Tivoli software

IBM Tivoli Identity Manager

Highlights

- ***Verringert die Gemeinkosten durch automatisches Management von Rollen, Accounts und Zugriffsberechtigungen während des gesamten Lebenszyklus von Benutzern***
- ***Korrigiert und entfernt nicht konforme Zugriffsberechtigungen mit Hilfe von Workflows für regelmäßige Rezertifizierungen oder automatisch über Richtlinien für eine rollenbasierte Zugriffssteuerung***
- ***Verwaltet und verhindert Konflikte bei Geschäftsprozessen mithilfe von Richtlinien zur Trennung von Aufgaben***
- ***Zentralisiert die Steuerung von Benutzerzugriffsrechten und stellt weiterhin die lokale Autonomie mit Hilfe von Self-Service-Funktionen sicher, die auch zur Entlastung von Help-Desk-Mitarbeitern beitragen***
- ***Schnellere Integration neuer Anwendungen und Benutzer durch vorkonfigurierte Richtlinien und Vorlagen***
- ***Unterstützung bei der Prüfung und der Einhaltung von Richtlinien durch das rasche Erstellen detaillierter Berichte***

Automatisiertes und richtlinienbasiertes Management von Benutzeridentitäten mit umfassenden Sicherheitsfunktionen

Um in der heutigen Geschäftswelt bestehen zu können, bieten Unternehmen immer mehr Benutzern – Kunden, Mitarbeitern, Bürgern, Geschäftspartnern und Zulieferern – die Möglichkeit, über Anwendungen, Mainframes, service-orientierte Architekturen, das Web und andere Umgebungen auf Informationen zuzugreifen. Daher müssen CIOs ständig drei wichtige Herausforderungen bewältigen: die Einhaltung interner und gesetzlich vorgeschriebener Richtlinien, die Einhaltung eines effektiven Sicherheitsstandards und das gleichzeitige Erreichen eines messbaren Return-on-Investment.

IBM Tivoli Identity Manager wird diesen Aufgaben durch eine einfach zu implementierende, benutzerfreundliche Lösung mit einem richtlinienbasierten Benutzer- und Rollenmanagement und umfassenden Sicherheitsfunktionen über die gesamte IT-Infrastruktur gerecht. Tivoli Identity Manager bietet:

- *Eine Rollenhierarchie mit optimierter Verwaltung, transparentem Benutzerzugriff und Verknüpfung der Sicht von Geschäftsbenutzern auf die IT-Ressourcen mit der tatsächlichen IT-Implementierung von Benutzerzugriffsrechten*
- *Web-Self-Service für das Management von Geschäftsrollen, Accounts, Gruppenzugehörigkeit und Kennwörtern*
- *Eine integrierte Workflowsteuerkomponente für die automatisierte Vorlage und Genehmigung von Benutzeranforderungen und für eine regelmäßige Zertifizierung von Benutzerzugriffsrechten*
- *Eine leistungsfähige Bereitstellungssteuerkomponente, die Benutzerzugriffsrechte auf der Grundlage der Zugehörigkeit in Geschäftsrollen oder von Anforderungen im Hinblick auf Benutzeraccounts und differenzierten Berechtigungen, wie z. B. gemeinsamen Ordnern oder Web-Portlets, hinzufügt oder entfernt*
- *Eine Reihe von Kontrollen zur Verbesserung der Sicherheit (z. B. präventive Aufgabentrennung (separation of duty) und geschlossener Datenabgleich, bei dem Änderungen erkannt und auf den Zielsystemen korrigiert werden)*
- *Umfassende, vordefinierte Unterstützung für das Verwalten von Benutzerzugriffsrechten und Kennwörtern auf Anwendungen und Systemen sowie ein Toolkit für die schnelle Integration von Management von kundenspezifischen Anwendungen*
- *Flexible Funktionen zur Berichterstellung von Benutzerzugriffsrechten, die die automatische Synchronisation von Benutzerdaten aus verschiedenen Repositorys ausnutzen*

