# Présentation

# Novell®
# Identity Manager

**4.0**

15 octobre 2010

www.novell.com

## Mentions légales

Novell, Inc. exclut toute garantie relative au contenu ou à l'utilisation de cette documentation. En particulier, Novell ne garantit pas que cette documentation est exhaustive ni exempte d'erreurs. Novell, Inc. se réserve en outre le droit de réviser cette publication à tout moment et sans préavis.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans notification préalable de ces modifications à quiconque.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous acceptez de vous conformer à toutes les réglementations de contrôle des exportations et à vous procurer les licences requises ou la classification permettant d'exporter, de réexporter ou d'importer des biens de consommation. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes d'exclusion d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou soumis à un embargo par la législation américaine en matière d'exportations. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou chimiques et biologiques. Reportez-vous aux Services de commerce international (http://www.novell.com/company/policies/trade_services) pour plus d'informations sur l'exploration des logiciels Novell. Novell décline toute responsabilité dans le cas où vous n'obtiendriez pas les autorisations d'exportation nécessaires.



Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

*Documentation en ligne :* pour accéder à la documentation en ligne la plus récente de ce produit et des autres produits Novell ou pour obtenir des mises à jour, reportez-vous au site Novell de documentation (http://www.novell.com/documentation).

## Marques de Novell

Pour connaître les marques commerciales de Novell, reportez-vous à la liste des marques commerciales et des marques de service de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

## Éléments tiers

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.

# Table des matières

# À propos de ce guide

Le présent guide vous présente Novell Identity Manager, un produit WorkloadIQ qui gère les identités et les accès dans les environnements physiques, virtuels et en nuage. Ce manuel explique les problèmes opérationnels qu'Identity Manager peut vous aider à résoudre tout en réduisant les coûts et en assurant la conformité. Il contient également un aperçu technique des composants et outils d'Identity Manager que vous pouvez utiliser pour créer votre solution Identity Manager. Ce guide est organisé de la manière suivante :



### Public

Ce guide est destiné aux administrateurs, aux consultants et aux ingénieurs réseau requérant une introduction de haut niveau aux solutions, aux technologies et aux outils professionnels d'Identity Manager.

### Mises à jour de la documentation

Vous trouverez la version la plus récente de ce document sur le site Web de la documentation relative à Identity Manager (http://www.novell.com/documentation/idm40/index.html).

### Documentation complémentaire

Pour de la documentation concernant les pilotes Identity Manager, reportez-vous au site Web des pilotes Identity Manager (http://www.novell.com/documentation/idm40drivers/index.html).

# 1 Identity Manager et l'automatisation des processus d'entreprise

Les informations de cette section décrivent certains des processus d'entreprise que vous pouvez automatiser grâce à l'implémentation d'un système Novell Identity Manager. Si vous connaissez déjà les solutions d'automatisation d'entreprise qu'offre Identity Manager, vous pouvez passer à l'introduction technique du Chapitre 3, « Architecture d'Identity Manager », page 21.

La gestion des besoins d'identité est une fonction essentielle de la plupart des entreprises. Imaginons par exemple, que nous soyons un lundi, tôt dans la matinée. Vous faites défiler la liste des requêtes de votre file d'attente :

- Le numéro du téléphone portable de Jim Taylor a changé. Vous devez le mettre à jour dans la base de données des ressources humaines, ainsi que dans quatre autres systèmes indépendants.
- Karen Hansen, qui revient juste d'une longue période d'absence, a oublié le mot de passe de sa messagerie. Vous devez l'aider à le retrouver ou à le réinitialiser.
- Jose Altimira vient d'embaucher un nouvel employé. Vous devez fournir à cet employé un accès au réseau ainsi qu'un compte de messagerie.
- Ida McNamee souhaite accéder à la base de données financière Oracle, ce qui suppose d'obtenir l'approbation de trois responsables différents.
- John Harris vient d'être transféré du service des comptes fournisseurs au service juridique. Vous devez lui donner accès aux mêmes ressources que les autres membres de l'équipe du service juridique et supprimer son accès aux ressources du service des comptes fournisseurs.
- Karl Jones, votre responsable, a vu une copie de la demande d'accès d'Ida McNamee à la base de données financière et s'inquiète du nombre de personnes pouvant y accéder. Vous devez lui adresser un rapport dressant la liste de toutes les personnes disposant d'un accès à cette base de données.

Vous respirez profondément et commencez par la première demande, en sachant que vous serez soumis à une forte pression pour suivre toutes ces requêtes et que vous aurez encore moins de temps pour terminer les autres projets dont vous êtes responsable.

Si cela ressemble fort à une journée de travail standard pour vous ou pour quelqu'un d'autre dans votre organisation, Identity Manager peut vous aider. En fait, les principales fonctionnalités d'Identity Manager, présentées sur la figure qui suit, peuvent vous aider à automatiser l'ensemble de ces tâches et bien d'autres encore. Ces fonctionnalités, à savoir workflows, rôles, attestation, self-service, audit et création de rapports, utilisent une synchronisation des données multi-système basée sur les stratégies de votre entreprise afin d'automatiser les processus impliqués dans le provisioning des utilisateurs et la gestion des mots de passe, deux des tâches les plus délicates et chronophages pour un service informatique.

***Figure 1-1*** *Principales fonctionnalités d'Identity Manager*


Les sections qui suivent présentent les fonctionnalités d'Identity Manager et montrent comment elles peuvent vous aider à satisfaire les besoins d'identité de votre organisation :

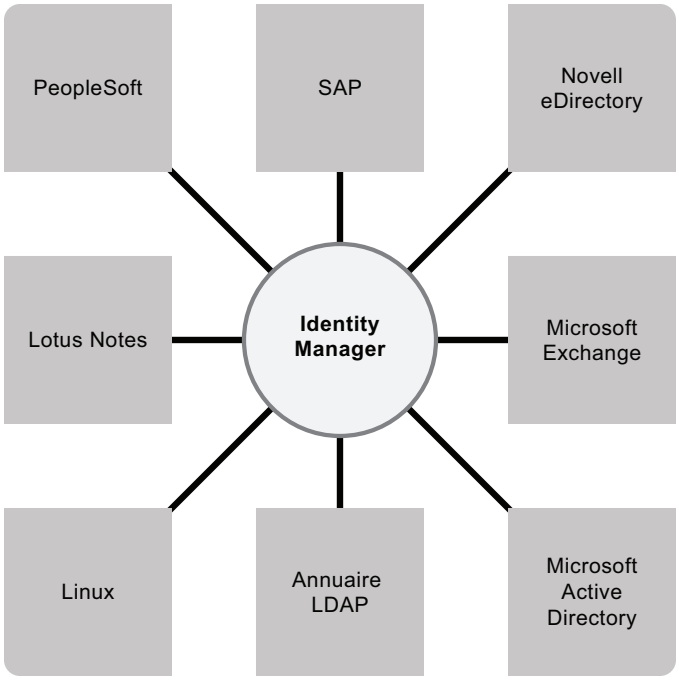


## 1.1 Synchronisation des données

Si votre organisation n'est pas différente des autres, vos données d'identité sont stockées sur plusieurs systèmes. Il est également possible que certaines de vos données d'identité soient stockées sur un système et que vous puissiez sans aucun doute les utiliser sur un autre. Dans les deux cas, vous devez être en mesure de partager et de synchroniser facilement ces données entre vos systèmes.

Identity Manager permet de synchroniser, de transformer et de distribuer des informations parmi une multitude d'applications, de bases de données, de systèmes d'exploitation et d'annuaires tels que SAP, PeopleSoft, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, Novell eDirectory, Linux, UNIX et les annuaires LDAP.

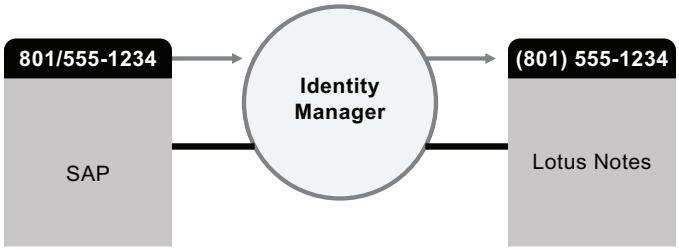
***Figure 1-2*** *Identity Manager pour connecter plusieurs systèmes*




Vous contrôlez le flux des données entre les différents systèmes connectés. Entre autres choses, vous pouvez déterminer quelles données seront partagées, quel système est la source experte de certaines données, et comment les données sont interprétées et transformées afin de satisfaire les exigences des autres systèmes.

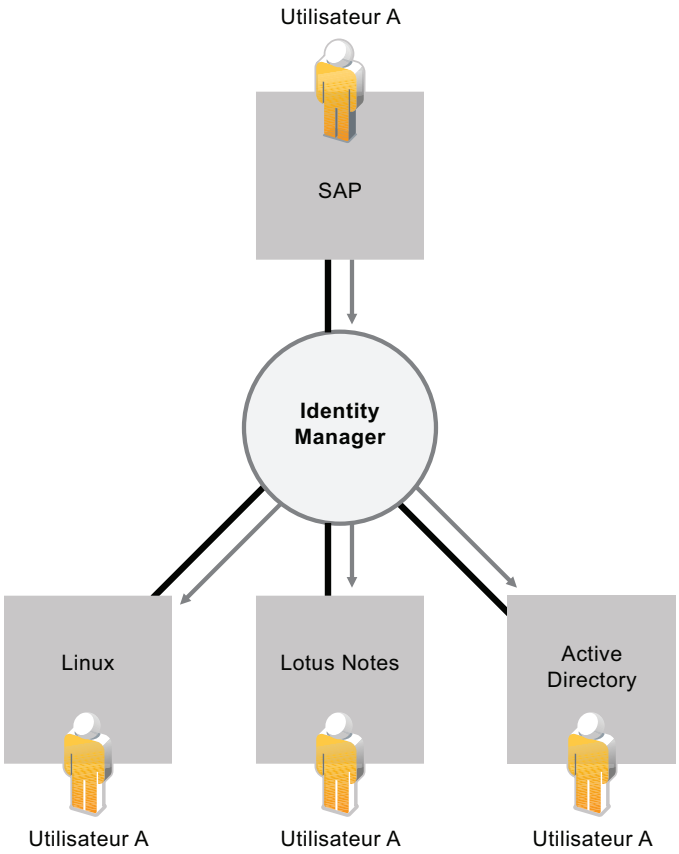
Dans le diagramme suivant, la base de données des ressources humaines SAP est la source experte du numéro de téléphone d'un utilisateur. Le système Lotus Notes utilise également des numéros de téléphone, c'est pourquoi Identity Manager convertit le numéro dans le format requis et le partage avec le système Lotus Notes. Chaque fois que le numéro de téléphone change dans le système de ressources humaines SAP, il est synchronisé sur le système Lotus Notes.

