IBM Tivoli Identity Manager

Automatizzare facilmente la gestione del ciclo di vita dei ruoli, delle identità e degli accessi degli utenti

Punti principali

- Ridurre i costi e gestire i problemi di conformità, automatizzando la creazione, la modifica, la ricertificazione e l'eliminazione dei privilegi concessi agli utenti, nel corso del loro intero ciclo di vita.
- Semplificare la progettazione, l'implementazione e la convalida della struttura dei ruoli e degli accessi all'interno dell'intera organizzazione aziendale.
- Gestire e prevenire i conflitti nelle politiche di business, attraverso il controllo e l'applicazione della separazione delle mansioni.

Una gestione delle identità e degli eccessi basata su politiche

Per competere in modo efficace in un mercato impegnativo come quello attuale, le organizzazioni aumentano il numero degli utenti – clienti, dipendenti, cittadini, partner e fornitori – autorizzati ad accedere alle informazioni attraverso applicazioni, mainframe, architetture SOA (Service-Oriented Architecture), il Web e altri ambienti. Di conseguenza, i CIO (Chief Information Officer) si trovano costantemente di fronte a tre problemi principali: soddisfare i requisiti prescritti dalle politiche aziendali interne e dalla normativa vigente, garantire condizioni di sicurezza ottimali e, nello stesso tempo, ottenere un ROI (Return On Investment) significativo.

IBM Tivoli Identity Manager consente alle organizzazioni di affrontare questi problemi con una soluzione per la gestione delle identità e degli accessi facile da implementare e utilizzare, che permette una gestione degli utenti e dei ruoli basata su politiche ed estremamente sicura all'interno dell'intera infrastruttura IT. Tramite l'utilizzo di ruoli, account e permessi di accesso, consente di automatizzare la creazione, la modifica e l'eliminazione dei privilegi assegnati agli utenti nel corso del loro intero ciclo di vita. Tivoli Identity Manager offre:

- Una gerarchia dei ruoli che semplifica l'amministrazione, assicura la visibilità degli accessi degli utenti e contribuisce ad annullare il divario tra la percezione delle risorse IT da parte degli utenti aziendali e l'effettiva implementazione tecnologica dei diritti di accesso assegnati agli utenti stessi.
- Funzioni self-service che consentono di gestire autonomamente via Web i ruoli, gli account, l'appartenenza ai gruppi e le password.
- Gestione dei gruppi, che semplifica l'amministrazione degli utenti e ne riduce il costo, offrendo la possibilità di aggiungere, eliminare o modificare gli attribuiti di un gruppo all'interno della console di Tivoli Identity Manager.
- Un motore di workflow integrato, che consente di automatizzare l'invio e l'approvazione delle richieste degli utenti e di certificarne periodicamente i diritti di accesso.

- Un motore di provisioning estremamente affidabile, che aggiunge ed elimina i diritti di accesso degli utenti in base alla loro appartenenza ai ruoli aziendali o alle richieste di account e singole autorizzazioni, come quelle riguardanti cartelle condivise o portlet Web.
- Una serie di controlli che rafforzano la sicurezza, tra cui la separazione preventiva delle mansioni e il ciclo completo di riconciliazione che rileva e corregge le modifiche apportate ai sistemi target nativi.
- Ampio supporto immediatamente utilizzabile per gestire i diritti di accesso e le password degli utenti su applicazioni e sistemi, oltre a un toolkit di integrazione rapida per la gestione di applicazioni personalizzate.
- Documentazione flessibile dei diritti di accesso degli utenti, che utilizza la sincronizzazione automatica dei dati memorizzati in archivi differenti.

Semplificare la progettazione di una struttura efficace dei ruoli e degli accessi

La funzionalità di role mining e gestione del ciclo di vita dei ruoli, fornita dal componente IBM Security Role and Policy Modeler, semplifica ed accelera la progettazione di una struttura dei ruoli e degli accessi per l'azienda. Inoltre, questa funzionalità automatizza il processo di convalida delle informazioni sugli accessi e della struttura dei ruoli con la partecipazione dei responsabili aziendali. Tivoli Identity Manager fornisce una struttura efficace per la gestione dei ruoli, che contribuisce ad annullare il divario tra la percezione delle risorse IT da parte degli utenti aziendali e l'effettiva implementazione tecnologica dei diritti di accesso assegnati agli utenti stessi, semplificando l'amministrazione dei diritti di accesso degli utenti e riducendone il costo. Questa soluzione offre una serie di controlli aggiuntivi per gestire la sicurezza interna ed estendere i processi esistenti per la creazione e la modifica dei diritti di accesso all'intera organizzazione aziendale.