Durch automatisierte Funktionen auf Prüfungen vorbereitet

Tivoli Identity Manager bietet Funktionen für die automatisierte Prüfbarkeit. Hierzu gehören Funktionen für die Zertifizierung differenzierter Zugriffsberechtigungen, die Trennung von Aufgabenbereichen, ein geschlossener Datenabgleich und vordefinierte Berichte, die einen direkten Zugriff für Prüfer ermöglichen und detaillierte IT-Berechtigungen in kundenfreundlichen Beschreibungen dessen abbilden, was Benutzer tatsächlich mit ihrem Zugriff tun können.

Automatische Rezertifizierung von Zugriffsberechtigungen

Mit Tivoli Identity Manager bleiben die einfachen Aufgaben einfach, erweiterte kundenspezifische Anpassungen können jedoch weiterhin vorgenommen werden. Leistungsfähige Funktionen für eine Rezertifizierung von Zugriffsberechtigungen bieten differenzierte, prüfer-orientierte Details für die Einhaltung von Richtlinien, die mit Hilfe von Assistenten und Vorlagen problemlos konfiguriert werden können. Nutzen Sie die Anwendung für folgende Aufgaben:

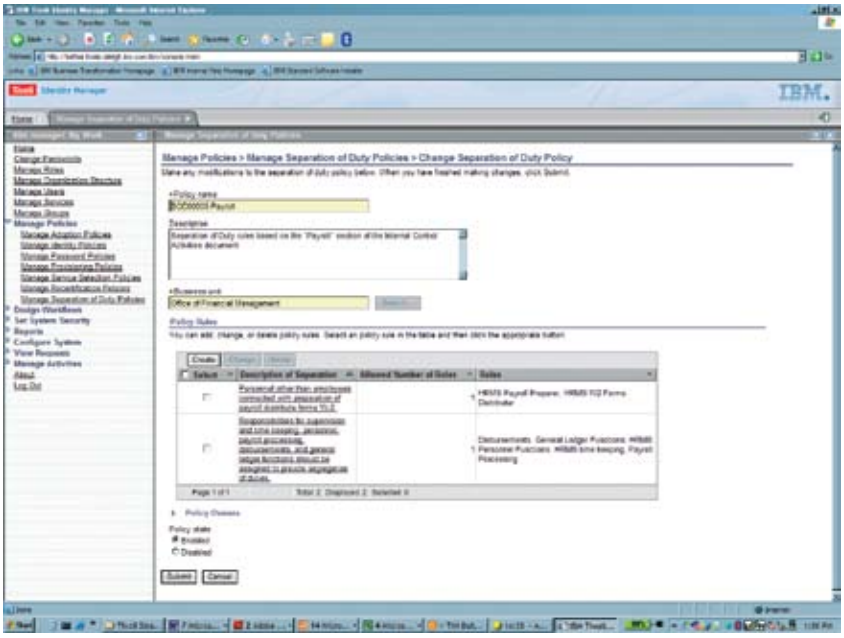
- *Schnelle Definition von Richtlinien für die Rezertifizierung auf der Grundlage von häufig verwendeten Szenarios (Beispiel: "Der Zugriff auf das Data-Warehouse mit Finanzdaten muss vierteljährlich vom Manager eines Mitarbeiters genehmigt werden")*
- *Vereinfachung der administrativen Auswirkungen der Managerfreigabe durch die Rezertifizierung zahlreicher Benutzerrollen, -konten und -gruppen in einem Schritt*
- *Gestalten von innovativen Workflows und Unternehmensprozessen mit dem webbasierten grafischen Workflow-Designer*
- *Durchführen von Compliance-Nachweisen für eine Vielzahl von IT-Ressourcen, die nicht für die automatische Kontobereitstellung konfiguriert wurden*