***Figure 1-3*** *Synchronisation des données entre les systèmes connectés*



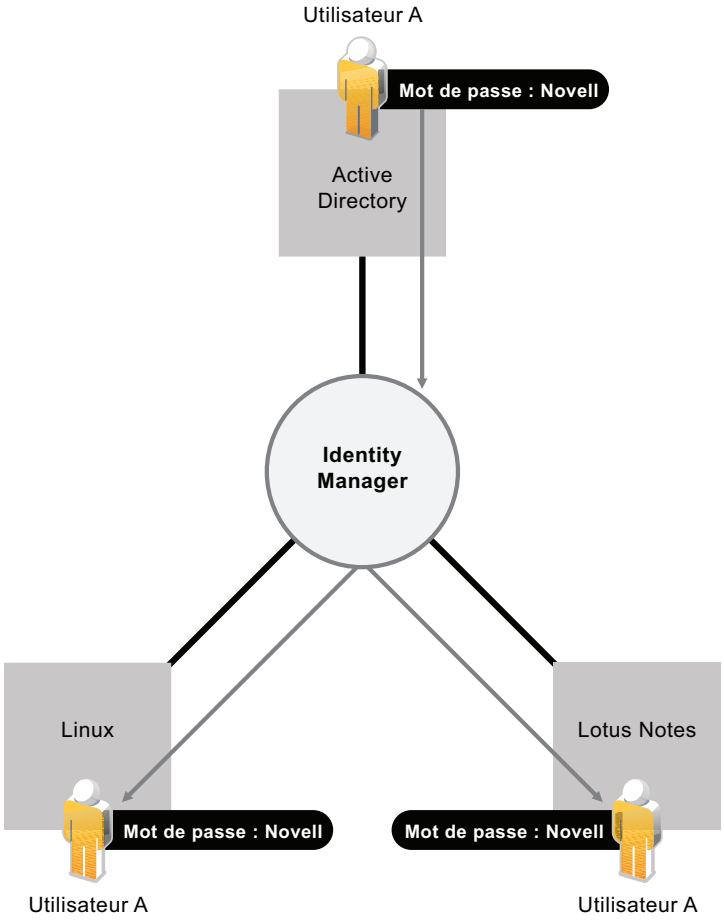

La gestion des données des utilisateurs existants n'est que le début des fonctionnalités de synchronisation des données d'Identity Manager. Identity Manager peut en outre créer de nouveaux comptes utilisateur et supprimer des comptes existants d'annuaires tels qu'Active Directory, de systèmes tels que PeopleSoft et Lotus Notes et de systèmes d'exploitation tels que UNIX et Linux. Par exemple, lorsque vous ajoutez un employé à votre système de ressources humaines SAP, Identity Manager peut créer automatiquement un compte utilisateur dans Active Directory, un compte dans Lotus Notes et un compte dans un système de gestion de comptes NIS Linux.

***Figure 1-4*** *Création de comptes utilisateur sur des systèmes connectés*




Dans le cadre de ses fonctions de synchronisation des données, Identity Manager peut également vous aider à synchroniser des mots de passe entre systèmes. Par exemple, si un utilisateur modifie son mot de passe dans Active Directory, Identity Manager peut le synchroniser dans Lotus Notes et Linux.

***Figure 1-5*** *Synchronisation de mot de passe entre systèmes connectés*

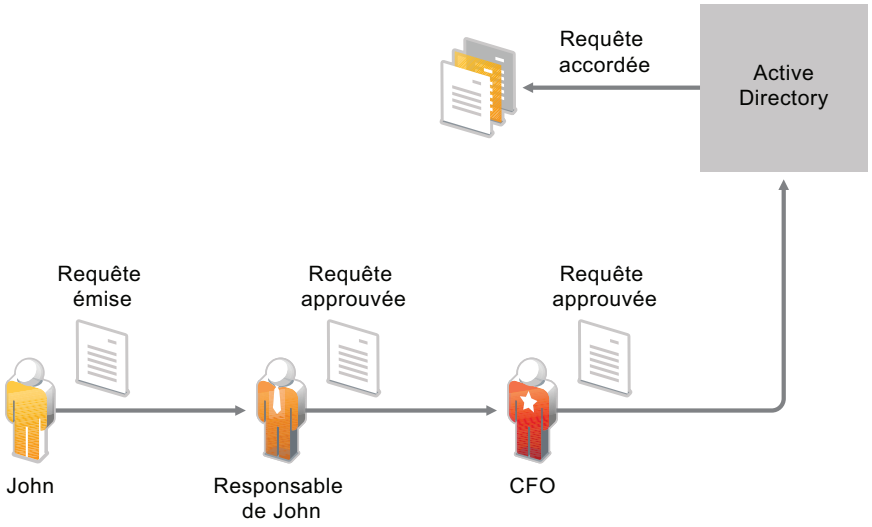



# 1.2 Workflow

Il est très probable que l'accès des utilisateurs à un grand nombre de ressources de votre organisation ne nécessite aucune approbation. En revanche, il se peut que l'accès à d'autres ressources soit restreint et nécessite l'approbation d'une ou plusieurs personnes.

Identity Manager offre des fonctionnalités de workflow qui permettent d'impliquer dans vos processus de provisioning les approbateurs de ressources appropriés. Supposons par exemple que John, qui dispose déjà d'un compte Active Directory, ait besoin d'accéder à certains rapports financiers via Active Directory. Cela nécessite l'approbation du responsable immédiat de John et du directeur financier. Heureusement, vous avez configuré un workflow d'approbation qui achemine la requête de John à son responsable et, après l'approbation de ce dernier, au directeur financier. L'approbation du directeur financier déclenche le provisioning automatique des droits d'Active Directory dont John a besoin pour accéder aux documents financiers et les consulter.

***Figure 1-6*** *Workflow d'approbation pour le provisioning de l'utilisateur*



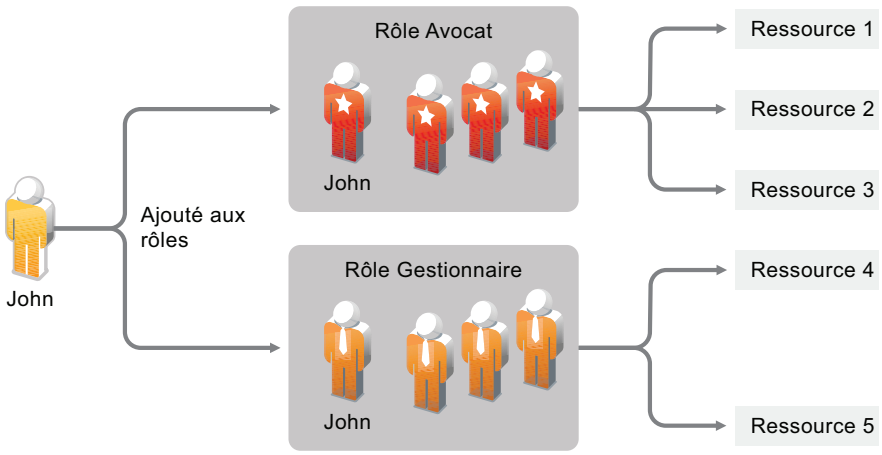

Les workflows peuvent être initiés automatiquement chaque fois qu'un événement déterminé se produit (par exemple, un nouvel utilisateur est ajouté à votre système des ressources humaines) ou manuellement suite à la demande d'un utilisateur. Pour vous assurer que les approbations interviennent au moment opportun, vous pouvez définir des mandataires comme approbateurs et des équipes d'approbation.

# 1.3 Rôles et attestation

Il est fréquent que les utilisateurs aient besoin d'accéder aux ressources en fonction de leurs rôles dans l'organisation. Par exemple, les avocats d'une société d'avocats peuvent avoir besoin d'accéder à un ensemble de ressources différent de celui utilisé par les adjoints juridiques de la société.

Identity Manager permet de fournir l'accès aux utilisateurs en fonction de leur rôle dans l'organisation. Vous définissez les rôles et effectuez les assignations en fonction des besoins de votre organisation. Lorsqu'un utilisateur est assigné à un rôle, Identity Manager lui donne accès aux ressources associées à ce rôle. Si un utilisateur a plusieurs rôles, il bénéficie de l'accès aux ressources associées à tous ces rôles, comme le montre la figure suivante :

***Figure 1-7*** *Provisioning des ressources en fonction des rôles*



Des utilisateurs peuvent se voir ajouter des rôles automatiquement à la suite d'événements intervenant au sein de votre organisation (par exemple, l'ajout d'un nouvel utilisateur possédant le titre d'avocat à votre base de données de ressources humaines SAP). Si une approbation est requise pour qu'un utilisateur soit ajouté à un rôle, vous pouvez définir des workflows pour acheminer les requêtes de ce rôle aux approbateurs appropriés. Vous pouvez également assigner manuellement des utilisateurs à des rôles.

Dans certains cas, il peut exister des rôles qui ne doivent pas être assignés à la même personne du fait d'un conflit entre ces rôles. Identity Manager offre une fonction de séparation des tâches qui permet d'éviter que des utilisateurs soient assignés à des rôles en conflit sauf si une personne de votre organisation définit une exception à ce conflit.

Les assignations de rôle déterminant l'accès d'un utilisateur aux ressources au sein de votre organisation, il est essentiel de les définir correctement. Des assignations incorrectes peuvent compromettre la conformité avec les réglementations de l'entreprise et les réglementations nationales. Identity Manager vous aide à valider la justesse de vos assignations de rôle par l'intermédiaire d'un processus d'attestation. Grâce à ce processus, les personnes responsables au sein de votre organisation certifient les données associées aux rôles :

- **Attestation du profil utilisateur :** les utilisateurs sélectionnés attestent de leurs propres informations de profil (prénom, nom, titre, service, adresse électronique, etc.) et corrigent les éventuelles informations erronées. Des informations de profil exactes sont essentielles pour disposer d'assignations de rôle correctes.
- **Attestation de violation de la séparation des tâches :** les personnes responsables examinent le rapport de violation de la séparation des tâches et attestent son exactitude. Ce rapport indique les exceptions qui permettent l'assignation d'un utilisateur à des rôles en conflit.
- **Attestation d'assignation de rôle :** les personnes responsables examinent le rapport qui répertorie les rôles sélectionnés, ainsi que les utilisateurs, les groupes et les rôles assignés à chaque rôle. Les personnes responsables doivent ensuite attester l'exactitude des informations.
- **Attestation de l'assignation des utilisateurs :** les personnes responsables examinent le rapport qui répertorie les utilisateurs sélectionnés, ainsi que les rôles auxquels ils sont assignés. Elles doivent ensuite attester l'exactitude des informations.

Ces rapports d'attestation sont principalement conçus pour vous aider à vérifier que les assignations de rôle sont exactes et qu'il existe des raisons valables pour autoriser des exceptions concernant les rôles en conflit.

## 1.4 Self-service

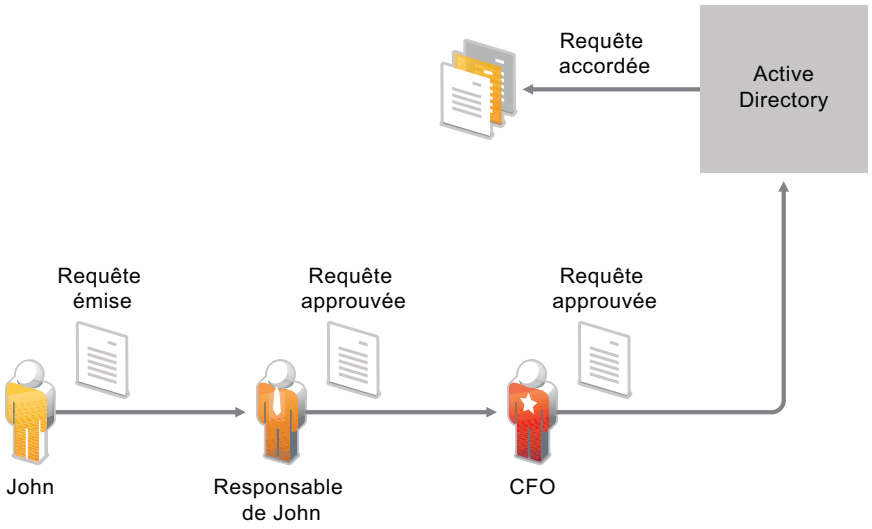
Votre entreprise compte probablement des responsables et des services qui revendiquent à grand cri la gestion des informations et des accès de leurs utilisateurs au lieu de vous les déléguer à vous et à votre équipe. Combien de fois avez-vous entendu « Pourquoi ne puis-je pas changer mon numéro de téléphone portable dans notre annuaire d'entreprise ? » ou « J'appartiens au service Marketing. Pourquoi suis-je tenu d'appeler le service d'assistance pour accéder à la base de données des informations Marketing ? ».

