

IBM Tivoli Access Manager for e-business

Highlights

- **Einheitliche Authentifizierung und Berechtigung für On Demand Initiativen im einzelnen Unternehmen oder im Unternehmensverbund**
- **Single-Signon (SSO) über Web-, Microsoft[®]-, Telnet- und Mainframe-Anwendungs-umgebungen hinweg**
- **Schnelle und skalierbare Implementierung von Web-anwendungen durch Scripts für J2EE-Anwendungen (Java[™] 2 Enterprise Edition), die auf Standards basieren**
- **Verbesserte Unterstützung für Mainframe-Anwendungen: APIs für Java 2 und Java Authentication and Authorization (JAAS) werden jetzt unter z/OS und auch auf WebSphere unter z/OS unterstützt**
- **Entwurfsflexibilität durch hoch skalierbare Proxy-Architektur und/oder einfach zu installierende Web-Server-Plug-ins, regel- und rollenbasierte Zugriffssteuerung, Unterstützung für die Benutzerregistrierung und Plattformen führender Anbieter sowie erweiterte APIs, mit denen die Sicherheitsmaßnahmen weiter angepasst werden können**
- **Kostensenkung bei Entwicklung, Implementierung und Management von Anwendungen durch einheitliches Identitäts- und Sicherheitsmanagement**
- **Zukunftsorientierte Kontinuität bei Sicherheits- und Identitätsmanagement**

Zuverlässige Sicherheit für On Demand und traditionelle Anwendungen

Moderne Unternehmen müssen sich heute mit kritischen Problemen in Bezug auf ihre Anwendungen und die Sicherheit der Transaktionen, die diese Anwendungen unterstützen, auseinandersetzen:

„Wie kann ich Anwendungen mit konsistenter Sicherheit implementieren, die über einheitliche Verfahren zur Zugriffssteuerung einfach zu verwalten sind?“

„Wie kann ich eine einheitliche Benutzerumgebung mit Funktionen wie z. B. Single-Signon (SSO) bereitstellen, wenn die Anzahl meiner Anwendungen, Server und Benutzer exponentiell ansteigt?“

„Warum sind meine proprietären Anwendungen nicht sicher, obwohl ich in diesem Bereich viel Geld investiere?“

„Verfügt mein Unternehmen über die Ressourcen, die für die effiziente Implementierung von Web-Services erforderlich sind?“

IBM Tivoli Access Manager for e-business unterstützt Sie beim Management von Wachstum und Komplexität sowie bei der Reduzierung der Managementkosten und bei der Implementierung von Sicherheitsrichtlinien über eine Vielzahl von Web- und Anwendungsressourcen hinweg.

IBM Tivoli Access Manager for e-business kann ohne weitere Anpassung mit On Demand Anwendungen integriert werden, um Sicherheit, Einheitlichkeit und Personalisierungsfunktionen für Anwendungen bereitzustellen. Durch die APIs für Authentifizierung und Berechtigung und durch Integration mit Anwendungsplattformen wie J2EE unterstützt Sie IBM Tivoli Access Manager for e-business bei der Sicherung des Zugriffs auf geschäftskritische Anwendungen und Daten, die über das gesamte erweiterte Unternehmensnetz verteilt sind.

Single-Signon (SSO) über das Internet kann mehrere Standorte oder Domänen umfassen, wenn Sie die domänenübergreifende SSO-Technologie von Access Manager oder SAML (Security Assurance Markup Language) und andere Protokolle für Tokenübergabe verwenden.

Richtlinienbasierte Sicherheit

Mit IBM Tivoli Access Manager for e-business können Sie eine umfassende Sicherheitsrichtlinie definieren, auf deren Basis Sie die Sicherheit verwalten. Dabei erhalten Mitarbeiter, Partner, Lieferanten und Kunden rollenbasierte Zugriffsrechte, die ihren Verantwortlichkeiten entsprechen. Sie können Benutzergruppen erstellen und diesen Berechtigungen zuordnen. So vereinfacht sich das Management der Zugriffssteuerung für mehrere Anwendungen und Ressourcen erheblich. Dynamische Rollen und tätigkeitsbezogene Berechtigungen sowie entsprechende Anwendungen werden unterstützt.