Trennung von Aufgabenbereichen, um Konflikte zwischen Geschäftsprozessen zu managen

Tivoli Identity Manager hilft mit IT-Benutzerzugriffsberechtigungen bei der Verwaltung von Konflikten zwischen Geschäftsprozessen. Eine präventive, auf Richtlinien basierende Aufgabentrennung bietet Ihnen die Möglichkeit, einen Konflikt zwischen Geschäftsprozessen zu definieren (beispielsweise kann ein Investment-Banker nicht gleichzeitig auch Börsenmakler sein) und eine geeignete Verwaltung von Benutzerzugriffsrechten sicherzustellen. Dies verbindet die Anforderungen in Bezug auf Sicherheit und Einhaltung von Richtlinien, die für die Vermeidung von Konflikten von Geschäftsprozessen wichtig sind, mit den Rollen und Einrichtungsrichtlinien, die die Benutzerzugriffsrechte regeln. Unternehmen können weiterhin ein hohes Maß an Flexibilität beibehalten, indem ein Ausnahmeworkflow den Geschäftsgrund für eine Umgehung der Regeln für Aufgabentrennung einfordert.

Automatischer Datenabgleich zum Erkennen und Korrigieren nicht konformer Accounts

Mit Hilfe von Funktionen für einen geschlossenen Datenabgleich können Verstöße gegen Zugriffsrichtlinien aufgrund fehlerhafter Änderungen, die an einer Verwaltungskonsole einer verwalteten Ressource vorgenommen wurden, automatisch erkannt und behoben werden. Sie können den Abgleich von Zugriffsrechten, die Rezertifizierung sowie die Berichterstellung für folgende Vorgänge verwenden:



Verwaltet und verhindert Konflikte bei Geschäftsprozessen mit Hilfe von Richtlinien zur Aufgabentrennung

- *Automatisches Laden und Abgleichen von Accountdaten*
- *Identifizieren und Löschen von ruhenden und "Schein"-Accounts*
- *Fortlaufender Nachweis der Einhaltung von Richtlinien und die entsprechende Prüfung*
- *Aufbewahren von Änderungsdatensätzen im Zusammenhang mit Zugriffsrechten*

Erstellen von Prüfprotokollen mit detaillierten Berichten

Mit Tivoli Identity Manager sind Sie in der Lage, Berichte zu konsolidierten Workflows sowie zu Änderungen von Zugriffsberechtigungen zu erstellen. Die Überwachung und Berichterstellung zur Einhaltung von Richtlinien umfasst eine Sammlung von Prüfprotokollen, deren Beziehung zueinander und die Berichterstellung, um Compliance-Anforderungen gerecht zu werden. Beispiele für Berichte:

- *Protokoll für Rezertifizierung*
- *Verwaiste und ruhende Accounts*
- *Zusammenfassung für die Aufgabentrennung (separation of duties)*

Durch die Verwendung des IBM Tivoli Common Reporting Module zusammen mit Tivoli Identity Manager können Sie das Erstellen von kundenspezifischen Berichten, die Berichtverteilung und das Ausführen und Verwalten von Berichten von mehreren Tivoli-Produkten nutzen.

Fehlervermeidung durch automatisierte Benutzerverwaltung

Die Benutzerverwaltung kann mithilfe von Rollen- und Self-Service-Anforderungen automatisiert werden. Beide Anforderungen tragen zur Vereinfachung und zu Kostensenkungen bei der Verwaltung des Benutzerzugriffs auf Ressourcen bei und helfen, mögliche Verwaltungsfehler und Inkonsistenzen bei manuellen Prozessen zu vermeiden.