Avec Identity Manager, vous pouvez déléguer des tâches administratives aux personnes qui doivent en être responsables. Par exemple, vous pouvez permettre à des utilisateurs de :

- Gérer leurs données personnelles dans l'annuaire de l'entreprise. Vous n'aurez plus à modifier les numéros de téléphone portable : les employés s'en chargent à un emplacement, cette modification se répercutant ensuite sur tous les systèmes que vous avez synchronisés avec Identity Manager.
- Changer leurs mots de passe, configurer un indice ou des questions-réponses de vérification d'identité pour les mots de passe oubliés. Plutôt que de vous demander de réinitialiser le mot de passe qu'ils ont oublié, ils peuvent le faire eux-mêmes après avoir reçu un indice ou répondu à une question de vérification d'identité.
- Demander l'accès à des ressources telles que des bases de données, des systèmes ou des annuaires. Plutôt que de vous demander l'accès à une application, ils peuvent la sélectionner dans la liste des ressources disponibles.

Outre le self-service pour les utilisateurs, Identity Manager propose l'administration en self-service des fonctions (gestion, service d'assistance, etc.) régissant l'assistance, la surveillance et l'approbation des demandes des utilisateurs. Examinons l'exemple du scénario utilisé dans la Section 1.2, « Workflow », page 13 et illustré ci-dessous.

***Figure 1-8*** *Workflow de provisioning avec self-service*




Non seulement John utilise la fonction de self-service d'Identity Manager pour demander l'accès aux documents dont il a besoin, mais le responsable de John et le directeur financier utilisent la fonction de self-service pour approuver cette demande. Le workflow d'approbation établi permet à John de lancer sa demande et d'en suivre la progression. Il permet également au responsable de John et au directeur financier d'y répondre. L'approbation de la requête par le responsable de John et le directeur financier déclenche le provisioning des droits d'Active Directory dont John a besoin pour accéder aux documents financiers et les consulter.

## 1.5 Audit, création de rapports et conformité

Sans Identity Manager, le provisioning des utilisateurs peut s'avérer fastidieux, long et coûteux. Cet effort peut néanmoins paraître dérisoire comparé à la nécessité de vérifier que vos activités de provisioning respectent bien les stratégies, les exigences et les réglementations de votre entreprise.

Les personnes concernées ont-elles accès aux ressources dont elles ont besoin ? Les autres sont-elles bien privées de l'accès à ces mêmes ressources ? L'employé qui a commencé son activité hier a-t-il accès au réseau, à sa messagerie et aux six autres systèmes dont il a besoin pour son travail ? L'accès de l'employé qui a quitté l'entreprise la semaine dernière a-t-il été supprimé ?

Avec Identity Manager, vous pouvez être tranquille car vous savez que toutes vos activités de provisioning des utilisateurs, passées et actuelles, sont suivies et consignées à des fins d'audit. Identity Manager contient un espace de stockage intelligent pour les informations relatives aux états en cours et souhaités du coffre-fort d'identité ainsi que des systèmes gérés de votre entreprise. En interrogeant l'entrepôt, vous pouvez récupérer toutes les informations requises pour vous assurer que votre entreprise respecte parfaitement toutes les lois et réglementations applicables.

Cet entrepôt vous offre une vue globale de vos droits métiers, de sorte que vous disposez de toutes les données nécessaires pour voir l'état passé et présent des autorisations accordées aux identités au sein de votre organisation. Fort de cette connaissance, vous pouvez répondre aux requêtes GRC (Governance, Risk and Compliance) les plus complexes.

Identity Manager contient des rapports prédéfinis qui vous permettent d'interroger l'entrepôt d'informations d'identité afin de prouver la conformité des stratégies métiers, informatiques et d'entreprise. Vous pouvez, par ailleurs, créer des rapports personnalisés si ceux prédéfinis ne répondent pas à vos attentes.

# Fonctions d'Identity Manager 4.0

2

Novell Identity Manager 4.0 propose un environnement identitaire intelligent, qui tire profit de vos ressources informatiques existantes ainsi que de nouveaux modèles informatiques tels que SaaS (Software As a Service) en réduisant les coûts et en assurant la conformité parmi les environnements physiques, virtuels et en nuage. Grâce aux solutions Novell Identity Manager, vous pouvez être sûr que votre entreprise dispose des informations d'identité utilisateur les plus récentes. Vous pouvez garder un contrôle au niveau de l'entreprise en gérant, provisionnant et déprovisionnant les identités au sein du pare-feu, ainsi qu'en réalisant une extension au nuage. Identity Manager peut également vous aider à étendre votre gestion de la conformité au nuage.

Identity Manager 4.0 vous offre des fonctions intégrées de gestion des identités, des rôles et du contenu, ainsi que de création avancée de rapports. Vous pouvez en outre appliquer des stratégies de sécurité à plusieurs domaines système. Cela vous permet de gérer le cycle de vie utilisateur en dépit du nombre croissant d'exigences réglementaires et d'appliquer un niveau de protection plus granulaire avec un provisioning des utilisateurs davantage stratégique afin de tenir compte des préoccupations de plus en plus nombreuses en termes de sécurité au sein du pare-feu ou dans l'environnement en nuage. L'environnement identitaire intelligent vous aide à utiliser votre infrastructure existante avec de nouveaux modèles informatiques tels que SaaS.

### Novell Identity Manager 4.0 : une solution complète de bout en bout

- **Création de rapports détaillés prêts à l'emploi :** le module intégré de création de rapports de la suite Novell Identity Manager 4.0 offre une meilleure visibilité de la conformité au sein des déploiements internes et en nuage. Les nouvelles fonctions de création de rapports permettent de consulter l'état d'identité et les droits d'accès d'un utilisateur, ainsi que de rendre compte des opérations et de l'historique de provisioning de ce dernier.
- **Meilleure intégration :** la suite Novell Identity Manager 4.0 s'intègre aisément aux applications que vous exécutez déjà. De nouveaux pilotes SharePoint et Salesforce.com facilitent l'intégration des identités de votre entreprise au sein des applications en nuage.
- **Tableau de bord amélioré :** la suite Novell Identity Manager 4.0 vous permet de voir et de gérer facilement les identités depuis des tableaux de bord améliorés qui font appel à une interface unique pour afficher des informations détaillées concernant les utilisateurs de votre entreprise.
- **Pilotes compatibles cloud :** Identity Manager 4.0 propose plusieurs pilotes pour une intégration prête à l'emploi avec SaaS. Il permet une intégration transparente avec SaaS et la solution hébergée en fournissant des fonctions telles que le provisioning, le déprovisioning, les processus de requête/d'approbation, les modifications de mot de passe, les mises à jour des profils d'identité et la création de rapports.
- **Coffre-fort d'identité intégré :** la nouvelle architecture des produits Novell Identity Manager 4.0 inclut un coffre-fort d'identité intégré de sorte qu'il n'est pas nécessaire de créer et de gérer une structure d'annuaire distincte à des fins d'identité. Par ailleurs, les produits Novell Identity Manager 4 comportent des pilotes qui permettent d'intégrer facilement ce coffre-fort à d'autres espaces de stockage d'informations d'identité de votre entreprise, tels qu'Active Directory ou diverses bases de données.

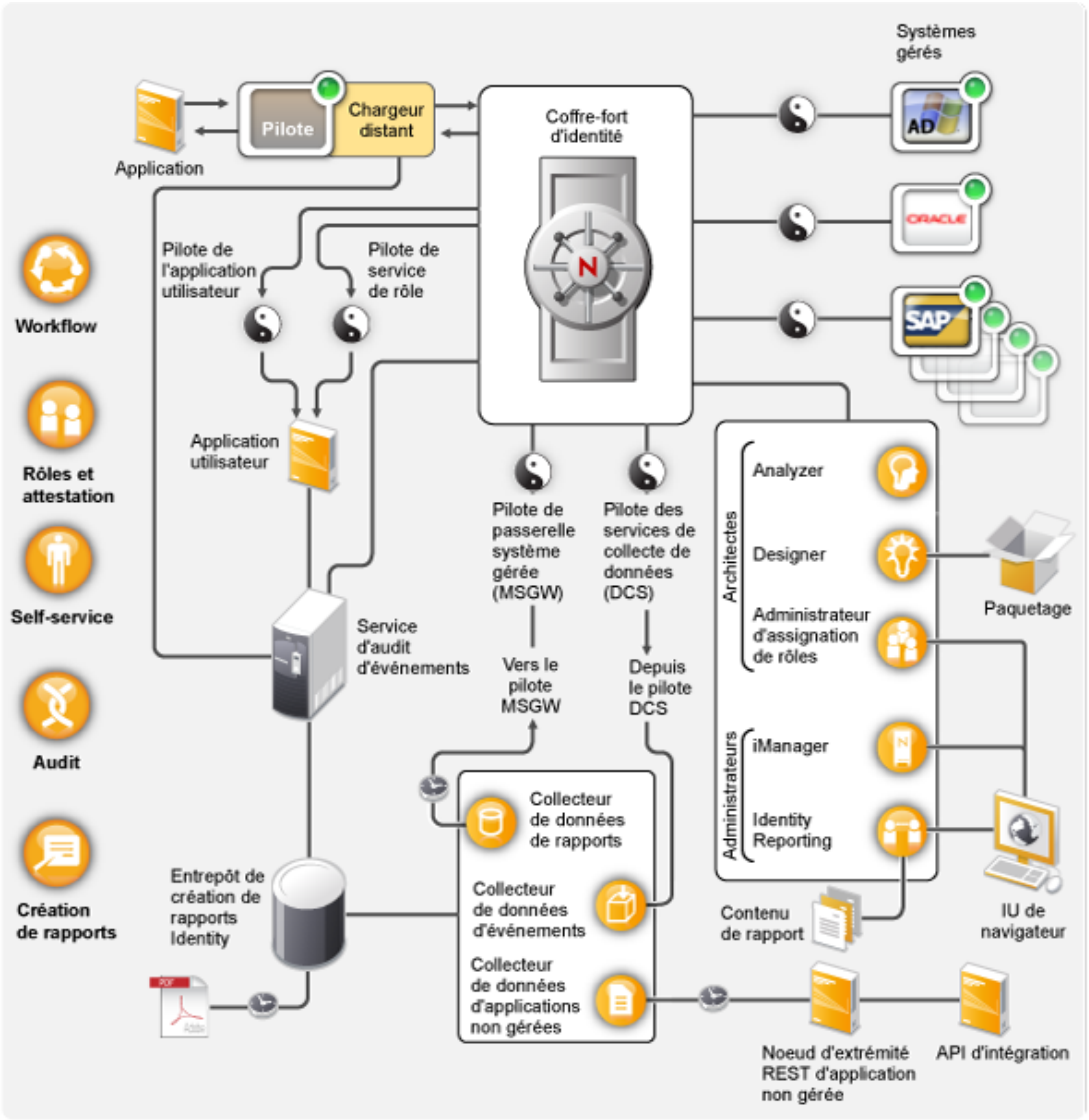
- **Gestion simplifiée des rôles et des identités :** la suite Novell Identity Manager 4.0 simplifie l'intégration de plusieurs espaces de stockage de rôles en un emplacement unique consolidé, de sorte que vous ne devez plus gérer différentes sources d'informations d'identité. Grâce à l'administrateur d'assignation de rôles et sa nouvelle interface intuitive, vous pouvez même assigner à Novell Identity Manager 4.0 des rôles et des profils tiers.
- **Gestion des paquetages :** Identity Manager 4.0 introduit un nouveau concept baptisé Gestion des paquetages. Il s'agit d'un système de création, de distribution et de consommation de blocs de construction de qualité supérieure du contenu de stratégie d'Identity Manager.

# Architecture d'Identity Manager

# 3

Le diagramme suivant illustre les composants d'architecture de haut niveau qui fournissent les fonctionnalités de Novell Identity Manager présentées dans le Chapitre 1, « Identity Manager et l'automatisation des processus d'entreprise », page 9 : synchronisation des données, workflow, rôles, attestation, self-service, audit et création de rapports.

