Tivoli® software

IBM Tivoli Federated Identity Manager

Points forts

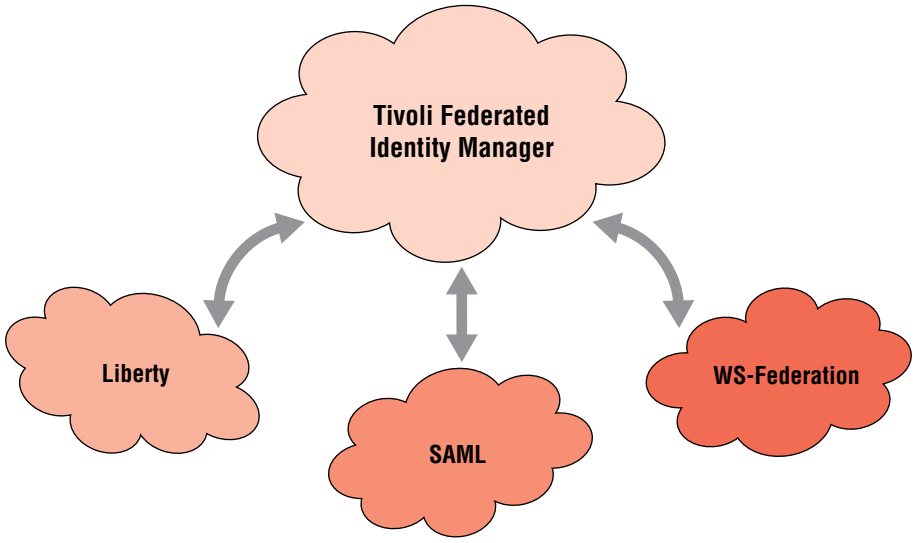
- Facilite les transactions de services sécurisées sur les environnements mainframe et distribués
- Prend en charge des fonctions à signature unique (SSO) fédérées afin d'optimiser la satisfaction de l'utilisateur et les coûts
- Prendre en charge un grand nombre de standards ouverts, dont le SAML (Security Assertion Markup Language) 1.x et 2.0, le Liberty Alliance ID-FF 1.x (Identity Federation Framework) et des spécifications de sécurité des services Web (avec WS-Federation, WS-Security et WS-Trust)
- Fournit des fonctions intégrées de rapport et de collecte de données d'audit afin de faciliter la conformité avec les politiques réglementaires et commerciales
- Optimise l'investissement dans les infrastructures d'identité et les coûts opérationnels par des fonctions parasites fédérées

Les entreprises sont de plus en plus contraintes d'étendre les informations et données critiques au-delà des limites de la société. Les partenaires, les clients, les distributeurs, les agences et les fournisseurs exigent un accès à des données qui s'étendent au-delà des ressources humaines de l'entreprise, de la gestion des relations avec la clientèle (GRC), de l'ERP et des systèmes centraux existants.

Avec la nécessité d'élargir cette intégration et cet accès, des redondances dans les processus surviennent très souvent, comme la prolifération des identifiants de connexion multiples, susceptibles d'avoir un impact aussi bien sur la productivité que sur la satisfaction de l'utilisateur. Par exemple, les clients qui se connectent au site de courtage d'une société de services financiers à service complet à l'aide d'une identité et d'un mot de passe sont obligés d'utiliser une identité et un mot de passe différents pour accéder à la filiale de carte de crédit appartenant à cette même société de services financiers. La société doit alors gérer deux fois l'infrastructure pour un coût deux fois supérieur, et les clients et les employés sont contraints d'utiliser des identifiants multiples.

Pour aider à traiter les défis de l'échange d'informations inter-entreprises, de nombreuses sociétés abandonnent le modèle classique des processus métier rigides pour adopter une approche plus souple, plus accessible et réutilisable, les services Web. A l'inverse d'une approche de remplacement, une architecture orientée service (SOA) est conçue pour permettre une utilisation maximale des équipements informatiques nouveaux et existants.

La gestion d'identité fédérée peut vous aider à intégrer et étendre les services dans l'écosystème de votre entreprise, tout en minimisant les risques liés au partage d'identités et de services. IBM Tivoli® Federated Identity Manager permet aux utilisateurs de se connecter avec une signature unique aux sites de différentes entreprises, tout en préservant la confidentialité de leurs données d'utilisateur. Conçu pour



minimiser l'impact sur les applications d'entreprise, Tivoli Federated Identity Manager vous aide à réduire les coûts et à accélérer les délais de déploiement pour intégrer les applications au sein de votre infrastructure de collaboration.