Rollen stellen normalerweise Verbunde von Benutzern und/oder Berechtigungen dar. Zusammen mit der Benutzereinrichtung automatisiert das Rollenmanagement den Verwaltungsprozess für Benutzerzugriffe, indem Zugriffsberechtigungen auf der Grundlage der Rollen, die jedem Benutzer zugeordnet wurden, an die Zielsysteme verteilt werden. Self-Service-Anforderungen können so konfiguriert werden, dass Sie definieren können, welche Attribute für den Self-Service berechtigt sind und für welche eine Genehmigung erforderlich ist. Sie können Anforderungen elektronisch über einen Web-Browser freigeben, ändern oder ablehnen, und Benutzer können automatisch über den Status ihrer Anforderungen informiert werden. Um den Prozess für Benutzer zu vereinfachen, werden über die Schnittstellen zur Selbstregistrierung automatisch Informationen erfasst. Die Freigabe von Benutzeranforderungen kann zudem über eine Workflow-Engine automatisiert werden.

Zugriff über eine Struktur mit hierarchischen Rollen

Tivoli Identity Manager bietet eine Rollenhierarchie, die Beziehungen von Vorgängerrollen zu Mitgliedsrollen festlegt, um über eine Art Vererbung zwischen Rollen Benutzerzugriffsrechte einzurichten. Sie können eine Rollenstruktur verwalten, die Geschäftsrollen (Benutzerverbunde) und/oder Anwendungsrollen (Berechtigungsverbunde) umfasst. Wenn Rollen Einrichtungsrichtlinien zugeordnet werden, können diese automatisch Benutzerzugriffsrechte erteilen, ändern oder löschen. Dies bedeutet, dass weniger Verwaltungsobjekte für das Management des Benutzerzugriffs erforderlich sind und die Transparenz des Zugriffs unternehmensweit verbessert wird.

Vorteile durch anforderungsbasierte Bereitstellung und Zugriffsberechtigungen

Manager und delegierte Administratoren können die Vorteile einer umfassenden, anforderungsbasierten Bereitstellung nutzen, um den Benutzerzugriff für Rollen, Accounts oder differenzierte Zugriffsberechtigungen, wie z. B. gemeinsame Ordner und Web-Portlets, (mit Freigabeworkflow) problemlos anzufordern.

Zudem können Endbenutzer und Geschäftsbereichsleiter aktuelle Zugriffsberechtigungen, Informationen zu Benutzerprofilen und den Status anstehender Anforderungen anzeigen, neuen Zugriff auf Rollen, Accounts oder Berechtigungen für differenzierten Zugriff (z. B. auf gemeinsame Ordner oder LDAP-Gruppen) anfordern, Profilinformationen aktualisieren, Kennwörter ändern oder zurücksetzen und Managementaufgaben ausführen (z. B. die Freigabe von Zugriffsberechtigungen oder die Rezertifizierung vorhandener Zugriffsberechtigungen).

Einfache oder erweiterte Workflows und Richtlinien erstellen

Das leistungsfähige Workflow- und Regelmodul von IBM Tivoli Identity Manager kann problemlos im "einfachen" oder "erweiterten" Modus konfiguriert werden. Im "einfachen Modus" werden zum Implementieren grundlegender Workflows für die Bereitstellung, Rezertifizierung und Compliance-Alerts vordefinierte Vorlagen basierend auf bewährten Verfahren verwendet. Bei der Konfiguration und Einrichtung werden lediglich Dropdown-Listen, Markierungsfelder und Optionsfelder verwendet. Kenntnisse zum Erstellen von Scripts und zur Programmierung sind nicht erforderlich.

Der "erweiterte Modus" umfasst einen grafischen Workflow-Designer mit Drag-and-drop-Funktionen, der ein rasches Verwalten und einfaches Entwickeln von Workflowprozessen zur Unterstützung der unternehmensinternen Einrichtungsrichtlinien ermöglichen. Beispielsweise unterstützt die Workflow-Engine parallele und serielle Freigabeprozesse und bietet außerdem Prüfpunkte in einem Workflowprozess, um die Eingabe zusätzlicher Bereitstellungsinformationen zu ermöglichen.