***Figure 3-1*** *Architecture d'Identity Manager*




Chaque composant est présenté dans les sections suivantes :

- Section 3.1, « Synchronisation des données », page 22
- Section 3.2, « Workflow, rôles, attestation et self-service », page 26
- Section 3.3, « Audit et création de rapports », page 29

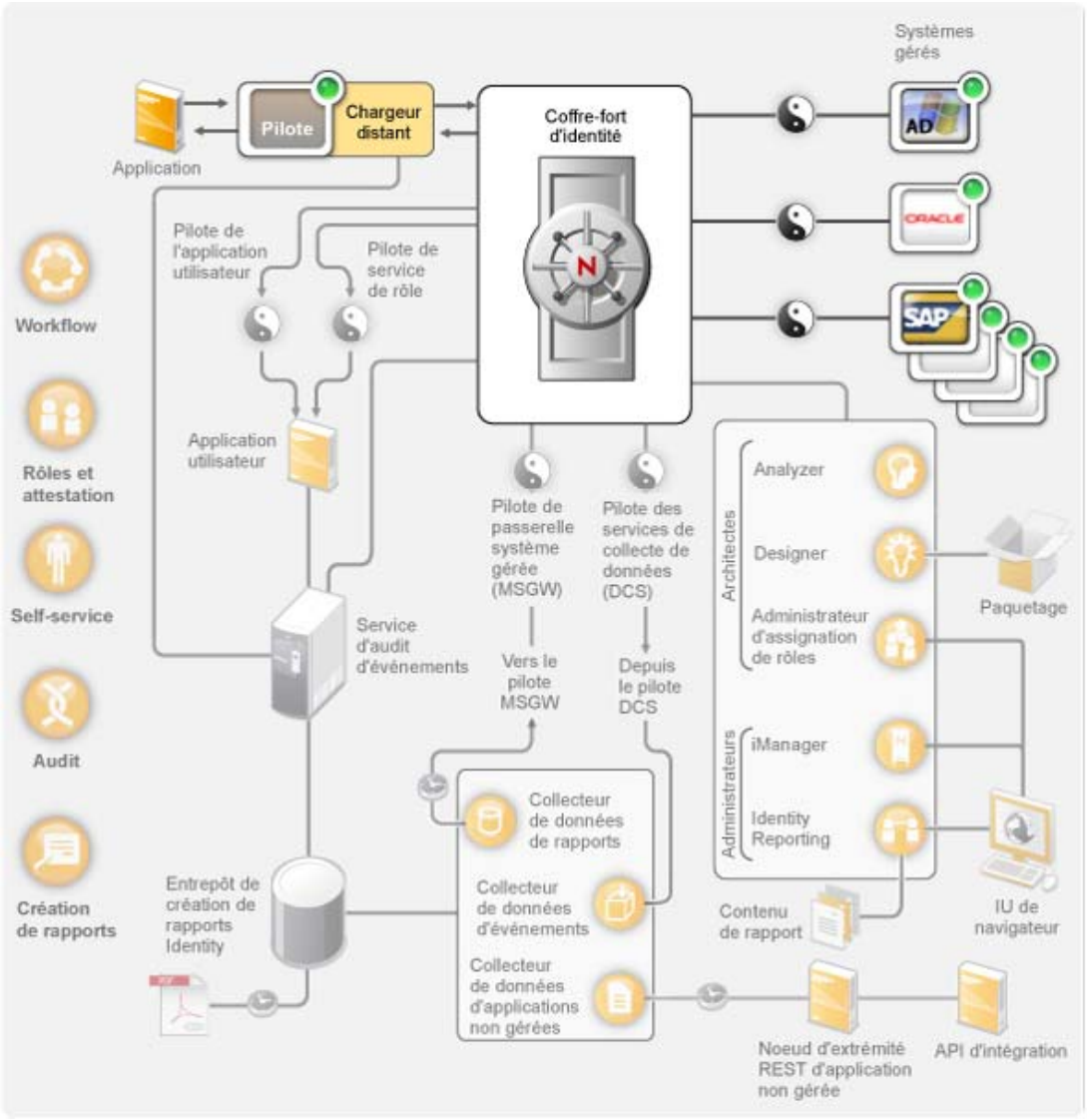
## 3.1 Synchronisation des données

La synchronisation des données constitue le fondement de l'automatisation des processus de l'entreprise. Sous sa forme la plus simple, la synchronisation correspond au mouvement des données dont un élément a été modifié de l'emplacement de la modification vers les autres emplacements où cet élément est requis. Par exemple, si le numéro de téléphone d'un employé est modifié dans le système des ressources humaines d'une entreprise, cette modification doit apparaître automatiquement dans tous les autres systèmes qui stockent le numéro de téléphone de cet employé.

Identity Manager ne se limite pas à la synchronisation des données d'identité. Identity Manager peut synchroniser n'importe quel type de donnée stockée dans l'application connectée ou dans le coffre-fort d'identité.

La synchronisation des données, notamment celle des mots de passe, est effectuée par les cinq composants de base de la solution Identity Manager : le coffre-fort d'identité, le moteur méta-annuaire, les pilotes, le chargeur distant et les applications connectées. Ces composants sont présentés dans le diagramme ci-dessous.

***Figure 3-2*** *Composants de l'architecture Identity Manager*




Les sections suivantes décrivent chacun de ces composants et expliquent les concepts que vous devez comprendre pour obtenir une synchronisation efficace entre les systèmes de votre organisation :

- Section 3.1.1, « Composants », page 23
- Section 3.1.2, « Principaux concepts », page 24

## 3.1.1 Composants

**Coffre-fort d'identité :** il sert de méta-annuaire pour les données à synchroniser entre les applications. Par exemple, les données synchronisées d'un système PeopleSoft vers Lotus Notes sont d'abord ajoutées au coffre-fort d'identité, puis envoyées au système Lotus Notes. Par ailleurs, le coffre-fort d'identité stocke les informations spécifiques à Identity Manager, telles que la configuration, les paramètres et les stratégies des pilotes. Novell eDirectory est utilisé pour le coffre-fort d'identité.

**Moteur méta-annuaire :** il traite les modifications apportées aux données du coffre-fort d'identité ou des applications connectées. Quant aux événements qui se produisent dans le coffre-fort d'identité, le moteur traite leurs modifications et émet des commandes vers l'application via le pilote. Si des événements se produisent dans l'application, le moteur reçoit les modifications du pilote, les traite et émet des commandes vers le coffre-fort d'identité. Le moteur méta-annuaire est également nommé *moteur d'Identity Manager*.

**Pilote :** les pilotes se connectent aux applications dont vous voulez gérer les informations d'identité. Un pilote remplit deux fonctions principales : signaler au moteur méta-annuaire les modifications apportées aux données (événements) dans l'application et exécuter les modifications de données (commandes) soumises par le moteur méta-annuaire à l'application.

**Chargeur distant :** les pilotes doivent être installés et exécutés sur le même serveur que l'application à laquelle ils se connectent. Si l'application se trouve sur le même serveur que le moteur méta-annuaire, il suffit d'y installer le pilote. Toutefois, si ce n'est pas le cas (en d'autres termes, si l'application est distante du serveur du moteur au lieu d'être locale), vous devez installer le pilote et le chargeur distant sur le serveur de l'application. Le chargeur distant charge le pilote et communique avec le moteur méta-annuaire pour le compte du pilote.

**Application :** système, annuaire, base de données ou système d'exploitation auquel un pilote se connecte. L'application doit fournir des API permettant au pilote de déterminer les modifications apportées à ses données et les rendre effectives. Les applications sont souvent appelées *systèmes connectés*.

## 3.1.2 Principaux concepts

**Canaux :** les données circulent entre le coffre-fort d'identité et un système connecté le long de deux *canaux* distincts. Le *canal Abonné* assure la circulation des données du coffre-fort d'identité vers un système connecté ; en d'autres termes, le système connecté s'abonne aux données du coffre-fort d'identité. Le *canal Éditeur* assure la circulation des données d'un système connecté vers le coffre-fort d'identité ; en d'autres termes, le système connecté publie les données dans le coffre-fort d'identité.

**Représentation des données :** les données circulent dans les canaux sous la forme de *documents XML*. Un document XML est créé lorsqu'une modification est apportée dans le coffre-fort d'identité ou dans le système connecté. Il est transmis au moteur méta-annuaire qui le traite par l'intermédiaire de l'ensemble de filtres et de stratégies associé au canal du pilote. Lorsque tous les traitements ont été appliqués au document XML, ce dernier est utilisé par le moteur méta-annuaire pour lancer les modifications appropriées dans le coffre-fort d'identité (canal Éditeur) ou par le pilote pour lancer les modifications appropriées dans le système connecté (canal Abonné).

**Manipulation des données :** lorsque les documents XML circulent dans les canaux du pilote, leurs données sont soumises aux *stratégies* associées aux canaux.

Ces stratégies permettent beaucoup de choses, notamment le changement des formats de données, l'assignation d'attributs entre le coffre-fort d'identité et le système connecté, le blocage conditionnel du flux des données, la génération des notifications par message électronique et la modification du type de modification des données.

**Contrôle du flux de données :** les *filtres*, ou *stratégies de filtre*, contrôlent le flux des données. Ils précisent les éléments de données synchronisés entre le coffre-fort d'identité et le système connecté. Par exemple, les données de l'utilisateur sont généralement synchronisées entre les systèmes. Par conséquent, les données de l'utilisateur sont répertoriées dans le filtre pour la plupart des systèmes

connectés. Toutefois, les imprimantes ne présentent généralement pas d'intérêt pour la plupart des applications, c'est pourquoi les données correspondantes n'apparaissent pas dans le filtre de la plupart des systèmes connectés.

Chaque relation entre le coffre-fort d'identité et un système connecté possède deux filtres : un filtre sur le canal Abonné qui contrôle le flux des données du coffre-fort d'identité vers le système connecté, et un filtre sur le canal Éditeur qui contrôle le flux des données du système connecté vers le coffre-fort d'identité.

**Sources expertes :** la plupart des éléments de données associés à l'identité ont un propriétaire conceptuel. Le propriétaire d'un élément de données est considéré comme la *source experte* de l'élément. En général, seule la source experte d'un élément de données est autorisée à le modifier.

Le système de messagerie de l'entreprise, par exemple, est généralement considéré comme source experte de l'adresse électronique d'un employé. Si un administrateur de l'annuaire des pages blanches de l'entreprise change l'adresse électronique d'un employé dans ce système, ce changement n'a pas d'effet sur le fait que l'employé reçoive ou non un message électronique à l'adresse modifiée car cette modification doit être faite dans le système de messagerie pour être effective.

Identity Manager utilise des filtres pour indiquer les sources expertes des éléments. Par exemple, si le filtre de la relation entre le système PBX et le coffre-fort d'identité permet au numéro de téléphone d'un employé de circuler du système PBX jusqu'au coffre-fort d'identité mais pas du coffre-fort d'identité au système PBX, ce dernier est la source experte du numéro de téléphone. Si toutes les autres relations du système connecté permettent au numéro de téléphone de circuler du coffre-fort d'identité aux systèmes connectés, mais pas l'inverse, le résultat est que le système PBX est la seule source experte des numéros de téléphones des employés de l'entreprise.

**Provisioning automatique :** il représente la capacité d'Identity Manager à générer des opérations de provisioning de l'utilisateur autres que la simple synchronisation des éléments de données.

Par exemple, pour un système Identity Manager classique dans lequel la base de données des ressources humaines est la source experte de la plupart des données des employés, l'ajout d'un employé à cette base de données déclenche la création automatique du compte correspondant dans le coffre-fort d'identité. La création du compte du coffre-fort d'identité déclenche à son tour la création automatique du compte de messagerie de l'employé dans le système de messagerie. Les données utilisées pour provisionner le compte du système de messagerie sont obtenues à partir du coffre-fort d'identité et peuvent inclure le nom, l'adresse, le numéro de téléphone de l'employé, etc.