Gérer différents standards à l'aide d'une seule solution

L'un des principaux défis à relever dans l'adoption d'une gestion d'identité fédérée par les entreprises est le nombre de standards de fédération d'identités différents. Par exemple, les standards SAML, Liberty Alliance et WS-Federation font appel à des technologies similaires mais reposent sur des protocoles différents et fournissent des fonctions différentes. En vous appuyant sur des standards ouverts, vous pouvez simplifier l'intégration de services inter-domaines et limiter les redondances entre les comptes d'utilisateur. Et sur le plan économique, vous pouvez profiter des données de sécurité des partenaires et bénéficier d'un modèle opérationnel simplifié pour l'authentification et l'autorisation dans l'ensemble de l'écosystème de vos partenaires, sans investissement superflu. Avec un très faible investissement supplémentaire de votre part, vous pouvez largement accroître le contenu, la valeur d'entreprise correspondante et l'attraction des utilisateurs vis-à-vis de vos sites Web. Tivoli Federated Identity Manager permet de garantir une expérience SSO sécurisée et continue pour vos utilisateurs.

Tivoli Federated Identity Manager est conçu pour interopérer avec la grande diversité de standards de fédération que vos partenaires existants ou potentiels sont susceptibles d'utiliser. En ayant recours à Tivoli Federated Identity Manager, vous déployez une solution qui vous permet de :

- prendre en charge la plus large fonctionnalité de fédération en permettant la personnalisation sécurisée SSO et la sécurité des services Web via les standards SAML 1.1.x et 2.0, Liberty ID-FF et WS-Federation.
- prendre en charge la gestion de l'identité à travers une architecture SOA grâce à l'utilisation de WS-Trust pour l'échange et la transformation d'identités et d'attributs.
- simplifier l'intégration de l'identité et de la sécurité, avec notamment des relations de confiance entre les plateformes d'application utilisant WS-Security et WS-Trust.
- communiquer des informations d'authentification et d'identification sur les partenaires commerciaux via une meilleure prise en charge des jetons de sécurité multiples, y compris des PassTickets, des certificats x.509 et des jetons Kerberos.
- automatiser l'approvisionnement des droits et des comptes d'utilisateur, à l'aide de WS-Provisioning.

Mettre en œuvre la signature unique (SSO) dans l'écosystème de votre entreprise

Comptant parmi l'une des premières étapes pour bénéficier des avantages d'un SOA, les capacités SSO fédérées peuvent vous aider à accélérer le temps de réalisation en intégrant les informations de différents domaines

au niveau de l'interface utilisateur. Les protocoles SSO fédérés, comme le SAML et WS-Federation, fournissent des moyens standard interopérables à différents partenaires commerciaux de fédération afin de négocier la présentation de données d'identification relatives à un utilisateur d'un fournisseur d'identité à un fournisseur de fédération sécurisée. Avec le SSO, les utilisateurs peuvent naviguer en continu sur les sites Web tout en conservant un seul et unique identifiant de connexion, et bénéficier de vues agrégées qui fournissent des informations essentielles dans le contexte du processus métier.

Les avantages du SSO, comme une productivité améliorée, une meilleure satisfaction et des coûts réduits, peuvent rapidement s'éroder si les fonctions SSO ne sont pas intégrées efficacement à vos applications d'entreprise. Par exemple, l'utilisation d'interfaces de programmation propriétaires (API) peut exiger d'importantes modifications sur vos applications, nécessitant beaucoup de temps et d'argent. Dans le même temps, cela peut limiter votre souplesse à ajouter des protocoles et des relations de fédérations pour répondre à vos besoins commerciaux en constante évolution.

Configurations matérielles et logicielles requises

Plateformes prises en charge

- IBM AIX® 5.2 et 5.3
- Sun Solaris 9 et 10 SPARC
- Red Hat Enterprise Linux® Advanced Server (IA32) 3.0 and 4.0 for IBM System z™ et Intel® Architecture, 32 bits
- SUSE Linux Enterprise Server 9 for System z and Intel Architecture, 32 bits
- z/OS, Version 1, version 6 et version 7 (pour composant WSSM uniquement)
- Serveur Microsoft Windows® 2003

