Bessere Zugriffskontrolle, einfachere Einhaltung von Vorschriften und Unterstützung der operativen Steuerung im gesamten Unternehmen

Tivoli software

IBM Tivoli Security Policy Manager

Highlights

- Minimierung von Ineffizienzen und Schwachstellen im Zusammenhang mit dem Management von Anwendungsberechtigungen und SOA-Sicherheitsrichtlinien
- Management von SOA-Sicherheitsrichtlinien während ihres gesamten Lebenszyklus – von der Erstellung und Bereitstellung bis zu ihrer Durchsetzung und Anpassung
- Management von Anwendungsberechtigungen und Durchsetzung von Richtlinien zur Laufzeit, dadurch Stärkung der Sicherheit Ihres Unternehmens
- Zentrale Änderung und Steuerung von Richtlinien für die schnellere, konsistentere und effizientere Erfüllung neuer oder strikterer Konformitätsanforderungen
- Nutzung des föderierten Richtlinienmanagements, um Unterschiede zwischen Business und IT in der Herangehensweise an Sicherheitsrichtlinien zu überbrücken

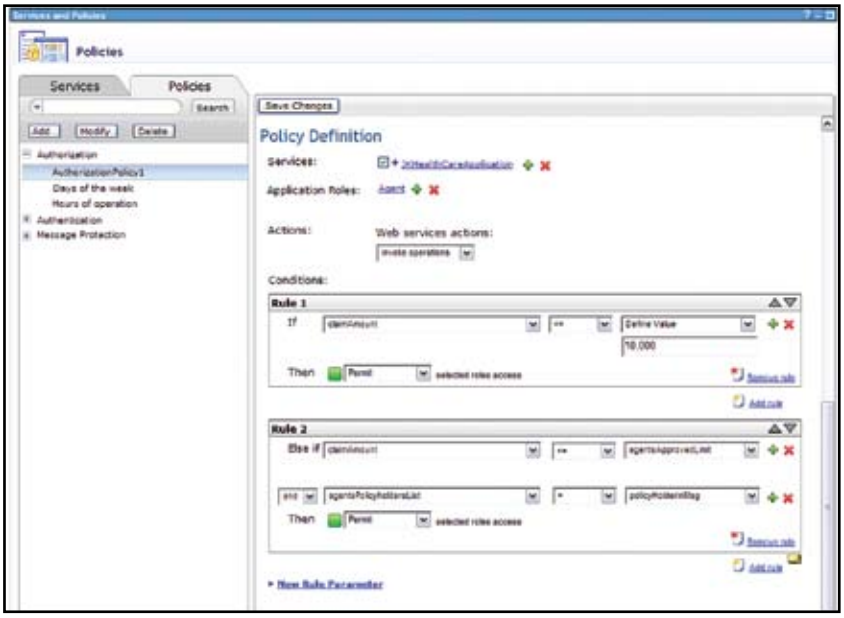
Unternehmen stehen derzeit vor neuen Herausforderungen im Zusammenhang mit der Absicherung des Zugriffs auf ihre Anwendungen und Services in der IT-Umgebung von heute. Um die immer größere Zahl von Branchenbestimmungen und gesetzlichen Auflagen erfüllen zu können, müssen Unternehmen den Zugriff auf Geschäftstransaktionen und -anwendungen mittels komplexer, differenzierter Berechtigungsrichtlinien kontrollieren. Darüber hinaus müssen sie zunehmend auf geschäftliche Veränderungen reagieren und sensible Daten über mehrere Anwendungen und Services hinweg verwenden. Dies führt zu steigenden Kosten für die Programmierung und Wartung sich überlappender Sicherheitsfunktionen in den einzelnen Anwendungen. Das wachsende Risiko eines Verlusts von geistigem Eigentum und die Zunahme von Sicherheitsbedrohungen erfordern Berechtigungskonzepte und Zugriffskontrollmaßnahmen auf Datenebene für eine immer größere Zahl von Benutzern – darunter eigene Mitarbeiter mit verschiedenen Aufgaben (Rollen), externe Auftragnehmer, Geschäftspartner und in manchen Fällen sogar Mitbewerber.