Le provisioning automatique des comptes, de l'accès et des données peut être contrôlé de plusieurs manières :

- **Valeurs des éléments de données :** la création automatique d'un compte dans la base de données d'accès de différents bâtiments peut être contrôlée, par exemple, par une valeur définie dans l'attribut d'emplacement d'un employé.
- **Workflows d'approbation :** la création d'un employé dans le service financier peut, par exemple, déclencher un message électronique automatique adressé au directeur de ce service pour demander l'approbation du compte du nouvel employé dans le système financier. Le message électronique contient un lien vers une page Web dans laquelle le directeur du service financier peut approuver ou rejeter cette demande. L'approbation peut ensuite déclencher la création automatique du compte de l'employé dans le système financier.

- **Assignations de rôles :** prenons l'exemple d'un employé se voyant attribuer le rôle de comptable. Identity Manager provisionne l'employé avec tous les comptes, accès et données assignés au rôle de comptable, par l'intermédiaire des workflows du système (sans intervention humaine), via par des flux d'approbation humains, ou par une combinaison des deux.

**Droits :** il s'agit des ressources dans les systèmes connectés, par exemple un compte ou l'appartenance à un groupe. Lorsqu'un utilisateur satisfait les critères établis pour un droit dans un système connecté, Identity Manager traite un événement relatif à l'utilisateur qui se voit ainsi accorder l'accès à la ressource. Bien entendu, cela nécessite que toutes les stratégies soient en place pour permettre l'accès à la ressource. Par exemple, si un utilisateur satisfait les critères d'un compte Exchange dans Active Directory, le moteur méta-annuaire traite l'utilisateur par l'intermédiaire de l'ensemble des stratégies de pilote d'Active Directory qui fournissent un compte Exchange.

Le principal avantage des droits tient à ce que vous pouvez définir la logique métier nécessaire à l'accès à une ressource dans un droit plutôt que dans plusieurs stratégies de pilote. Vous pouvez, par exemple, définir un droit de compte donnant à un utilisateur un compte dans quatre systèmes connectés. La décision de fournir ou non un compte à un utilisateur est déterminée par le droit, ce qui signifie qu'il n'est pas nécessaire que les stratégies pour chacun des quatre pilotes incluent la logique métier. Il suffit, au lieu de cela, que les stratégies fournissent le mécanisme pour accorder le compte. Si vous devez effectuer un changement de logique métier, vous le faites dans le droit plutôt que dans chaque pilote.

**Travaux :** pour une grande part, Identity Manager agit en réponse au modifications des données ou aux demandes des utilisateurs. Par exemple, lorsqu'un élément de donnée change dans un système, Identity Manager change l'élément correspondant dans les autres systèmes. Ou encore, lorsqu'un utilisateur demande l'accès à un système, Identity Manager lance les processus appropriés (workflows, provisioning de ressource, etc.) pour fournir l'accès.

Les travaux permettent à Identity Manager d'effectuer les opérations qui ne sont pas initiées par des modifications de données ou des demandes d'utilisateur. Un travail est constitué des données de configuration stockées dans le coffre-fort d'identité et d'une portion correspondante du code d'implémentation. Identity Manager comporte des travaux prédéfinis qui effectuent des opérations telles que le démarrage ou l'arrêt de pilotes, l'envoi de notifications par message électronique en cas d'expiration de mots de passe et la vérification de l'état de santé des pilotes. Vous pouvez également implémenter des travaux personnalisés pour effectuer d'autres opérations ; un travail personnalisé exige que vous (ou bien un développeur ou un consultant) créiez le code requis pour effectuer l'opération désirée.

**Bons de travail :** les modifications apportées aux données du coffre-fort d'identité ou d'une application connectée sont généralement traitées immédiatement. Les bons de travail permettent de planifier les tâches devant être effectuées à une date et une heure donnée. Par exemple, un nouvel employé a été embauché mais le début de son activité n'est pas prévu avant un mois. Il faut ajouter cet employé à la base de données des ressources humaines mais ne pas lui donner accès aux ressources de l'entreprise (messagerie, serveurs, etc.) avant la date de sa prise de fonction. Sans bon de travail, l'accès par l'utilisateur serait immédiat. Si vous avez implémenté les bons de travail, un bon de travail est créé pour ne démarrer le provisioning du compte qu'à la date prévue.

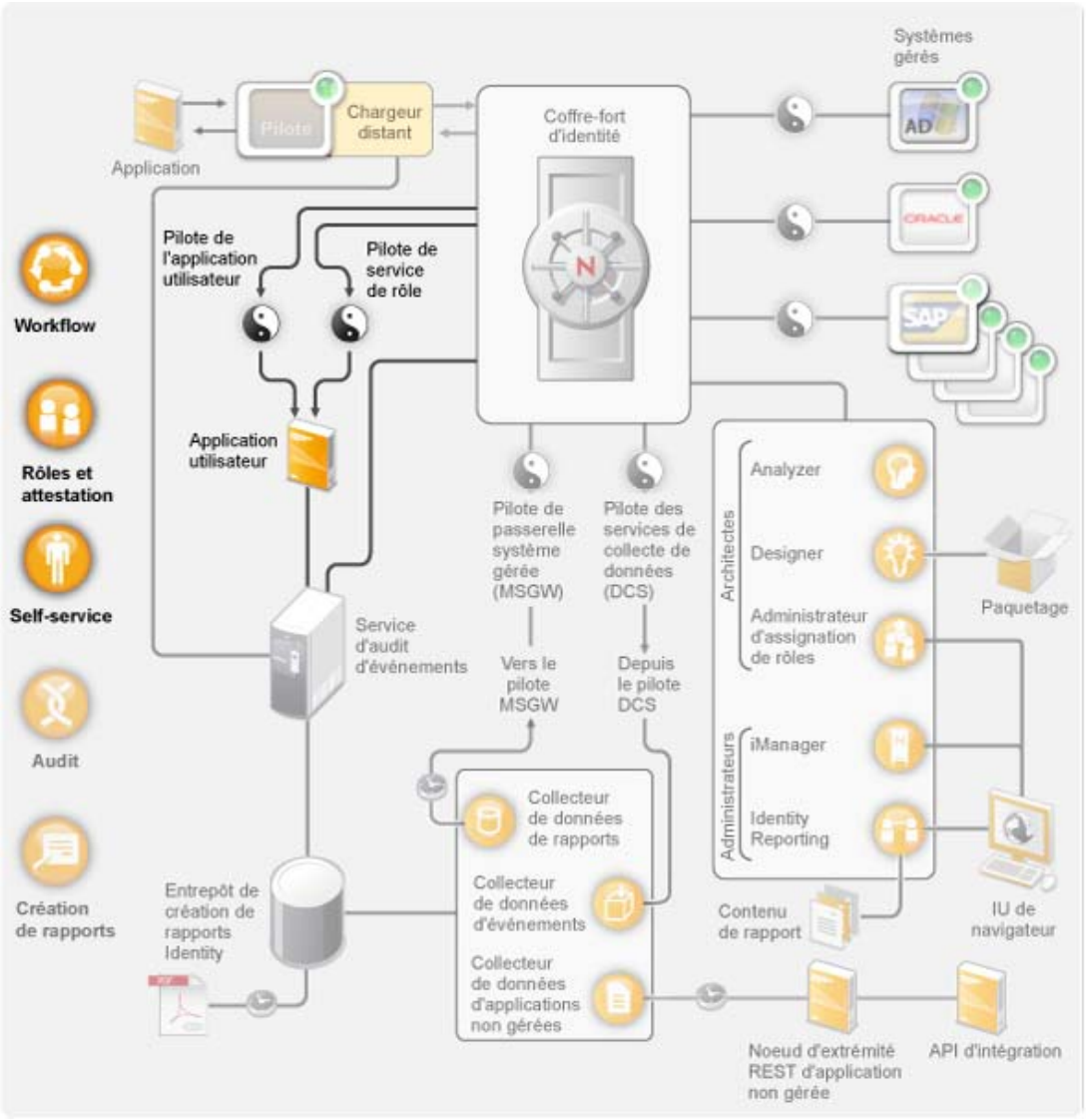
## 3.2 Workflow, rôles, attestation et self-service

Identity Manager met à disposition une application spécialisée, l'application utilisateur, qui permet les workflows d'approbation, l'assignation des rôles, l'attestation et le self-service d'identité.

L'application utilisateur standard est incluse avec Identity Manager. Elle offre le self-service du mot de passe pour aider les utilisateurs à mémoriser ou à réinitialiser les mots de passe oubliés, des organigrammes pour gérer les informations dans les annuaires d'utilisateurs, des fonctionnalités de gestion des utilisateurs permettant la création d'utilisateurs dans le coffre-fort d'identité, ainsi qu'un self-service d'identité de base incluant la gestion des informations des profils utilisateur.

Le module de provisioning basé sur le rôle de l'application utilisateur est un module complémentaire d'Identity Manager vendu séparément. Il étend la fonctionnalité d'application utilisateur standard en y incluant des fonctions avancées de self-service, de workflow d'approbation, provisioning basé sur le rôle, de contraintes de séparation des tâches et d'attestation.

***Figure 3-3*** *Identity Manager User Application (Application utilisateur Identity Manager)*




Les sections suivantes offrent des descriptions de chacun de ces composants et expliquent les concepts que vous devez comprendre pour les implémenter et les gérer efficacement :

- Section 3.2.1, « Composants », page 28
- Section 3.2.2, « Principaux concepts », page 28

### 3.2.1 Composants

**Application utilisateur :** il s'agit d'une application basée sur navigateur offrant aux utilisateurs et aux administrateurs la possibilité d'effectuer un grand nombre de tâches de self-service d'identité et de provisioning de rôle, notamment la gestion des mots de passe et des données d'identité, le démarrage et le suivi des requêtes de provisioning et d'assignation de rôle, la gestion du processus d'approbation des requêtes de provisioning, ainsi que la vérification des rapports d'attestation. Elle inclut le moteur de workflow qui permet l'acheminement des requêtes tout au long du processus d'approbation approprié.

**Pilote d'application utilisateur :** il stocke les informations de configuration et notifie l'application utilisateur chaque fois qu'un changement se produit dans le coffre-fort d'identité. Il peut également être configuré pour permettre à des événements du coffre-fort d'identité de déclencher des workflows et de signaler le succès ou l'échec d'une activité de provisioning d'un workflow à l'application utilisateur afin que les utilisateurs puissent consulter l'état final de leurs demandes.

**Pilote de service de rôle :** il gère les assignations de rôle, démarre les workflows pour les requêtes d'assignation de rôle nécessitant une approbation et gère les assignations de rôle indirectes en fonction de leur appartenance à un groupe ou à un conteneur. Le pilote a également deux autres fonctions : accorder et retirer les droits utilisateur en fonction de l'appartenance à un rôle, mais aussi réaliser des procédures de nettoyage pour les requêtes qui ont été menées à bien.

### 3.2.2 Principaux concepts

**Provisioning basé sur le workflow :** il permet aux utilisateurs de demander l'accès aux ressources. Les requêtes de provisioning sont acheminées par l'intermédiaire d'un workflow prédéfini qui peut inclure l'approbation d'une ou plusieurs personnes. Si toutes les approbations sont accordées, l'utilisateur reçoit l'accès à la ressource. Les requêtes de provisioning peuvent également être initiées de façon indirecte, en réponse à des événements qui se produisent dans le coffre-fort d'identité. L'ajout d'un utilisateur à un groupe, par exemple, peut initier une requête visant à donner à l'utilisateur l'accès à une ressource particulière.

**Provisioning basé sur les rôles :** il permet aux utilisateurs de recevoir l'accès à des ressources spécifiques en fonction des rôles qui leur sont assignés. Les utilisateurs peuvent se voir assigner un ou plusieurs rôles. Si une assignation de rôle requiert une approbation, la demande d'assignation démarre un workflow.