I CIO e i direttori IT sono impegnati a migliorare o semplificare il modo in cui i diritti di accesso vengono forniti. Questi processi sono molto impegnativi a causa delle analisi necessarie e richiedono un'interazione costante con i responsabili delle attività di business. Generalmente, questi progetti finiscono per richiedere troppo tempo e producono risultati già obsoleti nel momento in cui il progetto viene attuato. IBM Security Role and Policy Modeler offre una piattaforma che facilita il processo iterativo di definizione dei ruoli e role mining. Questo componente consente di creare un ambiente di test facilmente utilizzabile dagli utenti aziendali, in cui è possibile modellare e simulare scenari e politiche di accesso per creare una struttura dei ruoli e dei privilegi più efficace per l'azienda. Aiuta gli analisti ad affinare le definizioni dei ruoli con un'ampia serie di strumenti analitici all'avanguardia. Contribuisce, inoltre, ad automatizzare il processo di gestione della struttura dei ruoli in ogni sua fase, offrendo una piattaforma per l'automazione dei processi di approvazione e certificazione della struttura dei ruoli con la partecipazione dei responsabili aziendali. Tutto ciò consente di:

- Ridurre il tempo necessario per raccogliere i dati relativi agli accessi degli utenti, filtrarli e convalidarli, analizzarli per rilevare modelli di accesso comuni e, infine, produrre una struttura dei ruoli efficace.
- Ottenere una rapida approvazione da parte del business, per accelerare l'implementazione o la certificazione della struttura dei ruoli.
- Delegare le decisioni riguardanti le politiche di accesso ai responsabili delle attività di business.

Superare qualsiasi controllo con funzioni automatizzate

Tivoli Identity Manager consente di automatizzare le operazioni necessarie a superare eventuali verifiche da parte degli organi di controllo, grazie alla certificazione di diritti di accesso ad elevata granularità, alla separazione dei compiti, alla riconciliazione a circuito chiuso e a report precostituiti che offrono ai revisori un accesso diretto alle informazioni e associano autorizzazioni di basso livello a descrizioni comprensibili delle operazioni che gli utenti sono effettivamente autorizzati ad eseguire sulle risorse cui hanno accesso.

Ricertificazione automatica dei diritti di accesso

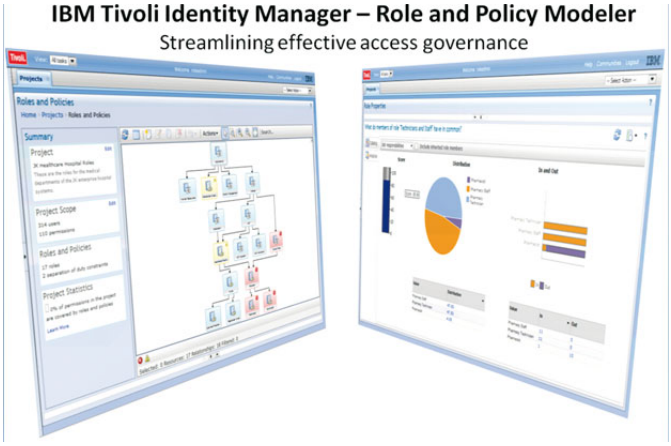
Tivoli Identity Manager impedisce che attività semplici diventino complesse, pur offrendo un'elevata personalizzazione. Le funzionalità avanzate per la ricertificazione dei diritti di accesso forniscono informazioni dettagliate e facilmente comprensibili per il controllo della conformità e politiche facilmente configurabili tramite procedure guidate e modelli predefiniti. Queste funzionalità consentono di:

- Definire rapidamente regole di ricertificazione basate sugli scenari più frequenti, come ad esempio: "l'accesso al data warehouse finanziario deve essere approvato dal manager di un dipendente una volta ogni trimestre."
- Ridurre l'impatto amministrativo dell'approvazione da parte dei manager, tramite l'aggregazione delle ricertificazioni di ruoli, account e gruppi di un utente.

- Definire workflow e processi organizzativi avanzati, utilizzando l'apposito tool grafico di progettazione basato su Web.
- Verificare la conformità alle regole di accesso per un gran numero di risorse IT non configurate per il provisioning automatizzato degli account.