Die Einführung einer serviceorientierten Architektur (SOA) und des Web 2.0 bringt völlig neue Herausforderungen im Zusammenhang mit dem Management von Sicherheitsrichtlinien mit sich. Denn aus der losen Verknüpfung von Services und zusammengesetzten Anwendungen (Mashups) innerhalb des Unternehmens und über dessen Grenzen hinweg entstehen zahlreiche Richtlinienmanagementpunkte (Policy Management Points, PMPs), von denen jeder einzelne administriert werden muss. Diese Sicherheitsrichtlinien und -konfigurationen beziehen sich derzeit auf einzelne Produkte mit toolspezifischen Definitionen. Das Management dieser Richtlinien durch die IT in einer heterogenen Umgebung muss heute manuell durchgeführt werden, ist fehlerträchtig und führt zur Entstehung von teuren Insellösungen im Bereich der Sicherheitsadministration. Zudem erhöht die rasche Implementierung von Web-Services das Risiko der Anwendung uneinheitlicher Zugriffskontrollrichtlinien und als Konsequenz unerwünschte Zugriffe auf sensible Geschäftsdaten. Insbesondere für Unternehmen wie Banken, Krankenhäuser und Versicherungen ist der Schutz der Daten, die in Anwendungen im gesamten Unternehmen gespeichert sind, von großer Bedeutung. Ebenso wichtig ist die Fähigkeit, auf Verlangen ein lückenloses Prüfprotokoll als Nachweis der Durchsetzung von Richtlinien vorzulegen.

Management von SOA-Sicherheitsrichtlinien und Anwendungsberechtigungen auf einer zentralen Plattform

IBM Tivoli Security Policy Manager bietet eine umfassende Lösung, mit der Sie diese Herausforderungen im Bereich der Sicherheit meistern können. Diese Lösung erlaubt das einheitliche Management von SOA-Sicherheitsrichtlinien und Anwendungsberechtigungen über unterschiedliche Benutzerverzeichnisse und Anwendungen hinweg. Mit Tivoli Security Policy Manager können Richtlinien während ihres gesamten Lebenszyklus verwaltet werden – von der Erstellung über die Umwandlung und Verteilung bis zu ihrer Durchsetzung und Überwachung. Dieses anpassungsfähige Tool bietet die Möglichkeit, Anwendungsrollen zu importieren, und kann mit vorhandenen Identitätssystemen verknüpft werden. Es nutzt Standards wie XACML, WS-Trust und WS-Policy (unter anderen) für die zentrale Steuerung und vereinfacht so die Erfüllung verschärfter oder neuer Konformitätsanforderungen.

Tivoli Security Policy Manager stellt Sicherheit als Service bereit, entkoppelt sie von den anwendungsspezifischen Authentifizierungs- oder Berechtigungsfunktionen und verbessert so die Sicherheit und trägt zur Vereinfachung der IT-Infrastruktur bei. Die auf (OSGi Open Services Gateway Initiative) basierende Plug-in-Architektur der Software arbeitet nicht nur reibungslos mit vorhandenen Sicherheitslösungen zusammen, sondern erlaubt außerdem die einfache Erweiterung des Produkts in mehreren Bereichen.



Tivoli Security Policy Manager bietet ein breites Spektrum an Funktionen, die Unternehmen bei der Erfüllung verschiedener Richtlinienanforderungen in SOA-Umgebungen unterstützen.

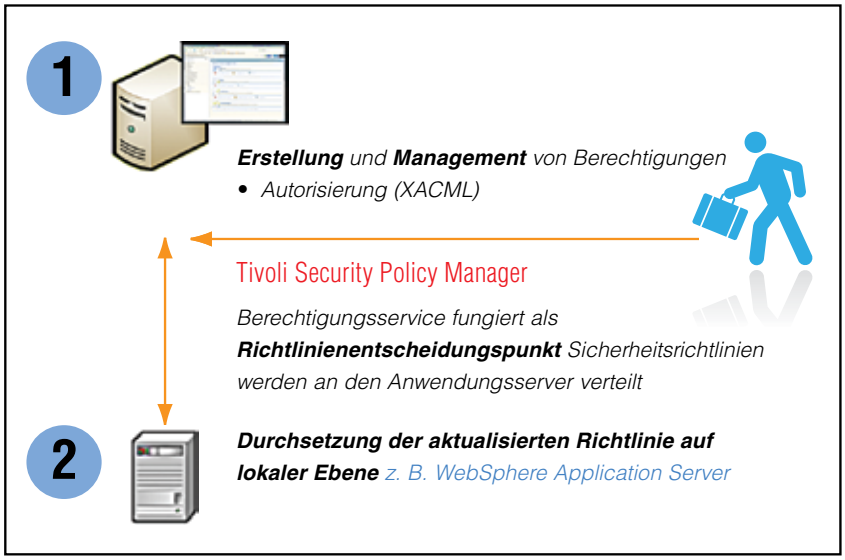
Ein Sicherheitsadministrator in einem Versicherungsunternehmen könnte beispielsweise ein einheitliches Sicherheitsrichtlinientool für das Management, die Delegation und die Verfolgung von Änderungen an allen Sicherheitsrichtlinien für Web-Services und Anwendungen verwenden. Er könnte das gemeinsame Berechtigungsframework von Tivoli Security Policy Manager für die Kontrolle des Zugriffs auf Schadensfälle, Rechnungen, Angebote, Unterlagen und Kreditauskünfte mit Sicherheitsrichtlinien für die Authentifizierung, Vertraulichkeit und Integrität von Nachrichten verwenden. Ein Anwendungsentwickler im selben Unternehmen könnte Zugriffskontrollentscheidungen auslagern und hierfür den Berechtigungsservice nutzen – und so den Zeit- und Kostenaufwand für die Zugriffskontrolle seiner Anwendung verringern.