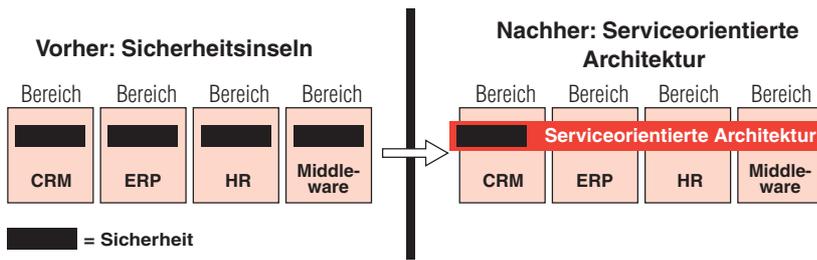
Über eine neue leistungsstarke und flexibel einsetzbare Funktion von IBM Tivoli Access Manager for e-business können Sie Geschäftsregeln in Entscheidungen zur Zugriffssteuerung integrieren. Die Regeln werden zur Laufzeit ausgewertet, so dass die Entscheidungsfindung bei der Zugriffssteuerung dynamisch erfolgt. In Übereinstimmung mit der Struktur von IBM Tivoli Access Manager for e-business sind diese Geschäftsregeln nicht Teil der Anwendung. Auf diese Weise können Sie die Richtlinienparameter für die Zugriffssteuerung ändern, ohne dass Anwendungen neu geschrieben oder kompiliert werden müssen. Diese Funktion kann die Implementierung und Anpassung von Anwendungen erheblich beschleunigen.

IBM Tivoli Access Manager for e-business umfasst ein webbasiertes Tool, mit dem Ihr Administrator Benutzer, Gruppen, Rollen, Berechtigungen, Richtlinien, Anschlussstellen und Zugriffseinrichtungen für Anwendungen verwalten kann. Dieses Tool bietet nicht nur delegiertes Benutzermanagement, sondern auch delegiertes Sicherheitsmanagement.

IBM Tivoli Access Manager for e-business erstellt Prüfsätze in einem Standard-XML-Format, aus dem Sie erforderliche Informationen problemlos extrahieren können. Ein Tool zur Informationserfassung ermöglicht die sichere und zentrale Erfassung von und Berichterstellung zu Prüf-, Protokoll-, Statistik- und anderen Daten im gesamten erweiterten Unternehmensnetz.

Implementierung von Sicherheitsfunktionen in einer serviceorientierten Architektur (SOA)

Anwendungsplattformen wie z. B. Web-Server bieten Sicherheits- und sonstige Services für den Anwendungsentwickler. Das Zugriffsmanagement erfolgt jedoch isoliert in den verschiedenen Unternehmensbereichen und ist von den Kenntnissen und Tools abhängig, die in der jeweiligen Anwendungsumgebung verfügbar sind.



IBM Tivoli Access Manager for e-business: Implementierung von Sicherheitsfunktionen in einer serviceorientierten Architektur (SOA)

Die Abbildung zeigt, dass der IBM Ansatz On Demand Business unterstützt, indem elementare Funktionen als gemeinsame Services bereitgestellt werden – eine so genannte serviceorientierte Architektur (SOA). IBM Tivoli Access Manager for e-business bietet Sicherheit für heterogene Umgebungen. Bei dieser Architektur basiert die Zugriffssteuerung auf einer einzigen, konsistenten Schicht, die im Vergleich zu „Insellösungen für Sicherheit“ eine schnellere Implementierung von Anwendungen und ein präziseres und konsistenteres Sicherheitsmanagement ermöglichen.

Integriertes Identitätsmanagement

IBM Tivoli Access Manager for e-business ist eine integrierte Komponente der IBM Lösung für Identitätsmanagement, die Sie dabei unterstützt, Systeme und Anwendungen schnell in Betrieb zu nehmen, die Benutzerproduktivität zu steigern, die Kosten zu reduzieren und den ROI zu erhöhen.

