Höhere Kundenzufriedenheit und bessere Zusammenarbeit in und zwischen Unternehmen durch benutzerorientiertes, föderiertes Identitätsmanagement

Tivoli® software

IBM Tivoli Federated Identity Manager

Highlights

- ***Einfache Integration von Anwendungen durch Unterstützung einer Vielfalt an Formaten von Benutzer-Credentials sowie sicherer Informationsaustausch zwischen sich vertrauenden Geschäftspartnern oder Abteilungen innerhalb eines Unternehmens***
- ***Mehr Benutzerkomfort durch Einrichtung eines benutzerorientierten, föderierten Single Sign-on (SSO)***
- ***Einrichtung eines Identitätsdienstes, mit dem das Konzept von Benutzeridentitäten in SOA- und Web-Service-Umgebungen eingeführt werden kann***
- ***Nutzung offener Standards und Spezifikationen für eine bessere Zusammenarbeit im gesamten Geschäftsumfeld***
- ***Vereinfachung der Integration der Anwendungssicherheit, insbesondere Unterstützung verschiedener Servervarianten für den Erstkontakt (Point-of-Contact-Server)***
- ***Standardversion plus z/OS-Version und Einstiegsvariante, die eine kostengünstige Zusammenarbeit auch mit Geschäftspartnern aus dem Mittelstand ermöglicht***

Der Austausch geschäftskritischer Informationen über die Grenzen von Unternehmen hinweg – mit Kunden, Lieferanten und Geschäftspartnern – ist im von raschen Veränderungen geprägten Umfeld von heute ein Muss. Die Endbenutzer erwarten, dass sie Zugriff auf alle Services eines Unternehmens über eine einzige Schnittstelle, mit nur einem Benutzernamen und einem Kennwort erhalten. Doch die Verbreitung von serviceorientierten Architekturen (SOA) und Web 2.0 schafft neue Herausforderungen in puncto Identitätsmanagement und Compliance. Die Onlinezusammenarbeit und das Management von Benutzer- und Serviceidentitäten im gesamten Geschäftsumfeld stellen enorme Anforderungen an die IT-Infrastruktur eines Unternehmens. Angesichts der ständig steigenden Menge wichtiger Informationen, die sich in unterschiedlichen Sicherheitsdomänen befinden, verspricht die Verwendung von Verfahren für föderiertes Single Sign-on (SSO) zur Integration dieser Informationen rasche Vorteile und Einsparungen.

IBM Tivoli Federated Identity Manager unterstützt Sie bei der Einrichtung eines Frameworks für das Identity-Trust-Management, damit Sie stets genau wissen, welche Benutzer auf Ihre Services zugreifen und welche Berechtigungsnachweise sie dafür verwenden. Tivoli Federated Identity Manager gibt die jeweils erforderlichen Berechtigungsnachweise durchgängig weiter – von einem Point-of-Contact-Server über einen Enterprise Service Bus (ESB) bis hin zu einem Back-End-Mainframesystem. Diese Software unterstützt parallel die führenden Protokolle für föderiertes Single Sign-on: Security Assertion Markup Language (SAML) 1.0/1.1/2.0, Liberty Identity Federation Framework (ID-FF) 1.1/1.2 und Web Services Federation (WS-Federation). Dadurch können die Benutzer auf die unterschiedlichsten Systeme verschiedener Unternehmen zugreifen, wobei die Vertraulichkeit der Benutzerdaten gewahrt bleibt

Tivoli Federated Identity Manager bietet zwei zentrale Funktionen:

- ***Föderiertes Single Sign-on***
  Steigerung der Benutzerproduktivität und Förderung des Vertrauens durch Möglichkeit der einmaligen Anmeldung (Single Sign-on) an voneinander unabhängig verwalteten Systemumgebungen
- ***SOA-Identitätsservice***
  Senkung der Administrationskosten, Aufbau von Vertrauensbeziehungen und Erleichterung der Einhaltung geltender Vorschriften durch Management, Anpassung und Weitergabe von Benutzeridentitäten