**Séparation des tâches :** pour empêcher les utilisateurs d'être assignés à des rôles en conflit, le module de provisioning basé sur le rôle de l'application utilisateur propose une fonction de séparation des tâches. Vous pouvez établir des contraintes de séparation des tâches qui définissent les rôles considérés comme étant en conflit. Lorsque des rôles sont en conflit, les approbateurs de séparation des tâches peuvent approuver ou refuser les exceptions aux contraintes. Les exceptions approuvées sont enregistrées sous la forme de violations de la séparation des tâches et peuvent être consultées par l'intermédiaire du processus d'attestation décrit ci-dessous.

**Gestion des rôles :** elle doit être effectuée par les personnes assignées aux rôles système Administrateur du module de rôles et Gestionnaire de rôles.

L'administrateur du module de rôles crée ou supprime les rôles et modifie les rôles existants, modifie les relations entre les rôles, accorde ou annule les assignations de rôles pour les utilisateurs et crée, modifie et supprime les contraintes de séparation des tâches.

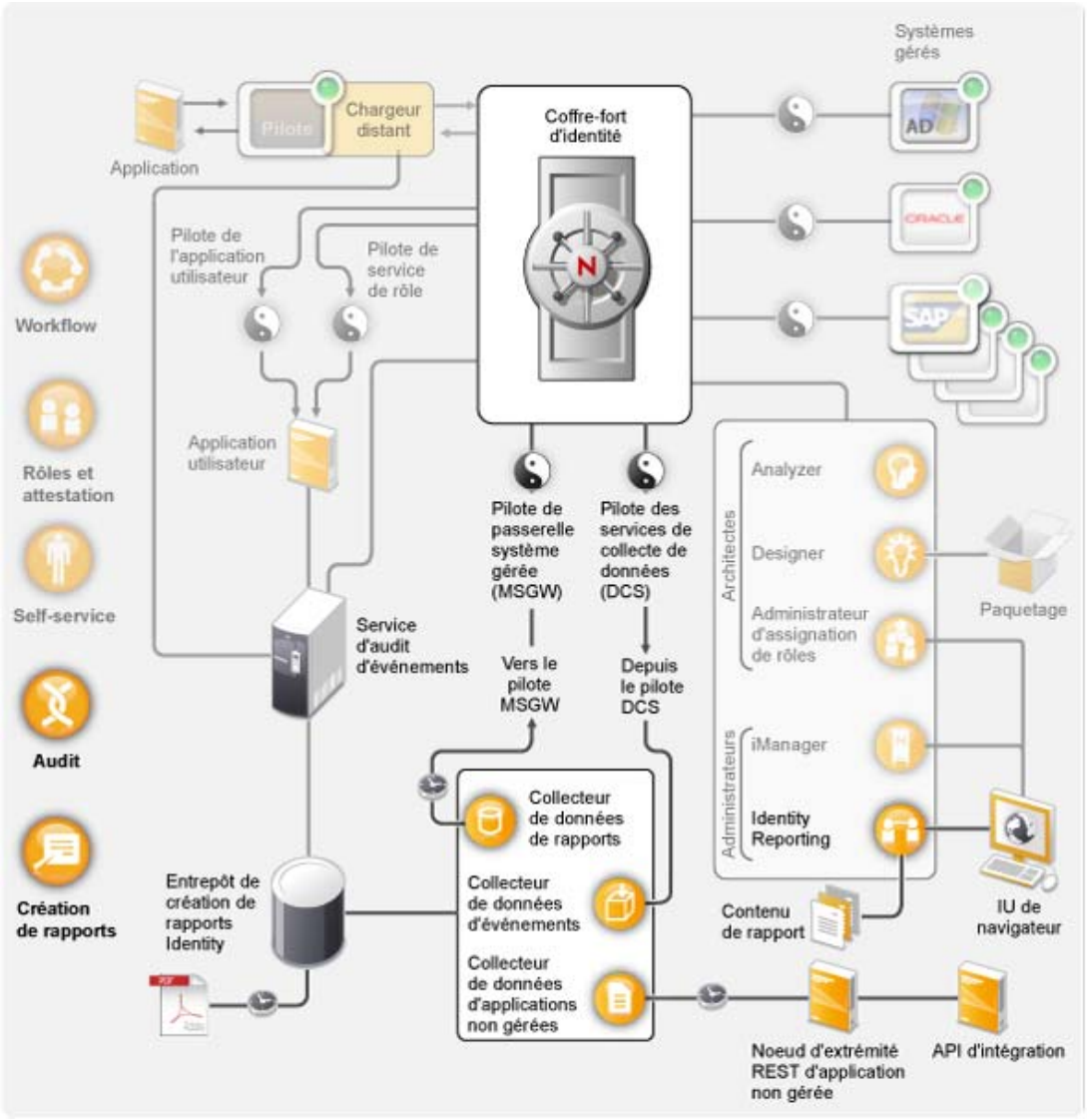
Le gestionnaire de rôles dispose des même fonctions que l'administrateur du module de rôles à l'exception de la gestion des contraintes de séparation des tâches, de la configuration du système de rôles et de la possibilité d'exécuter tous les rapports. De plus, si l'administrateur du module de rôles dispose d'une étendue illimitée au sein du système de rôles, l'étendue du gestionnaire de rôles est limitée à des utilisateurs, des groupes et des rôles bien spécifiques.

**Attestation :** les assignations de rôle déterminent l'accès des utilisateurs aux ressources au sein de votre organisation. Les assignations incorrectes risquent de compromettre les réglementations de l'entreprise et les réglementations nationales. Identity Manager vous aide à valider la justesse de vos assignations de rôle par l'intermédiaire d'un processus d'attestation. Grâce à ce processus, les utilisateurs peuvent valider leurs propres informations de profil et les gestionnaires de rôles valider les assignations de rôle et les violations de séparation des tâches.

## 3.3 Audit et création de rapports

Les fonctions d'audit et de création de rapports sont assurées par le module Identity Reporting, une nouvelle composante d'Identity Manager 4.0, comme l'indique le diagramme suivant.

***Figure 3-4*** *Audit et création de rapports Identity Manager*




Le module Identity Reporting génère des rapports qui fournissent des informations essentielles sur divers aspects de votre configuration Identity Manager, notamment les données collectées auprès de coffres-forts d'identité et de systèmes gérés tels qu'Active Directory ou SAP. Pour gérer les données, le module Identity Reporting utilise les composants suivants :

**Service d'audit d'événements :** service qui capture les événements de journal associés aux opérations réalisées dans le module de créations de rapports, telles que l'importation, la modification, la suppression ou la planification d'un rapport. Le service d'audit d'événements EAS capture les événements de journal associés aux opérations effectuées au sein du module de provisioning basé sur les rôles (RBPM) et de l'administrateur d'assignation de rôles (RMA).

**Entrepôt de création de rapports Identity :** espace de stockage pour les informations des types suivants.

- Informations de gestion de rapports (telles que les rapports terminés ainsi que les définitions et les planifications de rapports), vues de base de données utilisées pour la création de rapports et informations de configuration.
- Données d'identité recueillies par le collecteur de données de rapports, le collecteur de données d'événements et le collecteur de données d'applications non gérées.
- Données d'audit, qui incluent les événements collectés par le service d'audit d'événements.

L'entrepôt de création de rapports Identity stocke ses données dans la base de données SIEM (Security Information and Event Management).

**Service de collecte de données :** service qui recueille des informations de plusieurs sources au sein d'une organisation. Le service de collecte de données comporte trois sous-services :

- **Collecteur de données de rapports :** utilise un modèle d'extraction pour récupérer des informations d'une ou de plusieurs sources de données de coffre-fort d'identité. La collecte s'exécute de manière périodique, selon un ensemble de paramètres de configuration. Pour récupérer les données, le collecteur fait appel au pilote de passerelle système gérée.
- **Collecteur de données d'événements :** utilise un modèle de distribution pour rassembler les données d'événements capturées par le pilote du service de collecte de données.
- **Collecteur de données d'applications non gérées :** récupère les données d'une ou de plusieurs applications non gérées en appelant un noeud d'extrémité REST écrit spécifiquement pour chaque application. Les applications non gérées sont des applications de votre entreprise qui ne sont pas connectées au coffre-fort d'identité. Pour plus d'informations, reportez-vous à la section « REST Services for Reporting » (Services REST pour la création de rapports) du manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting).

**Pilote du service de collecte de données :** pilote qui capture les modifications apportées aux objets stockés dans un coffre-fort d'identité, tels que les comptes, rôles, ressources, groupes et adhésions à des équipes. Le pilote du service de collecte de données s'enregistre lui-même auprès du service de collecte de données et distribue à ce dernier les événements de modification (tels que la synchronisation de données et l'ajout, la modification ou la suppression d'événements).

Les informations capturées enregistrent les modifications apportées aux objets suivants :

- Identités et comptes utilisateur
- Rôles et niveaux de rôles
- Groupes

  **Remarque :** le module de création de rapports ne prend pas en charge les groupes dynamiques et génère uniquement des rapports sur des données de groupes statiques.

- Adhésions à des groupes
- Définitions de requêtes de provisioning
- Définitions et violations de séparations de tâches
- Associations de droits d'utilisateur
- Définitions et paramètres de ressources

- Assignations de rôles et de ressources
- Droits de coffre-fort d'identité, types de droits et pilotes

**Pilote de passerelle système gérée :** pilote qui collecte des informations des systèmes gérés. Pour récupérer les données des systèmes gérés, le pilote interroge le coffre-fort d'identité. Les données récupérées incluent les éléments suivants :

- Liste de tous les systèmes gérés
- Liste de tous les comptes des systèmes gérés
- Types de droits, valeurs et assignations, ainsi que profils de compte utilisateur pour les systèmes gérés

**Création de rapports Identity :** l'interface utilisateur du module de création de rapports permet de planifier facilement l'exécution des rapports aux heures creuses de manière à optimiser les performances. Pour plus d'informations sur le module Identity Reporting, reportez-vous au manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting).

**Rapports :** Identity Manager contient des rapports prédéfinis qui permettent d'afficher les informations de l'entrepôt d'informations d'identité de manière pratique. Vous pouvez toutefois aussi créer des rapports personnalisés. Pour plus d'informations sur les rapports, reportez-vous au manuel *Using Identity Manager 4.0 Reports* (Utilisation des rapports Identity Manager 4.0). Pour des informations concernant les rapports personnalisés, reportez-vous à la section « Creating Custom Report Definitions » (Création de définitions de rapports personnalisés) du manuel *Identity Reporting Module Guide* (Guide du module Identity Reporting).

**Noeud d'extrémité REST d'application non gérée :** une application non gérée est une application qui n'est pas connectée à un coffre-fort d'identité, mais qui contient des données que vous souhaitez reprendre dans des rapports. Si vous définissez un noeud d'extrémité REST pour une application, vous permettez au module de création de rapports de collecter des données auprès de cette dernière.