Stabilire la separazione delle mansioni per gestire i conflitti nei processi di business

Tivoli Identity Manager facilita la gestione dei conflitti nei processi di business attraverso la regolamentazione dei diritti di accesso concessi agli utenti. La separazione dei compiti preventiva e basata su regole consente di definire un conflitto di interesse (ad esempio, un addetto agli investimenti bancari non può essere nello stesso tempo un intermediario finanziario) e di assicurare un'amministrazione corretta dei diritti di accesso. Ciò associa i requisiti di sicurezza e conformità essenziali per prevenire i conflitti di interesse ai ruoli e alle politiche di provisioning che regolano i diritti di accesso degli utenti. Le organizzazioni possono comunque operare in modo flessibile, utilizzando un'apposito workflow per giustificare l'assegnazione di ruoli conflittuali ad uno stesso utente quando è necessaria un'eccezione alla politica della separazione delle mansioni.



Gestire i ruoli e le politiche di accesso con visualizzazioni grafiche dei progetti e analisi dettagliate.

Utilizzare la riconciliazione automatizzata per rilevare e correggere gli account non conformi

Le funzioni di riconciliazione "a ciclo chiuso" consentono di rilevare e correggere eventuali violazioni delle regole di accesso dovute a modifiche erroneamente apportate tramite le console di amministrazione native delle risorse gestite. È possibile utilizzare la riconciliazione, la ricertificazione e la documentazione dei diritti di accesso per:

- Caricare e riconciliare automaticamente i dati relativi agli account.
- Identificare ed eliminare gli account dormienti o fantasma.
- Dimostrare la conformità alle politiche aziendali interne e alla normativa vigente agli organi di controllo.
- Registrare le modifiche relative ai diritti di accesso.

Registrare le modifiche apportate con report dettagliati

Tivoli Identity Manager consente di produrre report contenenti informazioni riguardanti flussi di lavoro eseguiti e le modifiche apportate ai diritti di accesso. Il monitoraggio e la documentazione della conformità alle regole di accesso includono la registrazione, la correlazione e documentazione delle modifiche apportate ai diritti di accesso, come richiesto dalla normativa vigente. Gli esempi di report includono:

- Cronologia delle ricertificazioni.
- Account orfani e dormienti.
- Prospetto riepilogativo della separazione delle mansioni.

Utilizzando IBM Tivoli Common Reporting Module insieme a Tivoli Identity Manager, è possibile creare e distribuire report personalizzati, nonché gestire i report da più prodotti Tivoli.

Ridurre gli errori, automatizzando l'amministrazione degli utenti

L'amministrazione degli utenti può essere automatizzata, utilizzando i ruoli e le richieste self-service. Entrambi questi elementi consentono di semplificare l'amministrazione dell'accesso degli utenti alle risorse e di ridurne il costo, e contribuiscono a ridurre gli errori e le incongruenze che caratterizzano i processi manuali. I ruoli consistono

generalmente in gruppi di utenti e/o permessi. La gestione dei ruoli, insieme alle funzionalità di provisioning, automatizza il processo di amministrazione degli accessi, concedendo i diritti di accesso ai sistemi di destinazione in base ai ruoli assegnati a ciascun utente. È possibile configurare le richieste self-service in modo da definire quali attributi possano essere impostati autonomamente dagli utenti e quali debbano essere approvati. Le richieste possono essere approvate, modificate o respinte elettronicamente tramite un browser Web ed è possibile notificare automaticamente agli utenti lo stato delle loro richieste. Per semplificare il processo, le interfacce di autoregistrazione e autoiscrizione raccolgono informazioni automaticamente e, tramite un motore di workflow, è possibile automatizzare l'approvazione delle richieste inviate dagli utenti.

Gestire gli accessi tramite un'organizzazione gerarchica dei ruoli

Tivoli Identity Manager offre una gerarchia dei ruoli che definisce relazioni padre/figlio tra gli stessi, per creare automaticamente permessi di accesso attraverso il concetto di ereditarietà tra i ruoli. È possibile amministrare una struttura dei ruoli che contenga ruoli aziendali(gruppi di utenti) e/o ruoli applicativi (raccolte di permessi). Associando i ruoli alle politiche di provisioning, è possibile concedere, modificare o eliminare automaticamente i diritti di accesso degli utenti. Di conseguenza, Tivoli Identity Manager riduce il numero di oggetti amministrativi utilizzati per gestire gli accessi e ne migliora la visibilità all'interno dell'intera organizzazione.

Trarre vantaggio da processi di provisioning e permessi di accesso basati su richieste

I manager e gli amministratori delegati possono trarre vantaggio da un processo di provisioning completo e basato su richieste per richiedere facilmente (con il workflow di approvazione) l'accesso degli utenti a ruoli, account e singoli permessi, come quelli relativi a cartelle condivise e portlet Web.