Management von Sicherheitsrichtlinien in SOA-Umgebungen

Während jeder Phase des Managements von SOA-Sicherheitsrichtlinien kann Tivoli Security Policy Manager Richtlinien und Prozesse vereinfachen und konsolidieren. Tivoli Security Policy Manager beschafft zunächst die Servicedefinition und Metadaten vom WebSphere Service Registry and Repository (WSRR) und fungiert anschließend als zentraler Richtlinienadministrationspunkt (Policy Administration Point, PAP), an dem nicht nur Sicherheitsrichtlinien für Nachrichten, sondern auch Berechtigungsrichtlinien definiert werden können. Diese Richtlinien können entweder zurück an das Service-Registry oder an Durchsetzungspunkte (Policy Enforcement Points, PEP) wie WebSphere DataPower übertragen werden, wo die Richtlinien anschließend durchgesetzt werden können.

Management und Durchsetzung von Anwendungsberechtigungen

IT-Anwendungsverantwortliche können mit Tivoli Security Policy Manager Anwendungsberechtigungen und differenzierte Zugriffskontrollrichtlinien erstellen und in das normierte XACML-Format umwandeln, um so verteilte Richtlinienentscheidungen zu ermöglichen. Die Erteilung der Berechtigung für einen Zugriff hängt von der Kombination folgender Angaben ab: Identität (Wer?), Art der Transaktion (Was?) und Service/Ressource (Wo?). Die IT-Abteilung kann Sicherheitsrichtlinien konsistent über verschiedene IT-Anwendungsumgebungen hinweg, darunter WebSphere Application Server, sowie für kundenspezifische Anwendungen auslagern, verteilen und durchsetzen.



Tivoli Security Policy Manager kann der IT-Abteilung die Umsetzung von Entscheidungen der Geschäftsbereiche erleichtern.

Flexiblere Geschäftsabläufe und mehr IT-Effizienz

Tivoli Security Policy Manager besteht aus mehreren Komponenten, die dazu beitragen, die Flexibilität der Geschäftsbereiche und die Effizienz der IT zu verbessern.

- *Der Policy Manager bietet eine Benutzeroberfläche und einen Datenspeicher für das Management von Services und Richtlinien während ihres gesamten Lebenszyklus, einschließlich Serviceerkennung, Richtlinienerstellung, -konfiguration und -verteilung.*
- *Die Runtime Security Services (RTSS) stellen die Laufzeitkomponente für die Evaluierung von Zugriffsberechtigungen und -entscheidungen bereit.*
- *WebSphere Policy Enforcement Point (PEP) ist ein IBM WebSphere-Plug-in, das die containergesteuerte Berechtigungskontrolle unter Verwendung von RTSS für Berechtigungsentscheidungen (Policy Decision Point, PDP) erlaubt.*

Mit Tivoli Security Policy Manager kann die IT-Abteilung Sicherheitsrichtlinien von einer zentralen Plattform aus erstellen, verwalten, umwandeln und verteilen. Ein Krankenhaus kann beispielsweise eine Sicherheitsrichtlinie auf der Basis von Rollen und Gruppen (Benutzer/Subjekt, Service/Ziel) erstellen und anschließend dafür konfigurieren, die Herausgabe von Informationen bestmöglich zu kontrollieren. Das Krankenhaus könnte außerdem Ressourcen und Metadaten für die Erstellung oder Klassifizierung von Richtlinien automatisch erkennen und Services aus unterschiedlichen Registrys und Anwendungen importieren.