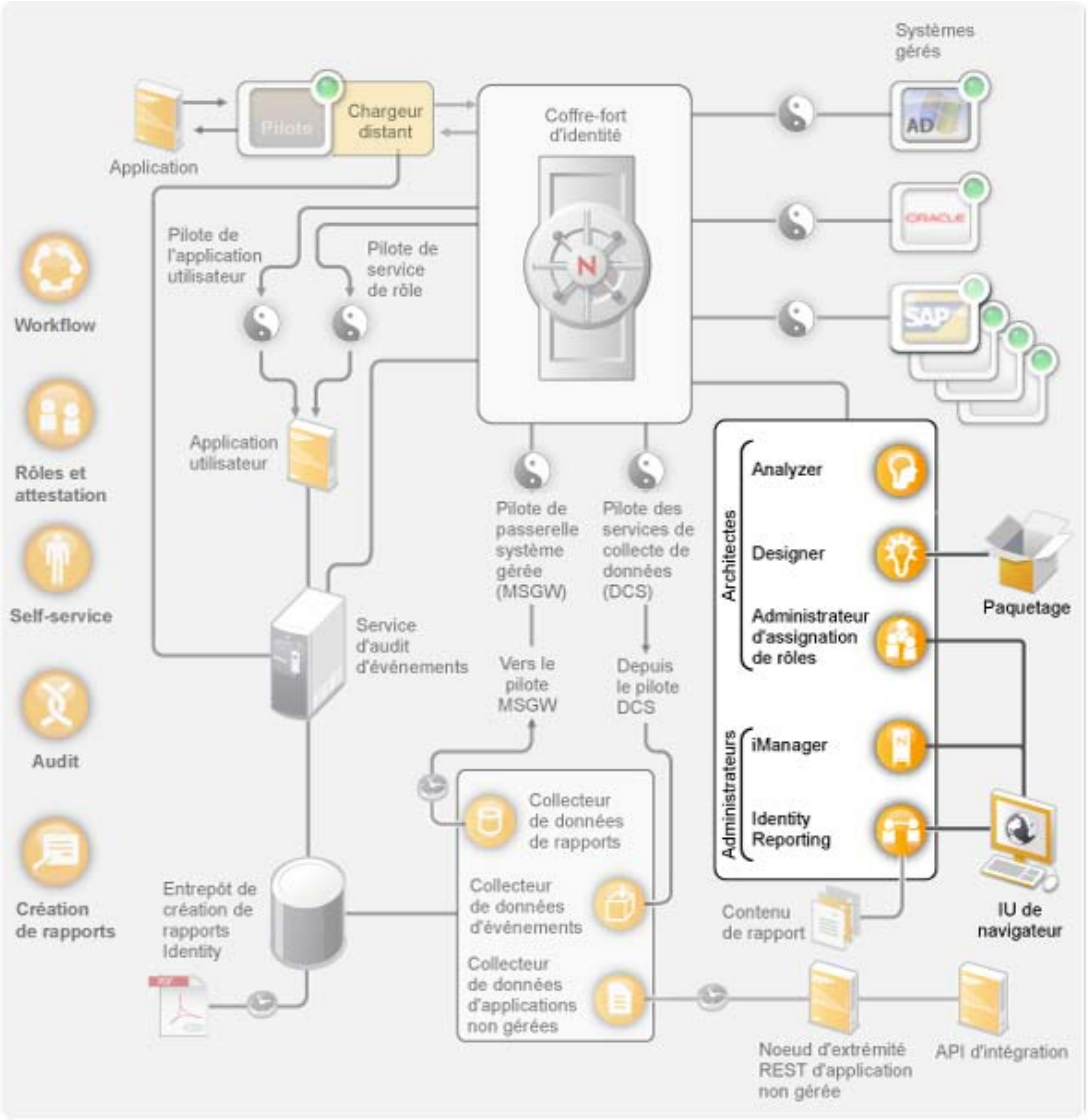
**API d'intégration :** la version initiale du module Identity Reporting prend en charge une API REST unique. Celle-ci permet d'implémenter un noeud d'extrémité REST pour une application non gérée.

# Outils d'Identity Manager

# 4

Identity Manager fournit des outils qui vous aident à créer et tenir à jour votre solution Identity Manager. Chacun remplit une fonction spécifique.

***Figure 4-1*** *Outils d'Identity Manager*




Designer permet de concevoir, de créer et de configurer votre système Identity Manager dans un environnement hors ligne, puis de déployer vos modifications dans votre système en ligne. Analyzer permet, lors de la création de votre solution Identity Manager, d'analyser, de nettoyer et de préparer vos données à des fins de synchronisation.

L'administrateur d'assignation de rôles permet de créer et de gérer les rôles dans l'ensemble de votre solution Identity Manager.

iManager permet d'effectuer les mêmes tâches que Designer, ainsi que de contrôler l'état de santé de votre système, mais il ne prend pas en charge la gestion des paquetages. Il est conseillé d'utiliser iManager pour les tâches d'administration et Designer pour les tâches de configuration qui nécessitent la modification de paquetages, une modélisation et des tests avant déploiement.

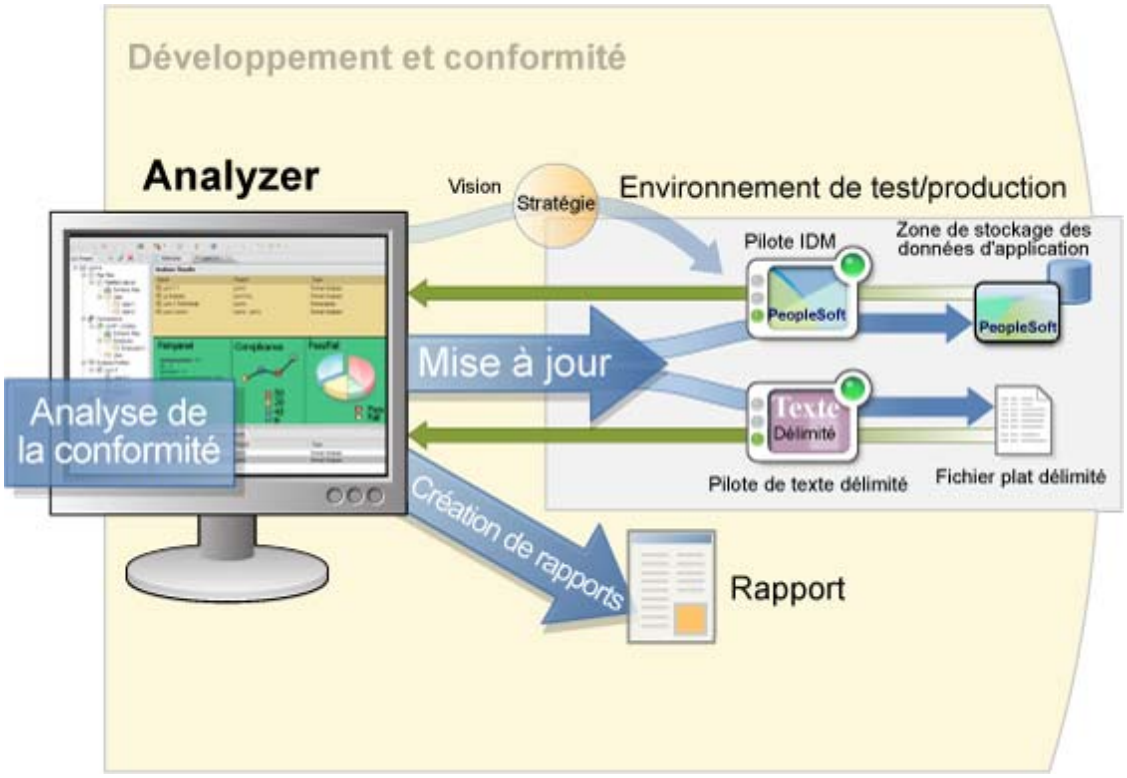
Vous trouverez plus d'informations sur chacun de ces outils dans les sections suivantes :



## 4.1 Analyzer

Analyzer est un ensemble d'outils de gestion des identités basé sur Eclipse qui contribue à garantir le respect des stratégies de qualité des données internes, et ce par le biais de l'analyse, du nettoyage, du rapprochement et de la surveillance des données, ainsi que par la création de rapports. Analyzer permet d'analyser, d'optimiser et de contrôler toutes les zones de stockage de données de l'entreprise.

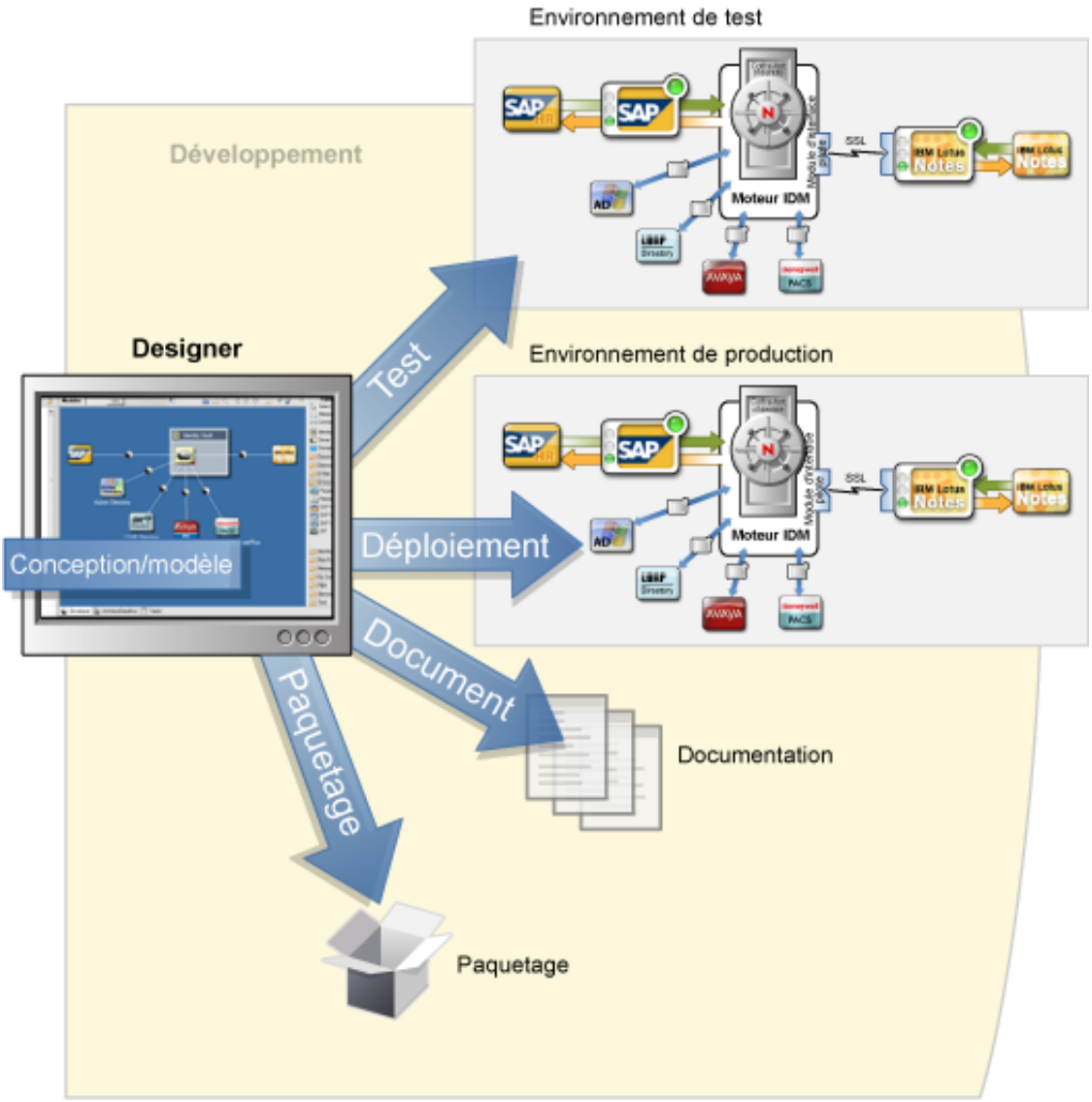
***Figure 4-2*** *Analyzer pour Identity Manager*



# 4.2 Designer

Designer est un outil basé sur Eclipse qui vous aide à concevoir, déployer et documenter votre système Identity Manager. L' interface graphique de Designer permet de concevoir et de tester votre système dans un environnement hors ligne, de déployer ce système dans votre environnement de production, et de documenter tous les détails de votre système déployé.

***Figure 4-3*** *Designer pour Identity Manager*




**Conception :** Designer dispose d'une interface graphique qui permet de modeler votre système. Cela inclut des vues qui permettent de créer et de contrôler les connexions entre Identity Manager et les applications, de configurer les stratégies et de manipuler la manière dont les données circulent entre les applications connectées.