Dank dieser leistungsstarken und modularen Funktionen ermöglicht Tivoli Federated Identity Manager vertrauenswürdige, einfache und nachprüfbare Interaktionen zwischen Partnern, durch die sich zentrale Compliance-Probleme im Zusammenhang mit dem Zugriff von Partnern aus anderen Domänen lösen lassen. Tivoli Federated Identity Manager minimiert den Anpassungsbedarf Ihrer Geschäftsanwendungen bei deren Öffnung für externe Zugriffe. Dies reduziert die Kosten und beschleunigt die Implementierung einer Integration von Anwendungen für die Onlinezusammenarbeit. Nutzen Sie die Software, um folgende Ziele zu erreichen:

- *Unterstützung umfangreicher Föderationsfunktionen durch Möglichkeit der einmaligen Anmeldung, umfassenden Sicherheitsanpassung und Web-Service-Sicherheit*
- *Einführung von Identity-Awareness in Ihrer SOA- und Web-Service-Umgebung*
- *Einfachere Integration von Identität und Sicherheit*
- *Weitergabe von Authentifizierungs- und Identifikationsdaten über Geschäftspartner durch Unterstützung von verschiedenen Formaten von Security-Tokens*
- *Automatisierte Registrierung von Benutzeraccounts und Berechtigungen*

Umstellung auf das benutzerorientierte Identitätsmanagement

Vertrauen zwischen allen an einer Transaktion beteiligten Parteien ist von entscheidender Bedeutung. Heute ist dieses Vertrauen jedoch angesichts der kontinuierlichen Zunahme von Identitätsdiebstählen und weiteren Betrugsfällen immer mehr gefährdet. Die für das Identitätsmanagement zuständigen Mitarbeiter müssen einen Wandel vom unternehmensorientierten zum benutzerorientierten Identitätsmanagement vollziehen. Beim benutzerorientierten Identitätsmanagement können Kunden, Partner und Lieferanten die Vertrauensbestätigung selbst steuern und außerdem selbst bestimmen, wo die Anmeldung stattfindet und welche Benutzerattribute der Identitätsprovider an einen Service-Provider weitergeben darf.

Tivoli Federated Identity Manager geht über herkömmliche Lösungen für das Identitätsmanagement hinaus. Die Software unterstützt das benutzerorientierte Identitätsmanagement durch die Verbindung mit Frameworks auf der Basis offener Standards, z. B. OpenID und Information Card Profile, und nutzt Identitätsselektoren aus Microsoft® Windows® CardSpace und dem Higgins Trust Framework, die keinen Austausch von Metadaten zwischen Identitäts- und Service-Provider erfordern. Diese offenen Identitätsframeworks fördern die Zusammenarbeit zwischen Unternehmen und Geschäftspartnern und tragen zu besserem Service für die Endbenutzer bei.

Die Umstellung auf das föderierte, benutzerorientierte Identitätsmanagement verhilft Ihnen zu folgenden Vorteilen:

- *Senkung der Kosten für Identitätsmanagement und Wartung (für Verbraucher, Mitarbeiter und Auftragnehmer)*
- *Erhöhung der Authentifizierungsgüte*
- *Verbesserte Compliance-Berichte und -Auditierbarkeit*

Vereinfachung des Identitätsmanagements bei Anwendungen

Mit Tivoli Federated Identity Manager können Sie Ihren Kunden, Partnern und Mitarbeitern größere Flexibilität für den Zugriff auf mehrere Geschäftsanwendungen bieten und gleichzeitig das Management mehrerer Identitäten vereinfachen. Beispielsweise können Sie Tivoli Federated Identity Manager mit den Webanwendungen eines Unternehmens verbinden, ohne proprietäre Anwendungsprogrammierschnittstellen (APIs) zu verwenden.