Gruppenmanagement

Tivoli Identity Manager hilft, die Definition von Gruppen für das Management des Benutzerzugriffs für native Anwendungen und Systeme zu automatisieren und zu zentralisieren. Tivoli Identity Manager ermöglicht außerdem das Hinzufügen, Ändern oder Entfernen von Gruppen und damit die Optimierung des Prozesses zum Definieren des Zugriffs und Zuordnen der Benutzerzugehörigkeit zu den Gruppen.

Self-Service-Funktionen zur Verringerung der Anzahl an Anrufen beim Help-Desk

Durch integrierte intuitive, anpassungsfähige Webschnittstellen zur Selbstverwaltung bietet Tivoli Identity Manager Benutzern die Möglichkeit, Aufgaben wie Kennwortänderung und Anforderung neuer Zugriffsberechtigungen auszuführen, sodass sich die Anzahl teurer Anrufe beim Help-Desk verringert. Beispielsweise ist ein Self-Service-Frage-/Antwortsystem integriert, mit dem Benutzer ohne Anruf beim Help-Desk das übliche Problem des vergessenen Kennworts lösen können. Dank einer hochentwickelten Self-Service-Schnittstelle und einer integrierten Workflow-Engine sind Benutzer in der Lage, Teile ihrer eigenen Informationen sicher und ohne großen Aufwand zu verwalten. Webbasierte, Self-Service-, rollen- und regelbasierte Verwaltungsfunktionen bieten die Möglichkeit, Benutzer je nach Geschäftsanforderungenen zu gruppieren und Funktionen an andere Organisationen und Geschäftsbereiche zu delegieren (z. B.: Wer kann Benutzer hinzufügen, entfernen, ändern und anzeigen und Benutzerkennwörter zurücksetzen?).

> *IBM Tivoli ist im "Leaders Quadrant" des "Magic Quadrant for User Provisioning" von Gartner, Inc. aufgeführt.*
>
> *– Gartner Magic Quadrant for User Provisioning, Research Note G00159740, 15. August 2008* [1]

Optimale Funktionalität für den Benutzer dank anpassungsfähiger Schnittstelle

Tivoli Identity Manager basiert nicht auf einem "one-site-fits-all"-Ansatz für das Identitätsmanagement. Es handelt sich vielmehr um eine einfache, extrem anpassungsfähige Benutzerschnittstelle, die vordefinierte Konfigurationen für diejenigen umfasst, die in den einzelnen Phasen des Lebenszyklus beteiligt sind, wie z. B. Prüfer, Endbenutzer, Manager, Help-Desk-Mitarbeiter, Anwendungseigentümer und Administratoren. Auf diese Weise können Benutzer die Informationen anzeigen, die für sie am wichtigsten sind.

Die Schnittstelle lässt sich problemlos anpassen und in eine bereits vorhandene Intranet- oder Extranet-Site integrieren. Anpassungsoptionen umfassen Style-Sheets und On/Off-Konfigurationsoptionen, z. B. ob Navigationspfade oder eine Headermarkierung angezeigt werden sollen. Zudem müssen Anpassungen während Software-Upgrades nicht erneut implementiert werden.

Rasche Konfiguration des Systems und Integration neuer Services

Tivoli Identity Manager hilft Ihnen, den Zeitraum für die Aktivierung neuer Accounts und die Integration neuer verwalteter Services deutlich zu verkürzen. Vorinstallierte Adapter, über einen Assistenten gesteuerte Vorlagen und integrierte Accountvorlagen tragen zu einer rascheren Implementierung und einem geringeren Einarbeitungsaufwand für neue Benutzer bei.

Unterstützung vorhandener, neuer und angepasster Umgebungen mit wenig oder gar keiner Codierung

Tivoli Identity Manager bietet eine vordefinierte Unterstützungsfunktion für mehr als 50 verwaltete Endsysteme, die remote oder mit einem lokalen Adapter verwaltet werden können und vereinfacht damit die Implementierung. Die Software umfasst zudem Tools, mit denen diese neuen Geschäftsressourcen integriert werden können, wenn sie hinzugefügt werden.