IBM Identitätsmanagement bietet Lebenszyklusmanagement für Identitäten (Benutzerselbstverwaltung, Registrierung und Provisioning), Identitätskontrolle (Zugriffssteuerung und Vertraulichkeit, Single-Signon

und Prüfung), Identitätsverbund (gemeinsame Nutzung von Benutzerberechtigungs- und Attributinformationen durch mehrere sichere Web-Service-Anwendungen) und Identitätsbasisdaten (Verzeichnis und Workflow). Dank dieser Merkmale können Sie sowohl interne Benutzer als auch eine steigende Zahl an Kunden und Partner über das Internet verwalten.

Sichere, einheitliche Benutzerumgebung

IBM Tivoli Access Manager for e-business unterstützt eine große Anzahl an Benutzern, an komfortablen, verfügbaren und personalisierten Transaktionen teilnehmen zu können. Authentifizierungs- und Zugriffssteuerungsservices für On Demand Business und Unternehmensanwendungen und -ressourcen garantieren die Sicherheit der Verbindungen zu Kunden, Lieferanten, Mitarbeitern und Partnern. Dabei wird Folgendes unterstützt:

- *Web-Server*
- *J2EE-basierte Anwendungsserver wie WebSphere Application Server, BEA WebLogic Server und Oracle 9iAS*

- *Branchenführende Webanwendungen wie Siebel 7, Siebel 2000, Microsoft Exchange 2003, PeopleSoft 8, PeopleSoft PeopleTools, WebSphere Portal, WebSphere Edge Server, WebSphere Host On-Demand 6, WebSphere Host Publisher, WebSphere Host Access Transformation Server, IBM Content Manager, WebSphere Everyplace Server Service Provider Offering, Lotus Domino, Lotus iNotes, Lotus QuickPlace, Lotus Sametime, mySAP.com, SAP Internet Transaction Server (ITS), SAP Enterprise Portal, BEA WebLogic Server, Epicentric Foundation Server, BroadVision One-To-One Enterprise, Vignette V5, Plumtree Corporate Portal, Oracle 9iAS Portal, KANA Platform, i2 TradeMatrix, iPlanet Calendar, iPlanet Messenger Express, Aelita Directory Manager, Blockade ESconnect, Cash-U-Pecan, Citrix Metaframe/Nfuse XP, Kintana Suite 4.5, OpenConnect WebConnect, Rocksteady Rocknet 2.1, Verity K2 Enterprise und WinCom Switching Server*

IBM Tivoli Access Manager for e-business unterstützt eine breite Palette an Mechanismen zur Benutzerauthentifizierung, darunter Benutzer-IDs und Kennwörter, Zertifikate der Clientseite, Identitäten für mobile und drahtlose Geräte und aktualisierte Unterstützung für RSA-SecurID-Token. Kunden mit individuellen

Authentifizierungsanforderungen können den Authentifizierungsmechanismus verwenden, der als Plug-in mit IBM Tivoli Access Manager for e-business geliefert wird.

Wenn Sie IBM Tivoli Access Manager for e-business als Berechtigungs-engine für On Demand Business verwenden, können Sie die oben erwähnten Sicherheitsfunktionen (Zertifikate, drahtlose Geräte und Token) und viele andere hervorragende Angebote im Bereich Sicherheit nutzen. Dank der Arbeit, die IBM zusammen mit Anbietern von Sicherheitstechnologien leistet, sind Ihre Anwendungen automatisch für folgende Einrichtungen aktiviert, wenn Sie IBM Tivoli Access Manager for e-business verwenden:

- *Lesegeräte für Fingerabdrücke (Software DaonConnect for IBM Tivoli Access Manager)*
- *VPN-Geräte (Ingrian Secure Transaction Appliance und Neoteris IVE)*
- *Karten zur SSL-Beschleunigung (IBM 4960 PCI, nFast, Rainbow Technologies CryptoSwift PCI und Eracom Protect Server Orange)*
- *Kombinationskarten (SSL-Beschleunigung und Hardware-Schlüsselspeicherung) – IBM 4758 PCI und nCipher nForce*
- *Verzeichnisse (Siemens DirX 6.0 und SecurIT CDAS for Vasco DigiPass)*