Ein in Tivoli Federated Identity Manager enthaltener Reverse Proxy unterstützt die Verbindung mit einer Webanwendung über eine HTTP/HTTPS-Verbindung. Dank der daraus entstehenden losen Verbindung zwischen der Middleware für föderiertes Single Sign-on und der Anwendungsebene kann eine Vielzahl verschiedener Webanwendungen in eine föderierte Umgebung eingebunden werden – ohne oder mit nur geringfügigen Änderungen an den Anwendungen. Darüber hinaus können Anwendungen und ihre zugehörige Middleware sowie Server aufgerüstet werden, ohne dass Änderungen an der Verbindung mit den Services für föderiertes Single Sign-on vorgenommen werden müssen, und neue Föderationsbeziehungen und -protokolle können auf einfache Weise hinzugefügt werden. Diese Funktionalität für die Implementierung der Föderation kann zu einer sehr viel schnelleren Wertschöpfung und deutlich niedrigeren Wartungskosten beitragen, verglichen mit API- oder Plug-in-basierten Methoden, die tiefergehende Anpassungen erfordern.

Erweiterte Funktionen für das operative Management vereinfachen das Identitätsmanagement

Ihr für das Identitätsmanagement zuständiges Team kann eine breite Palette an Funktionsfähigkeiten und benutzerfreundlichen Features nutzen, die in Tivoli Federated Identity Manager integriert sind, darunter folgende:

- *Verschiedene Point-of-Contact-Server, darunter IBM Tivoli Access Manager for e-business, Angebote anderer Anbieter für das Zugriffsmanagement, IBM WebSphere 6.1, Web-Server anderer Anbieter über einen angepassten Web-Server und kundenspezifische Plug-ins für Point-of-Contact-Server*
- *Administration des Produkts jetzt auch über Befehlszeilenkommandos (skriptfähig), grafischer Trust-Chain-Editor für die rasche Implementierung von Identitätsservices in SOA- und Web 2.0-Umgebungen*
- *Die neuesten Prüf- und Berichtsfunktionen, darunter Business Intelligence Reporting Tool (BIRT), Verbindung mit IBM Tivoli Compliance Insight Manager und integrierte Berichte über eine Konsole oder die Befehlszeile*
- *Erweitertes Schlüsselmanagement über eine Konsole für die einfache Änderung von Kennwörtern für den Schlüsselspeicher und das Management von Zertifikaten während des Betriebs*
- *Die Fähigkeit, Konfigurationsänderungen während der Laufzeit ohne Serverneustart zu aktivieren*

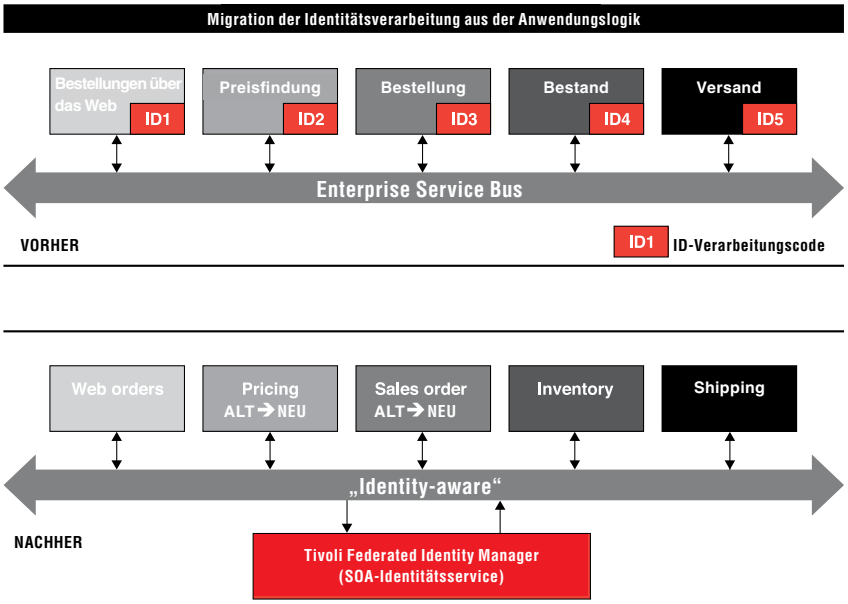
Unterstützung für einzelne Web-Services oder Identitätsservices im Rahmen einer SOA