Standards supportés

- SSO et fédération d'identité entre les fournisseurs d'identité et les prestataires de services utilisant :
  - SAML 1.0, 1.1, 2.0
  - Liberty ID-FF 1.1, 1.2
  - WS-Federation
    - des services de jetons de sécurité utilisant WS-Trust
    - Les types de jetons standard suivants sont pris en charge dans les en-têtes WS-Security des messages SOAP:
      - jetons SAML
      - jetons de nom d'utilisateur
      - jetons X.509
      - jetons Kerberos
      - jetons binaires
- Intégrité des jetons WS-Security grâce à des signatures numériques XML
- Confidentialité des jetons WS-Security avec chiffrement XML
- Prise en charge d'approvisionnement fédéré avec WS-Provisioning
- Contrat JACC (Java™ Authorization Contract for Containers) pour l'autorisation Java
- Prise en charge de la sécurité Java 2
- Architecture OATH (Open Authentication Reference Architecture)

En s'appuyant sur le proxy inverse d'IBM Tivoli Access Manager for e-business, leader du marché, Tivoli Federated Identity Manager vous permet d'intégrer une application Web via une connexion HTTP/HTTPS. La connexion souple entre la couche application et la fonctionnalité SSO fédérée supprime le besoin d'utiliser des API propriétaires et vous permet de connecter un grand nombre d'applications Web sur votre environnement fédéré, avec un minimum de modifications sur vos applications. Par ailleurs, les applications et leurs intergiciels et serveurs associés peuvent être mis à niveau sans modifier l'intégration à vos services SSO fédérés. De la même façon, de nouveaux protocoles et relations de fédération peuvent être ajoutés, en évitant quasiment tout impact sur les applications.

Déployer un contrôle d'accès à base de règles

Pour vous permettre de profiter pleinement des identités d'utilisateur que vous gérez avec Tivoli Federated Identity Manager, le logiciel comprend le même serveur de règles que le logiciel primé Tivoli Access Manager for e-business. Outre la prise en charge de vos initiatives SSO, le serveur de règles vous aide à définir et à administrer les règles de sécurité sur vos services Web de façon aussi simple et cohérente que pour les applications et portails Web de votre entreprise.

L'architecture de Tivoli Federated Identity Manager vous permet d'évaluer les règles métier pendant l'exécution, en-dehors d'une ressource ou d'une application, et vous pouvez ainsi modifier les paramètres qui influencent l'accès sans réécrire ou recompiler les applications. Ainsi, le logiciel vous aide à simplifier la gestion et à réagir rapidement aux changements dans vos besoins professionnels et dans vos relations avec les partenaires commerciaux et les utilisateurs tiers.

Fédérer les services Web sur des plateformes d'application hétérogènes

Si Tivoli Federated Identity Manager fournit une plateforme qui vient simplifier la signature des identités d'utilisateur, ce logiciel vous permet également d'utiliser la même plateforme pour garantir l'accès aux services Web que votre société fournit et utilise. Et tout comme les protocoles SSO fédérés (comme le SAML ou WS-Federation) ciblent les approches de clients passifs basées sur un navigateur,Tivoli Federated Identity Manager permet la fédération de services Web sans besoin de rapprocher avec rigueur les référentiels d'identités des partenaires et des clients. Avec le service Tivoli Federated Identity Manager Security Token Service, vous bénéficiez de la gestion d'identités et d'attributs nécessaire pour exposer une application existante à un client ou un partenaire sans avoir besoin de modifier la base de registre utilisateur interne de vos applications. Par exemple, vous pouvez étendre la fonctionnalité de sécurité sur les plateformes de services Web, comme IBM WebSphere® Application Server, Microsoft® .NET et SAP NetWeaver. Vous pouvez également :

- vous appuyer sur un point unique d'administration et de gestion des services Web internes et externes.
- simplifier le développement des services Web qui entretiennent des plateformes d'application hétérogènes.
- développer rapidement et efficacement des services Web en « déléguant » la couche sécurité des services Web à Tivoli Federated Identity Manager.

Depuis la console de Tivoli Federated Identity Manager, vous pouvez configurer les règles de fédération pour activer des fonctions comprenant l'inscription des partenaires, les données d'identification d'authentification et d'autorisation et le mappage des règles.

Gérer les flux d'identités à travers les services

La réutilisation des équipements existants à moindre coût et l'augmentation de la souplesse comptent parmi les principaux avantages d'un environnement SOA. Mais puisque les services sont liés ensemble dans les processus métier, des incohérences dans les identités d'utilisateur et leurs implémentations peuvent rapidement faire dévier une initiative SOA. Un traitement efficace de ces différentes identités d'utilisateur et de formats d'échange d'identité est indispensable à la réussite d'une architecture SOA.

