden, verteilte Benutzer-IDs mit Benutzer-IDs der z/OS Security Server Remote Access Control Facility (RACF) und zugehörigen RACF PassTickets (einmaligen Kennwörtern für die Authentifizierung bei RACF) abzugleichen. Die RACF-ID und das PassTicket können dann für die Verbindung zu von z/OS gehosteten Ressourcen mit individuellen Benutzeridentitäten verwendet werden. Dies ermöglicht eine vollständigere und stabilere Überprüfung von z/OS-Benutzern und -Anwendungen und stellt sicher, dass der Zugriff auf die wertvollste IT-Ressource eines Unternehmens – System z – stets sicher überwacht ist. Die Verfügbarkeit von Tivoli Federated Identity Manager auf z/OS ermöglicht einen umfassenden Tokensupport für Web-Services in Umgebungen mit WebSphere auf z/OS.

Nutzen Sie offene Standards zur konsistenten und sicheren Einrichtung von Benutzerkonten

Tivoli Federated Identity Manager ermöglicht Ihnen die sichere Einrichtung von Identitätskonten und Berechtigungen über Identitätsdomänen hinweg mit WS-Provisioning. Die Software ermöglicht Ihnen:

- *Die Übertragung und den Empfang von WS-Provisioning-Nachrichten an und von Identitätsmanagementsystemen Ihrer Partner zur Einrichtung von Benutzerkonten*
- *Die Überprüfung der Sicherheit anhand von WS-Provisioning-Nachrichten, die Sie erhalten*

Tivoli-Software von IBM

Tivoli Software von IBM unterstützt Unternehmen bei der effizienten Verwaltung von IT-Ressourcen, -Aufgaben und -Prozessen, um den sich ständig ändernden geschäftlichen Anforderungen gerecht zu werden, eine flexible und reaktionsschnelle Verwaltung von IT-Services zu ermöglichen und gleichzeitig die Kosten zu senken. Das Tivoli-Portfolio umfasst Softwarelösungen für die Bereiche Sicherheit, Compliance, Speicherung, Leistung, Verfügbarkeit, Konfiguration, Prozesse und IT-Lebenszyklus-Verwaltung. Gestützt wird dies durch die weltweit erstklassigen IBM Leistungen in den Bereichen Services, Support- und Forschungsleistungen.

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Tivoli Federated Identity Manager Ihnen bei der Vereinfachung der Benutzerkontenverwaltung und bei der Optimierung der Sicherheit durch Nutzung der Beziehungen zu Ihren vertrauenswürdigen Geschäftspartnern helfen kann, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/tivoli/solutions/security

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Hergestellt in den USA
07-06

G507-1137-01-GE