Inoltre, gli utenti finali e i responsabili delle linee di business sono in grado di visualizzare lo stato attuale dei diritti di accesso, delle informazioni contenute nei profili personali e delle richieste pendenti; richiedere un nuovo accesso a ruoli, account o singoli privilegi (ad esempio, cartelle condivise o gruppi LDAP [Lightweight Directory Access Protocol]); aggiornare le informazioni contenute nei profili; modificare o reimpostare le password ed eseguire attività gestionali, come l'approvazione di nuovi di diritti di accesso o la ricertificazione dei diritti di accesso esistenti.

Stabilire flussi di lavoro e criteri di accesso semplici o avanzati

Il potente motore per la gestione dei flussi di lavoro e delle politiche di Tivoli Identity Manager può essere configurato per operare in modalità "semplice" o "avanzata". In "modalità semplice", il motore utilizza modelli predefiniti basati su best practice per implementare workflow basilari di provisioning, ricertificazione e avvisi di conformità. L'utilizzo di semplici elenchi a tendina, caselle di spunta e pulsanti di opzione rende la configurazione estremamente semplice; non è richiesta alcuna conoscenza di scripting o programmazione.

La "modalità avanzata" offre un tool grafico per la progettazione dei workflow con funzionalità drag-and-drop, che consente di organizzare rapidamente e sviluppare facilmente flussi di lavoro conformi alle politiche di provisioning dell'organizzazione. Ad esempio, il motore di workflow supporta processi di approvazione paralleli e seriali e consente di stabilire dei punti di controllo per l'eventuale inserimento di informazioni aggiuntive nel corso del processo di provisioning.

Gestire gli accessi utilizzando i gruppi

Tivoli Identity Manager consente di automatizzare e centralizzare la definizione dei gruppi utilizzati per gestire gli accessi degli utenti su applicativi e sistemi nativi. È possibile aggiungere, modificare o eliminare i gruppi direttamente da Tivoli Identity Manager e semplificare il processo di definizione degli accessi e assegnazione degli utenti ai gruppi.

Utilizzare funzioni self-service per ridurre le chiamate al supporto tecnico

Tivoli Identity Manager offre interfacce Web intuitive e personalizzabili, che consentono agli utenti di eseguire autonomamente attività, come modifica delle password e richiesta di nuovi diritti di accesso, contribuendo a ridurre le costose chiamate al supporto tecnico. Ad esempio, un sistema di challenge/response consente agli utenti di risolvere autonomamente il frequente problema delle password

dimenticate, senza chiamare il supporto tecnico. Un'interfaccia self-service avanzata e un motore di workflow integrato aiutano gli utenti a gestire in modo facile e sicuro alcune delle proprie informazioni. Le funzioni amministrative self-service, basate su Web, ruoli e regole, consentono di raggruppare gli utenti secondo le esigenze di business e delegare le funzioni gestionali, come l'aggiunta, l'eliminazione, la modifica e la visualizzazione degli utenti e la reimpostazione delle password, ad altre organizzazioni e unità aziendali, quando necessario.

L'interfaccia personalizzabile offre all'utente un'esperienza ottimale

Tivoli Identity Manager non è stato realizzato adottando un approccio indifferenziato alla gestione delle identità. Piuttosto, offre un'interfaccia semplice ed altamente personalizzabile, che include differenti configurazioni immediatamente utilizzabili per i diversi partecipanti a ciascuna delle fasi del ciclo di vita, tra cui revisori, utenti finali, manager, personale addetto all'help-desk, titolari di applicazioni e amministratori; in tal modo, gli utenti accedono alle informazioni più importanti per le rispettive mansioni.

È possibile personalizzare facilmente l'interfaccia e integrarla agevolmente all'interno di una rete interna o esterna esistente. Le opzioni di personalizzazione includono l'utilizzo di style sheets e la possibilità di attivare o disattivare determinati parametri di configurazione, come ad esempio se visualizzare o meno le singoli elementi durante la navigazione o il banner all'inizio della pagina. Gli aggiornamenti del software non comportano la necessità di personalizzare nuovamente l'interfaccia.

Configurare sistemi e aggiungere nuovi servizi rapidamente

Tivoli Identity Manager può aiutarvi a ridurre notevolmente il tempo necessario per attivare nuovi account e aggiungere nuovi servizi gestiti. Gli adattatori preinstallati, i modelli assistiti da procedure guidate e i profili amministrativi predefiniti contribuiscono ad accelerare l'implementazione della soluzione e a facilitarne l'apprendimento da parte dei nuovi utenti.