Tivoli Security Policy Manager kann Anwendungsrollen importieren und mit bestehenden Identitätssystemen verknüpfen. Damit steht Ihnen ein flexibles Tool zur Verfügung, das mit den Anforderungen und dem Wachstum Ihres Unternehmens Schritt halten kann und das Sie bei der Einhaltung von sich ändernden Konformitätsvorschriften unterstützt. Jede Anwendung benötigt Informationen über den Service-Level oder die Rolle eines Benutzers. Diese Informationen sind häufig auf viele verschiedene Anwendungen verteilt (z. B. LDAP, Personalsystem, Datenbanken etc.). Der Identitätsservice der Software nutzt eine gemeinsame Schnittstelle für die Kommunikation und sorgt für Sicherheit und Datenschutz.

Umwandlung von Geschäftsrichtlinien in durchsetzbare Anweisungen
Die Runtime Security Services (RTSS) der Software stellen die erforderliche Leistung, Skalierbarkeit und Zuverlässigkeit für die Durchsetzung von Richtlinien bereit. Diese Services können verwendet werden, um Entscheidungen über Geschäftsberechtigungen auf höherer Ebene in Berechtigungsanweisungen auf operativer Ebene umzusetzen. Diese Anweisungen können dann mithilfe eines Richtliniendurchsetzungspunkts (Policy Enforcement Point, PEP), z. B. mit dem WebSphere Plug-in, angewandt und durchgesetzt werden. Die RTSS-Software kann Berechtigungsentscheidungen auf spezielle Weise entweder in einem Remote- oder Lokalmodus (für die Anwendung) fällen, wobei sie Unterstützung für die partielle, anwendungssspezifische Replikation der Policydaten mit dem Policy-Server bietet. Dadurch kann die IT-Abteilung eine hoch performante Umgebung aufbauen, wie sie für einen produktiven Einsatz unabdingbar ist.

Bereichsübergreifende Zusammenarbeit mit föderiertem Richtlinienmanagement
Da die Software das föderierte Richtlinienmanagement unterstützt, erleichtert sie der IT-Abteilung die Überbrückung von Unterschieden zwischen Business und IT in der Herangehensweise an Sicherheitsrichtlinien und ermöglicht so die Zusammenarbeit über verschiedene Bereiche hinweg. Mit Tivoli Security Policy Manager können Administratoren Metadaten und Durchsetzungsregeln organisieren und verwalten. Sie können koordinieren, wer diese Regeln definiert, wie sie definiert, verteilt und durchgesetzt werden und wie ihr Lebenszyklus definiert wird.

Durchgängige Autorisierung
Tivoli Security Policy Manager for Application Entitlements externalisiert die Sicherheit und ermöglicht die durchgängige Autorisierung von Anwendungen. Zu den wichtigsten Funktionen für das Management von Anwendungsberechtigungen gehören ein Richtlinienadministrationspunkt (Policy Administration Point, PAP), eine intuitive Benutzeroberfläche, die Assistenten und Drag-and-drop-Funktionen nutzt, und ein integrierter Richtlinienentscheidungspunkt (Policy Decision Point, PDP), bei dem es sich um eine auf ihre Interoperabilität getestete Richtlinienengine handelt. Die Policy-Enforcement-Komponente (PEP) unterstützt geeignete Plug-ins, die auf Standards basierende Richtlinienabfragen von der jeweiligen Plattform absetzen. So können etwa kundenspezifische Anwendungen in Java™ und .NET sowie mainframebasierte Anwendungen unterstützt werden. Tivoli Security Policy Manager for Application Entitlements erlaubt dank seiner Flexibilität die Nutzung von zusätzlichen Informationen für Entscheidungen aus verschiedenen Datenquellen (Policy Information Points, PIP).

Interoperabilität und Integration durch offene Standards
Tivoli Security Policy Manager kann mit weiteren Tivoli-Produkten wie IBM Tivoli Federated Identity Manager, IBM Tivoli Access Manager for e-business und IBM Tivoli Security Information and Event Manager kombiniert werden. Dadurch profitieren Sie von erweiterter Funktionalität und können den Wert Ihrer bereits getätigten Investitionen in Tivoli-Software steigern.
Tivoli Security Policy Manager bietet außerdem Interoperabilität mit auf offenen Standards basierenden Serviceverzeichnissen von Microsoft®, Oracle, SAP, Sun und weiteren Anbietern in diesem Bereich. Zu den unterstützten Standards gehören:

- *Serviceschnittstellen*
  - *Tokenaustausch und -authentifizierung: WS-Trust*
  - *Identitätsservice: IdAS*
- *Richtlinienausdrücke*
  - *Berechtigungsrichtlinien: XACML*
  - *Richtlinien für den Schutz von Nachrichten wie WS-Security Policy*
- *Programmiermodell*
  - *Web-Services: WS-Trust, XACML*
  - *Java*

Implementierung eines richtlinienbasierten Ansatzes in Ihrem Unternehmen
Mit Tivoli Security Policy Manager sparen Sie Zeit und Geld, da Ineffizienzen und Schwachstellen im Zusammenhang mit dem Management von Berechtigungen und Sicherheitsrichtlinien minimiert werden. Sie profitieren von verbesserter Kontrolle und Transparenz, während Sie Entwicklungskosten minimieren, Prozesse optimieren und Prüfanfragen (Audits) besser behandeln können.

Tivoli Security Policy Manager wird in zwei Paketen angeboten, die den unterschiedlichen IT- und anwendungsspezifschen Anforderungen von Kunden Rechnung tragen:

- *Tivoli Security Policy Manager for Application Entitlements*
- *Tivoli Security Policy Manager for SOA*

Mit Tivoli Security Policy Manager for Application Entitlements können Anwendungsverantwortliche und Administratoren die Sicherheit aus der Anwendungslogik auslagern und das Management komplexer Berechtigungsrichtlinien für neue und vorhandene Anwendungen, darunter auch kundenspezifische Anwendungen, vereinfachen. Mit dieser Lösung können Unternehmen Anwendungsrollen, Berechtigungen und die Zugriffskontrolle auf Datenebene zentralisieren, um rasch auf geschäftliche Änderungen zu reagieren, und das Konformitäts- und Sicherheitsmanagement durch die Zugriffskontrolle auf Rollen-, Regel- und Attributbasis verbessern. Dieses Paket enthält den Policy Manager, die Run-Time Security Services und den WebSphere Policy Enforcement Point.

Mit Tivoli Security Policy Manager for SOA können Architekten und Sicherheitsverantwortliche eines Unternehmens Sicherheitsrichtlinien für Web-Service-Ressourcen zentral verwalten und durchsetzen – über mehrere Policy Enforcement Points, einschließlich WebSphere DataPower SOA Appliances, hinweg.

Dieses Paket trägt dazu bei, die manuelle, inkonsistente und kostenintensive Administration von Sicherheitsrichtlinien an jedem Policy Enforcement Point zu reduzieren und erlaubt die operative Steuerung mit der Möglichkeit der Delegation und Prüfung aller Änderungen an Richtlinien. Dieses Paket enthält den Policy Manager mit der sofort einsatzfähigen Integration mit WebSphere Services Registry and Repository und WebSphere DataPower.

IBM Tivoli Security Policy Manager auf einen Blick

Unterstützte Plattformen:

- IBM AIX 5.3
- Red Hat Enterprise Linux® (RHEL) 5.0 AS/ES IA64
- Red Hat Enterprise Linux (RHEL) 5.0 AS/ES x86-32
- Red Hat Enterprise Linux (RHEL) 5.0 AS/ES x86-64
- Red Hat Enterprise Linux (RHEL) 5.0 WS x86-32
- Red Hat Enterprise Linux (RHEL) 5.0 WS x86-64
- Solaris 10 SPARC
- Solaris 9 SPARC
- SuSE Linux (SLES) 10.0 Enterprise Server x86-32
- SuSE Linux (SLES) 9.0 Enterprise Server x86-32
- Windows Server® 2003 Enterprise Edition x86-32
- Windows Server 2003 Standard Edition x86-32
- Windows Server 2008 Enterprise Edition x86-32
- Windows Server 2008 Standard Edition x86-32

Weitere Informationen

Wenn Sie mehr über IBM Tivoli Security Policy Manager erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter:

ibm.com/tivoli

Tivoli-Software von IBM

Tivoli-Software bietet eine Service-Management-Plattform für Unternehmen, die dank ihrer Transparenz, Steuerung und Automation die Bereitstellung qualitativ hochwertiger Services ermöglicht. Transparenz bedeutet, dass Sie die Abläufe in Ihrem Unternehmen erkennen und nachvollziehen können. Steuerung 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

Recyclable, please recycle.

TAKE BACK CONTROL WITH Tivoli.

TID14029-DEDE-00