Viele Vorteile einer SOA sind darauf zurückzuführen, dass vorhandene Anwendungsressourcen wiederverwendet werden können, indem sie in einzelne Geschäftsservices aufgeschlüsselt werden, die dann in verschiedenen Kombinationen neu zusammengefügt werden, um Geschäftsprozesse zu implementieren. Bestehende Anwendungen sind meist unabhängig voneinander entwickelt worden und verwenden unterschiedliche Darstellungen der Benutzeridentität und unterschiedliche Methoden des Austauschs von Identitäten. Viele Unternehmen verwenden beispielsweise eine generische Identität, um den Zugriff auf geschäftskritische Daten auf dem Mainframe zu ermöglichen. Das erfolgreiche Management dieser unterschiedlichen Benutzeridentitäten und die Verbesserung der Transparenz durch Verwendung realer Identitäten sind für den Erfolg einer SOA von entscheidender Bedeutung.

Tivoli Federated Identity Manager bietet ein leistungsfähiges, eigenständiges Identitätsservice-Tool, das Identity-Awareness in SOA- und Web-Service-Umgebungen bereitstellt – nutzbar durch IBM WebSphere DataPower SOA Appliances, den ESB oder IBM CICS (Customer Information Control System).

Zahlreiche Features erweitern die Funktionalität Ihrer SOA-Umgebung und erhöhen die Transparenz über mehrere Sicherheitsdomänen hinweg und für die gesamte IT-Infrastruktur des Unternehmens:

- *Ein Secure Transaction Service (STS) stellt Services für die Identitätsvermittlung für Ihre SOA- und Web-Service-Implementierung durch das Management, den Abgleich und die Weitergabe überprüfbarer Identitäten bereit. Der in Tivoli Federated Identity Manager enthaltene Identitätsservice ist von führenden XML-Firewall-Gateways, ESBs und/oder einer Mainframe-CICS-Umgebung aus nutzbar. Damit stehen Identitätsvermittlungsservices für Interaktionen zwischen verschiedenen Sicherheitsdomänen sowie mit externen Unternehmen und Services zur Verfügung.*
- *Unterstützung für eine Vielfalt von Sicherheitstokens – darunter SAML-Assertions, IBM RACF PassTicket, X.509-Zertifikate und Kerberos-Tickets sowie anpassbare Tokentypen – zur Weitergabe von Authentifizierungsdaten über einen Geschäftspartner oder einen Service an Back-End-, Mainframe- oder traditionelle Anwendungen*
- *Der STS kann die Identitätsnachweise eines Partners oder einer Domäne umwandeln und mit der Identitätsinfrastruktur eines anderen Partners oder einer anderen Domäne austauschen. Dies ermöglicht die Implementierung wiederverwendbarer Services und die schnellere Einführung einer föderierten ESB-Lösung.*
- *Administratoren können mithilfe von RACF PassTicket den Zugriff auf Web-Service-Transaktionen mit einer realen Benutzeridentität verbinden, um die Transparenz von IBM z/OS- oder anderen traditionellen Anwendungen in einer SOA zu verbessern.*



***Sie können einen alten Preisfindungs- oder Bestellservice durch einen neuen Service ersetzen, ohne die Anwendung für die Sicherheit erfassen zu müssen.**

Der Identitätsservice in Tivoli Federated Identity Manager vereinfacht die Identitätsverarbeitung in einer SOA, indem er Identitäten „abstrahiert“ – durch die Verlagerung der Identitätsverarbeitung weg von der Anwendungslogik.