- *Token (Aladdin Knowledge Systems eToken)*
- *Digitale Zertifikate für mobile Geräte (Entrust TruePass)*
- *Einrichtungen für Lastausgleich (F5 Networks BIG-IP)*
- *Token für Single-Signon (Sena Systems PortalPass)*

IBM Tivoli Access Manager for e-business unterstützt Sie bei der Bereitstellung einer konsistenten und sicheren Benutzerumgebung, da Endbenutzer nach einer einzigen Anmeldung beim Unternehmensportal oder Microsoft-Desktop anhand von Berechtigungsregeln Zugriff auf Ressourcen erhalten. Durch Unterstützung für Web-SSO und sicheres Sitzungsmanagement über verschiedene Benutzergruppen hinweg hilft IBM Tivoli Access Manager for e-business Ihnen dabei, Ihre Geschäftspartner auf sichere Weise in die Geschäftsprozesse einzubeziehen.

IBM Tivoli Access Manager for e-business führt über replizierte Server einen intelligenten Lastausgleich durch und kann Ihre Serverimplementierung skalieren. Diese Lösung unterstützt Implementierungen mit mehr als einer Million Benutzern, nutzt die Technologie von Beschleunigungskarten für Secure Sockets Layer (SSL) sowie sichere Hardware-Schlüsselspeicher und bietet Überbrückungsfunktionen zur automatischen Umschaltung auf einen Backup-Web-Server.

Unterstützung für Autonomic Computing

IBM Tivoli Access Manager for e-business stellt durch die folgenden Merkmale eine selbst-schützende Umgebung bereit:

- *Verhinderung von unbefugtem Zugriff durch Verwendung eines einzigen Servers für Sicherheitsrichtlinien, mit dessen Hilfe Sicherheitsmaßnahmen über verschiedene Dateitypen, Anwendungsanbieter, Geräte und Protokolle hinweg umgesetzt werden*
- *Web-SSO für die Integrität von Kennwörtern und Benutzer-IDs*
- *Zuverlässige Tools zur Prüfung und Informationserfassung für die Identifizierung von Problemen oder potenziellen Problemen*

Darüber hinaus stellt IBM Tivoli Access Manager for e-business durch die folgenden Merkmale eine selbstoptimierende Umgebung bereit:

- *Lastausgleich und automatische Reflexion von Webobjektbereichen*
- *Hoch verfügbare und skalierbare Architektur, die auf offenen Standards basiert*

Modulare Struktur vereinfacht die Verwendung

Auf Grund der modularen Architektur von IBM Tivoli Access Manager for e-business ist der Sicherheitscode vom Anwendungscode getrennt.

Dies erlaubt kürzere Entwicklungszeiten für Ihre On Demand Initiativen, da Sie in der Regel den Sicherheitscode ohne Auswirkungen auf den Anwendungscode ändern können und umgekehrt.

Zur Vereinfachung des Programmiermodells können die zentralen Authentifizierungs- und Berechtigungs-services von IBM Tivoli Access Manager for e-business für Servlets, JavaServer Pages und Enterprise JavaBeans bereitgestellt werden.

Neben den Java 2-Services und der Berechtigungs-API von The Open Group unterstützt IBM Tivoli Access Manager for e-business zahlreiche offene Industriestandards und Integrationsmöglichkeiten; darunter:

- *Lightweight Directory Access Protocol (LDAP) zum Speichern von Benutzer- und Gruppeninformationen. IBM Directory Server, Sun ONE Directory Server, Novell eDirectory, Microsoft Active Directory und Lotus Domino Server werden u. a. als Benutzerregistrierung unterstützt. Zusätzliche Funktionen umfassen die Mehrdomänenunterstützung von IBM Directory Server sowie Unterstützung für dynamische Gruppen von IBM Directory Server und Sun ONE Directory Server*