Durch den dynamischen Schemaerkennungsprozess und die flexible Architektur sorgt die integrierte IBM Tivoli Directory Integrator-Technologie bei Tivoli Identity Manager für administrative Kontrollmöglichkeiten über unternehmenseigene Anwendungen – ohne dass Sie Code schreiben oder verwalten müssen.

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie IBM Tivoli Identity Manager und integrierte Lösungen von IBM Ihrem Unternehmen bei der Steigerung der IT-Effizienz, der Verringerung der Verwaltungskosten und der Einhaltung der Richtlinien unterstützt, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter:

ibm.com/tivoli/solutions/security

Tivoli-Software von IBM

Tivoli-Software stellt verschiedene Angebote und Funktionen bereit, die das IBM Service-Management unterstützen – einen skalierbaren, modularen Ansatz zur Bereitstellung effizienterer und effektiverer Services für Unternehmen. Tivoli-Software wird den Anforderungen von Unternehmen aller Größen gerecht und ermöglicht Ihnen die Bereitstellung exzellenter Services, die auf Ihre geschäftlichen Ziele abgestimmt sind – durch die Integration und Automatisierung von Prozessen, Arbeitsabläufen und Aufgaben. Die sichere, auf offenen Standards basierende Tivoli-Service-Management-Plattform wird durch proaktive Lösungen für das operative Management ergänzt, die für durchgängige Transparenz und Kontrolle sorgen. Die Plattform wird außerdem durch erstklassige IBM Service- und Supportangebote sowie ein Netzwerk von 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 Global Financing bietet Finanzierungslösungen, die auf Ihre IT-Anforderungen zugeschnitten sind. Weitere Informationen zu attraktiven Raten, flexiblen Zahlungsplänen und Krediten sowie zum Rückkauf und zur Entsorgung von Komponenten finden Sie auf folgender Website:

ibm.com/financing

Tivoli Identity Manager auf einen Blick

Unterstützte Plattformen:

- HP-UX
- IBM AIX
- Red Hat Enterprise Linux®
- Sun Solaris
- SUSE Linux Enterprise Server
- Microsoft® Windows® Server
- z/OS

Unterstützte verwaltete Systeme:

Kann in Dutzende bewährter Anwendungen und Plattformen integriert werden:

- Betriebssysteme
- Datenbanken, Verzeichnisse, Content-Management-Systeme
- Zugriffssteuerungssysteme
- E-Mail- und Messaging-Systeme
- Service-Desks
- Geschäftsanwendungen und Enterprise-Resource-Planning-Systeme

[1] "Gartner Magic Quadrant" wurde 2008 von Gartner Inc. urheberrechtlich geschützt. Er wird mit Genehmigung verwendet. Bei "Magic Quadrant" handelt es sich um eine grafische Darstellung eines Markts in einem und für einen bestimmten Zeitraum. Sie veranschaulicht die Analyse Gartners, wie sich bestimmte Anbieter an Kriterien für diesen Markt, wie von Gartner definiert, messen lassen. Gartner unterstützt keine Anbieter, Services oder Produkte, die im "Magic Quadrant" aufgeführt sind und gibt keine Empfehlungen für IT-Benutzer ab, sich nur für diese Anbieter zu entscheiden, die im "Quadrant" der führenden Unternehmen aufgelistet sind. Der "Magic Quadrant" ist lediglich ein Recherche-Tool und kein spezieller Leitfaden. Gartner gibt keinerlei Gewährleistung (ausdrücklich oder stillschweigend) bezüglich dieser Recherche, einschließlich den Gewährleistungen der Handelsüblichkeit oder Verwendbarkeit für einen bestimmten Zweck.

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

Recycelbar, bitte recyceln

TID10294-DEDE-02