Tivoli Federated Identity Manager fournit un service de jetons de sécurité (STS) pour aider à gérer les complexités du transfert d'identités d'utilisateur entre les services. Basé sur la norme WS-Trust, le STS peut être appelé directement depuis des applications ou autres intergiciels via le protocole défini par la norme WS-Trust. Avec le STS, les données d'identification

de sécurité d'un partenaire ou d'un domaine sont transformées et échangées en temps réel avec l'infrastructure d'identité d'un autre partenaire ou domaine. Cela vous permet de simplifier la gestion des identités et d'intégrer rapidement les sites Web et les plateformes d'application, sans besoin de remplacer une infrastructure existante.

A titre de couche de sécurité supplémentaire, les jetons de sécurité, comme les PassTickets, les certificats x.509 et les tickets Kerberos, sont eux-mêmes protégés par un chiffrement et des signatures numériques. Il est également possible d'accéder à la fonctionnalité STS depuis les coupe-feu / passerelles XML, notamment DataPower XS40 XML Security Gateway, l'une des passerelles de sécurité XML les plus utilisées dans l'industrie.

Améliorer votre capacité à prouver la conformité de votre entreprise

L'un des principaux obstacles pour réaliser un audit et garantir la conformité est le manque d'imputabilité pour accorder des droits utilisateur et des autorisations d'accès aux systèmes d'entreprise. Afin d'améliorer la conformité aux exigences réglementaires et aux standards de gouvernance d'entreprise, Tivoli Federated Identity Manager fournit un composant intégré de collecte et de rapport de données d'audit.

Etendre la valeur de vos investissements IBM System z

Tivoli Federated Identity Manager vous aide à améliorer vos résultats en étendant les applications existantes sans sacrifier la capacité à contrôler les droits d'accès, un élément essentiel aussi bien pour la sécurité que pour l'audit. Pour aider les sociétés à vérifier que les bonnes informations sont fournies à la bonne personne, Tivoli Federated Identity Manager vous permet de corréler une transaction IBM z/OS® à l'identité d'utilisateur qui a initié la transaction, ce qui peut faciliter la tâche de conformité aux réglementations correspondantes, comme la loi Sarbanes-Oxley, la loi Health Insurance Portability and Accountability Act (HIPAA) et le référentiel COBIT (Control Objectives for Information and related Technology), parallèlement à d'autres réglementations et meilleures pratiques industrielles.

Le service Tivoli Federated Identity Manager Security Token Service peut aussi être utilisé pour mapper les identifiants d'utilisateur répartis sur les identifiants d'utilisateur RACF du serveur z/OS Security Server et sur les PassTickets RACF associés (mots de passe uniques pour l'authentification au RACF). L'identifiant RACF et le PassTicket peuvent ensuite être utilisés pour se connecter aux ressources hébergées sur z/OS, en utilisant des identités d'utilisateur individuelles. Cela permet de garantir un audit plus complet et plus solide des utilisateurs et applications z/OS et de garantir que l'accès à un équipement informatique plus coûteux d'une entreprise, son System z, est toujours parfaitement contrôlé. La disponibilité da prise en charge des composants de Tivoli Federated Identity Manager sur z/OS permet une prise en charge complète des jetons pour les services Web dans des environnements impliquant WebSphere on z/OS.

S'appuyer sur les standards ouverts pour approvisionner des utilisateurs de façon cohérente et sécurisée

Tivoli Federated Identity Manager vous permet d'approvisionner en toute sécurité des droits et des comptes d'identité sur des domaines d'identité, à l'aide de WS-Provisioning.
Ce logiciel vous permet de :

- transmettre et recevoir des messages WS-Provisioning des systèmes de gestion d'identité des partenaires pour approvisionner les comptes d'utilisateur.
- vérifier la sécurité des messages WS-Provisioning que vous recevez.

A propos des logiciels IBM Tivoli

Les logiciels IBM Tivoli aident les entreprises à gérer efficacement les ressources, tâches et processus informatiques afin de répondre aux besoins fluctuants des entreprises et de fournir une gestion de service informatique souple et réactive, tout en réduisant les coûts. Le portefeuille Tivoli comprend des logiciels de sécurité, de conformité, de stockage, d'exécution, de disponibilité, de configuration, d'exploitation, de gestion du cycle de vie informatique, et est soutenu par les meilleurs services, équipes d'assistance technique et de recherche IBM.

Pour en savoir plus

Pour en savoir plus sur la manière dont Tivoli Federated Identity Manager vous aide à simplifier la gestion des comptes d'utilisateur et à optimiser la sécurité, contactez votre représentant ou partenaire commercial IMB ou visitez le site **ibm.com**/software/fr/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
Etats-Unis

Produit aux Etats-Unis

7-06

G507-1137-01