Verwendung eines Federated ESB

Viele der heute eingesetzten ESB-Implementierungen können Identitäten über separat gesteuerte Domänen hinweg nicht effizient verbinden und verfolgen. Wenn Sie den SOA-Identitätsservice von Tivoli Federated Identity Manager zusammen mit Ihrem ESB einsetzen, können Sie die Administration vereinfachen und die Compliance unterstützen, indem Sie Ihren ESB „identity-aware“ machen. Damit erübrigt sich das Management mehrerer Identitäten aus heterogenen Standorten. Zudem kann sichergestellt werden, dass die Benutzer Zugang zu Anwendungen, Daten und Informationen auf der Basis ihrer Sicherheitsnachweise und Zugriffsebene haben, unabhängig davon, auf welche Anwendung sie zugreifen.

Wenn Sie den von Tivoli Federated Identity Manager bereitgestellten SOA-Identitätsservice mit Ihrem ESB kombinieren, können Sie die Flexibilität steigern, um bei Bedarf neue Services hinzuzufügen oder bestehende Services zu ändern. Zudem können Sie die Identitätsverarbeitung für neue oder geänderte Services vereinfachen (siehe Diagramm). Diese Identity-Awareness-Funktion bietet Unternehmen außerdem die Möglichkeit, bei einem Audit die Einhaltung der Regeln für das Identitätsmanagement gegenüber Prüfern nachzuweisen.

Der SOA-Identitätsservice von Tivoli Federated Identity Manager ist eine wichtige Komponente von IBM WebSphere Enterprise Service Bus, IBM WebSphere Message Broker, WebSphere DataPower und ESB-Implementierungen anderer Anbieter, die eine auf Standards basierende Schnittstelle für Identitätsbestätigungen unterstützen.

Wählen Sie eine umfassende Sicherheitslösung für SOA und Web-Services

Sie können den Identitätsservice in Tivoli Federated Identity Manager mit WebSphere DataPower SOA Appliances kombinieren, um eine leistungsstarke, integrierte Sicherheitslösung für SOA und Web-Services zu erhalten. Der Identitätsservice in Tivoli Federated Identity Manager bietet Folgendes:

- *Universelles Trust-Management*
- *Einen zentralen Authentifizierungsservice, nutzbar durch mehrere Geräte*
- *Möglichkeit der Erweiterung des Identitätsservice um Java™-Komponenten für die Token-Umsetzung oder proprietäre Authentifizierungsverfahren*

WebSphere DataPower SOA Appliances bieten Folgendes:

- *Firewall und Schutz vor Sicherheitsbedrohungen*
- *IBM WebSphere-Proxy-Verarbeitung*

Überwachung des Zugriffs von Identitäten auf die Mainframe-Umgebung

Mit dem Identitätsservice von Tivoli Federated Identity Manager können Sie „Identitätsprüfungen und -umsetzungen" durchführen, indem Sie die Identität vom Zeitpunkt der Anmeldung über den Datenzugriff bis zum Abschluss der Transaktion überprüfen. Berechtigungsnachweise werden zu Beginn verifiziert und dann von Schritt zu Schritt weitergeleitet. So können Sie neue Services rasch in Betrieb nehmen oder bestehende Services für einen anderen Zweck einsetzen, um Ihre geschäftlichen Ziele zu unterstützen. Dank der besonderen Fähigkeit von Tivoli Federated Identity Manager, überprüfbare Identitäten gleichzeitig aus der verteilten Umgebung zur Back-End-Mainframe-Umgebung zu übertragen, sind Sie außerdem in der Lage, Ihrer Rechenschaftspflicht nachzukommen und wachsende Compliance-Anforderungen zu erfüllen, indem Sie eine zentrale, konsistente Quelle von Benutzeridentitäten verwenden.