- *Metaverzeichnisimplementierungen einschließlich IBM Directory Integrator*
- *Virtuelle Verzeichnisimplementierungen einschließlich Radiant Logic und OctetString*
- *X.509 V3-Clientzertifikate für die strikte Authentifizierung webbasierter Ressourcen. Zahlreiche Zertifikatanbieter werden unterstützt, darunter VeriSign, Entrust und Baltimore*
- *Gegenseitig authentifizierte und geschützte Komponenteninteraktionen durch SSL. IBM Tivoli Access Manager for e-business ist eine offene, auf Standards basierende Implementierung*
- *Dank der Integration mit IBM Tivoli Identity Manager können Sie die in einem Produkt registrierten Benutzer in das jeweils andere Produkt importieren und die Kennwörter synchronisieren. Durch Selbstregistrierung und Selbstbedienung der Benutzer sparen Sie Kosten*
- *Die Prüfinformationen von IBM Tivoli Access Manager können Sie an IBM Tivoli Risk Manager und IBM Tivoli Data Warehouse senden. Diese Produkte bieten Funktionen zur Berichterstellung und Entscheidungsunterstützung*

- *IBM Tivoli Configuration Manager kann die Authentifizierungs- und Berechtigungsfunktionen von IBM Tivoli Access Manager for e-business nutzen, um Benutzern das eigenständige, selektive Management ihrer Workstationkonfiguration zu ermöglichen. Auf diese Weise lässt sich die Benutzerproduktivität erhöhen und der Managementaufwand reduzieren*

IBM Tivoli Access Manager for e-business wurde im Rahmen des Common Criteria-Prozesses, der vom National Information Assurance Partnership durchgeführt wird, mit einer Common Criteria-Zertifizierung ausgezeichnet.

Plattformen

IBM AIX 5.1 oder 5.2

Sun Solaris 8 oder 9

Microsoft Windows® 2000 Advanced Server, Service Pack 3

Microsoft Windows 2003 Standard Server und Enterprise Server

HP-UX 11.0, 11i

United Linux® einschließlich SuSE Linux Enterprise Server for Intel®, S/390 und zSeries

Red Hat Enterprise Linux

WebSphere Application Server und Java-APIs für z/OS

IBM RISC System/6000

Sun SPARC

Intel x86- oder Intel Pentium-Prozessor

(Aktuelle Informationen zu unterstützten Plattformen können Sie den Release-Informationen zu Ihrem Produkt entnehmen.)

IBM Tivoli Access Manager for e-business funktioniert mit den Browsern Netscape Navigator, Mozilla und Microsoft Internet Explorer sowie mit Einheiten für Pervasive Computing, die das Wireless Application Protocol oder i-mode-Protokoll unterstützen.

Weitere Informationen

Wenn Sie mehr über IBM Tivoli Access Manager for e-business und über integrierte Lösungen von IBM erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder besuchen Sie uns unter **ibm.com/tivoli/solutions/security**

Tivoli Software von IBM

Als integraler Bestandteil der umfassenden On Demand Infrastrukturlösung von IBM hilft Tivoli Management-Software traditionellen Unternehmen, On Demand Unternehmen und

Internetunternehmen weltweit, den Wert früherer und zukünftiger IT-Investitionen zu maximieren. Mit Unterstützung erstklassiger IBM Service-, Support- und Forschungsleistungen bietet IBM Tivoli-Software eine nahtlos integrierte und flexible On Demand Lösung für das Infrastrukturmanagement, die Mitarbeiter, Geschäftspartner und Kunden über zuverlässige Sicherheitsfunktionen miteinander verbindet.



IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

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

IBM Schweiz
Bändliweg 21, Postfach
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo, ibm.com sind Marken der International Business Machines Corporation.

On Demand Business, das On Demand Business Logo, AIX, Domino, iNotes, Lotus, QuickPlace, Rational, RISC System/6000, S/390, Sametime, Tivoli, WebSphere, z/OS und zSeries sind Marken der International Business Machines Corporation in den USA und/oder anderen Ländern.

Intel und Pentium sind Marken der Intel Corporation in den USA und/oder anderen Ländern.

Java und alle Java-basierten Marken sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Alle Informationen in diesem Dokument zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Hergestellt in den USA
10-03

© Copyright IBM Corporation 2004
Alle Rechte vorbehalten.