Supportare ambienti esistenti, nuovi e personalizzati senza o con una minima programmazione

Tivoli Identity Manager supporta immediatamente la gestione di oltre 50 sistemi, che possono essere amministrati in remoto o tramite un adattatore locale, semplificando l'implementazione. Fornisce anche strumenti che facilitano l'integrazione delle risorse aziendali progressivamente aggiunte.

Grazie a un processo di rilevamento dinamico degli schemi e a un'architettura flessibile, la tecnologia di IBM Tivoli Directory Integrator, integrata in Tivoli Identity Manager, consente di controllare e gestire le applicazioni sviluppate internamente dalle organizzazioni, senza richiedere alcuna attività di programmazione.

Tivoli Identity Manager in sintesi

Piattaforme supportate:

- IBM AIX
- Red Hat Enterprise Linux®
- Sun Solaris
- SUSE Linux Enterprise Server
- Microsoft® Windows® Server

Sistemi supportati:

Si integra con molte applicazioni e piattaforme diffusamente utilizzate:

- Sistemi operativi
- Database, directory, sistemi di gestione dei contenuti
- Sistemi di controllo degli accessi
- Sistemi di posta elettronica e messaggistica
- Sistemi di assistenza
- Applicazioni aziendali e sistemi ERP (Enterprise Resource Planning)

Ulteriori informazioni

Per ulteriori informazioni su come IBM Tivoli Identity Manager e le soluzioni di sicurezza fornite da IBM vi consentano di adattarvi ai nuovi problemi di sicurezza, ridurre i costi di amministrazione e operare nel rispetto delle politiche aziendali, contattate il vostro rappresentante o Business Partner IBM, o visitate il sito **ibm.com**/software/it/tivoli/security

Informazioni sul software IBM Tivoli

Il software Tivoli fornito da IBM facilita una gestione efficiente ed efficace delle risorse, delle attività e dei processi IT, consentendo di soddisfare esigenze di business costantemente mutevoli, garantendo una gestione flessibile e dinamica dei servizi IT e contribuendo a ridurre i costi. Il portafoglio Tivoli comprende software per la gestione della sicurezza, della conformità, dello storage, delle prestazioni, della disponibilità, delle configurazioni, delle operazioni e del ciclo di vita dell'infrastruttura IT e si basa sui servizi, sul supporto e sulla ricerca all'avanguardia di IBM.

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page di IBM Italia si trova all'indirizzo **ibm.com**/it

IBM, il logo IBM, ibm.com, AIX e Tivoli sono marchi o marchi registrati di International Business Machines Corporation negli Stati Uniti e/o in altri paesi. Se questi e altri termini commerciali di IBM sono contrassegnati da un simbolo del marchio (® o ™) alla loro prima ricorrenza nel presente documento informativo, tali simboli indicano marchi registrati o non registrati di proprietà di IBM negli Stati Uniti al momento della pubblicazione del presente documento informativo. Tali marchi possono anche essere marchi registrati o comunemente riconosciuti in altri paesi.

Un elenco aggiornato dei marchi IBM è disponibile sul Web nella pagina "Informazioni su copyright e marchi" all'indirizzo: **ibm.com**/legal/copytrade.shtml

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Microsoft e Windows sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Altri nomi di società, prodotti e servizi possono essere marchi o marchi di servizio di altre società.

I riferimenti contenuti in questa pubblicazione a prodotti, programmi o servizi di IBM non implicano la volontà, da parte di IBM, di rendere tali prodotti, programmi o servizi disponibili in tutti i paesi in cui IBM opera.

Qualsiasi riferimento a prodotti, programmi o servizi di IBM non implica che possano essere usati solo prodotti, programmi o servizi IBM. In alternativa, è possibile utilizzare qualsiasi prodotto, programma o servizio funzionalmente equivalente.

Questa pubblicazione è fornita a titolo esclusivamente informativo. Le informazioni sono soggette a modifiche senza preavviso. Per informazioni più aggiornate sui prodotti e sui servizi IBM, contattate l'ufficio vendite o il rivenditore IBM più vicino.

IBM non fornisce assistenza legale, contabile o di controllo e non dichiara né garantisce che i propri prodotti o servizi siano conformi alla legislazione vigente. I clienti sono responsabili dell'osservanza di ogni legge ed obbligo normativo applicabile, comprese le leggi e le norme nazionali.

Le fotografie possono mostrare dei prototipi.

© Copyright IBM Corporation 2011
Tutti i diritti riservati.

Si prega di riciclare

Tivoli software

TID10294-ITIT-03