Wählen Sie die richtige Föderationslösung für Ihr Unternehmen

Sie können Tivoli Federated Identity Manager nicht nur auf verteilten Systemen, sondern auch unter z/OS ausführen. Damit erhalten Sie eine Lösung für das Identitätsmanagement mit hoher Verfügbarkeit, die Single Sign-on und Identitätsservices nativ in Ihrer IBM System z Mainframe-Umgebung unterstützt.

Unternehmen, die das föderierte Identitätsmanagement in der Zusammenarbeit mit einem Geschäftspartner aus dem Mittelstand nutzen wollen, können IBM Tivoli Federated Identity Manager Business Gateway verwenden. Mit dieser Einstiegsversion können Ihre Partner eine Verbindung zu Ihrem Unternehmen herstellen, um eine umfassende Lösung für das Identitätsmanagement zu nutzen, die die neuesten Protokolle wie SAML 2.0 unterstützt. Tivoli Federated Identity Manager Business Gateway kann die Zusammenarbeit in Ihrer gesamten Lieferkette oder im Geschäftsumfeld Ihrer Branche unterstützen.

Tivoli Federated Identity Manager auf einen Blick

Unterstützte Plattformen:

- IBM AIX 5.2, 5.3, 6.1
- Sun Solaris 9, 10 (SPARC)
- Microsoft Windows 2003, 2008 Standard Server und Enterprise Server
- Red Hat Linux® Advanced Server 3.0 und 4.0 für IBM System x
- Red Hat Linux Advanced Server und Enterprise Server 5.0 für System x
- Red Hat Linux Advanced Server 4.0 und 5.0 für IBM System p
- Red Hat Linux Advanced Server 4.0 und 5.0 für System z
- SUSE Linux Enterprise Server 9 und 10 für System p, System x und System z
- HP-UX 11i V2 und V3 auf Integrity

Die Web-Server-Plug-in-Komponente unterstützt Folgendes:

- Apache Web Server 2.0 und 2.2
- IBM HTTP Server 6.1
- Microsoft Windows Internet Information Server 6.0

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Tivoli Federated Identity Manager Ihr Unternehmen bei der Nutzung eines neuen benutzerorientierten, vertrauenswürdigen Identitätsmanagements und von Web-Services mit Identity-Awareness unterstützen kann, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter:

ibm.com/tivoli/solutions/security

Informationen zu IBM Tivoli Service-Management-Software

Tivoli-Software bietet eine Service-Management-Plattform für Unternehmen, die dank ihrer Transparenz, Kontrolle und Automation die Bereitstellung qualitativ hochwertiger Services ermöglicht. Transparenz bedeutet, dass Sie die Abläufe in Ihrem Unternehmen erkennen und nachvollziehen können. Kontrolle steht für das effektive Management Ihrer Geschäftsabläufe, die Minimierung von Risiken und den Schutz Ihrer Unternehmensmarke. Automation erlaubt die Optimierung Ihres Unternehmens, die Senkung der Betriebskosten und die schnellere Bereitstellung neuer Services. Anders als das IT-orientierte Service-Management stellt Tivoli-Software eine gemeinsame Grundlage für das Management, die Integration und die Abstimmung von Business- und IT-Anforderungen bereit. Tivoli-Software ist dafür konzipiert, die dringendsten Service-Management-Anforderungen eines Unternehmens rasch zu erfüllen und das Unternehmen dabei zu unterstützen, proaktiv auf sich ändernde geschäftliche Anforderungen zu reagieren. Das Tivoli-Portfolio wird durch erstklassige IBM Services und Supportangebote sowie ein Netz aus aktiven IBM Business Partnern unterstützt. Tivoli-Kunden und -Business Partner können sich zudem an unabhängig geführten IBM Tivoli-Benutzergruppen weltweit beteiligen und dabei bewährte Verfahren austauschen. Weitere Informationen hierzu finden Sie unter:

www.tivoli-ug.org

IBM Deutschland GmbH
Pascalstrasse 100
70569 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

TAKE BACK CONTROL WITH Tivoli.

TID14021-DEDE-00