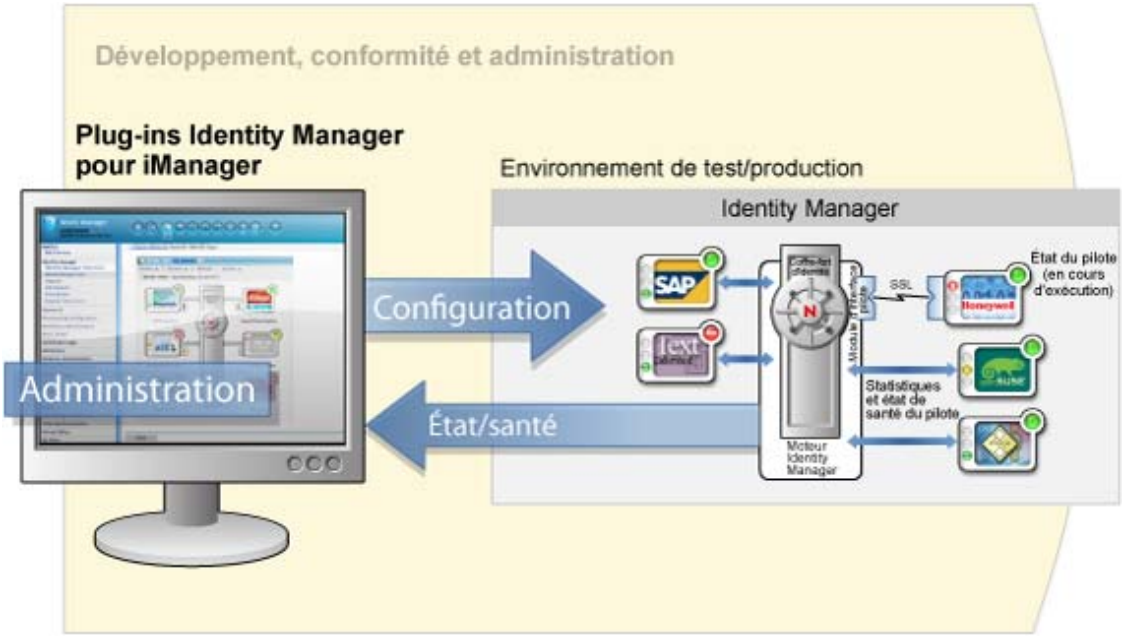
**Déploiement :** le travail que vous effectuez dans Designer n'est déployé sur votre environnement de production que si vous initiez le déploiement. Cela donne la liberté d'expérimenter, de tester les résultats et de résoudre les problèmes avant de mettre en ligne votre environnement de production.

**Documentation :** vous pouvez générer une documentation complète illustrant la hiérarchie de vos systèmes, la configuration des pilotes, la configuration des stratégies, etc. Vous disposez de toutes les informations nécessaires pour comprendre les aspects techniques de votre système et pouvez en vérifier la conformité avec les règles et les stratégies de votre entreprise.

## 4.3 iManager

Novell iManager est un outil basé sur un navigateur qui offre un point d'administration unique pour un grand nombre de produits Novell, notamment Identity Manager. En utilisant les plug-ins d'Identity Manager pour iManager, vous pouvez gérer Identity Manager et recevoir des informations en temps réel sur la santé et l'état de votre système Identity Manager.

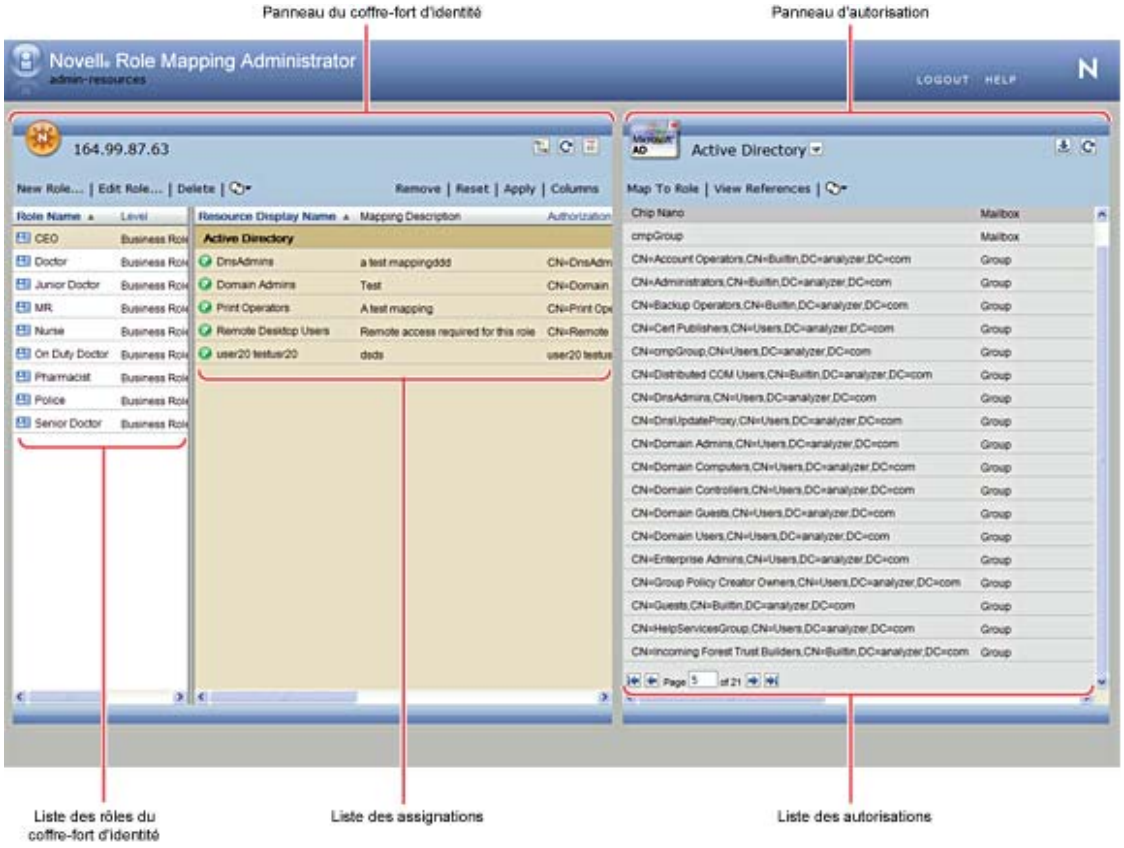
***Figure 4-4*** *Novell iManager*




## 4.4 Administrateur d'assignation de rôles

L'administrateur d'assignation de rôles est un service Web qui découvre les autorisations pouvant être octroyées au sein de vos principaux systèmes informatiques. Il permet aux administrateurs informatiques mais aussi aux analystes d'entreprise de définir et gérer les autorisations associées aux différents rôles.

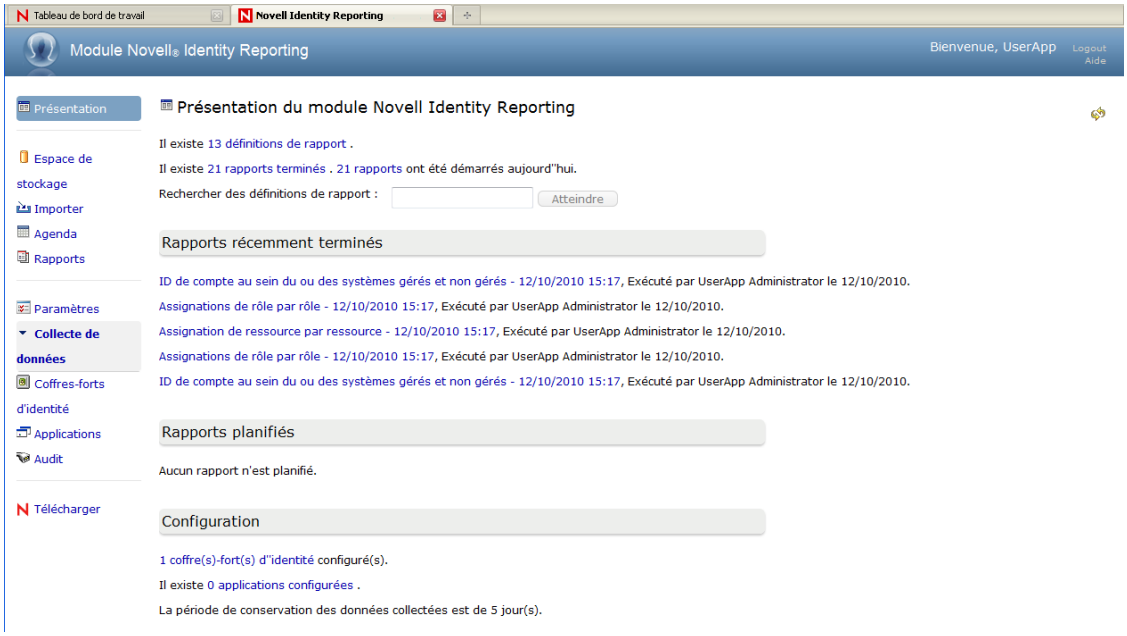
***Figure 4-5*** *Administrateur d'assignation de rôles*




# 4.5 Identity Reporting

Le module Identity Reporting génère des rapports qui fournissent des informations essentielles sur divers aspects de votre configuration Identity Manager, notamment les données collectées auprès de coffres-forts d'identité et de systèmes gérés tels qu'Active Directory ou SAP. Le module de création de rapports comprend un ensemble de définitions de rapport prédéfinies que vous pouvez utiliser pour générer des rapports. En outre, il permet d'importer des rapports personnalisés définis dans un outil tiers. L'interface utilisateur du module de création de rapports permet de planifier facilement l'exécution des rapports aux heures creuses de manière à optimiser les performances.

***Figure 4-6*** *Module Identity Reporting*




Le module de création de rapports fournit plusieurs points d'intégration ouverts. Par exemple, si vous souhaitez collecter des données concernant des applications tierces non connectées à Identity Manager, vous pouvez implémenter un noeud d'extrémité REST personnalisé afin de recueillir des informations de ces applications. En outre, vous pouvez personnaliser les données distribuées au coffre-fort d'identité. Une fois ces données disponibles, vous pouvez écrire des rapports personnalisés pour les consulter.

# Étapes suivantes

5

Une fois que vous avez compris les différents composants qui constituent Identity Manager 4.0, vous pouvez utiliser la documentation afin de créer votre solution Identity Manager. Les sections suivantes expliquent où trouver la documentation requise pour les tâches mentionnées :



## 5.1 Élaboration d'une solution Identity Manager

La première étape pour concevoir une solution Identity Manager est de décider avec précision ce que vous souhaitez que cette solution fasse au sein de votre entreprise. Reportez-vous à la section « Planning » (Planification) du manuel *Identity Manager 4.0 Framework Installation Guide* (Guide d'installation du moteur Identity Manager 4.0) pour créer un plan de votre solution Identity Manager à l'aide de Designer. Vous pouvez également concevoir votre application utilisateur à l'aide du manuel *User Application: Design Guide* (Guide de conception de l'application utilisateur).

Designer permet de capturer des informations dans un projet et de les partager avec d'autres personnes. Vous pouvez également modéliser la solution dans Designer avant de commencer les modifications. Pour plus d'informations sur Designer, reportez-vous au manuel *Understanding Designer for Identity Manager* (Présentation de Designer pour Identity Manager).

## 5.2 Préparation de vos données à des fins de synchronisation

Une fois le plan créé, vous devez préparer les données de votre environnement en vue de la synchronisation. Analyzer est l'outil qui permet d'analyser, de nettoyer et de préparer les données à cette fin. Pour plus d'informations, reportez-vous au manuel *Analyzer 1.2 for Identity Manager Administration Guide* (Guide d'administration de la version 1.2 d'Analyzer pour Identity Manager).

## 5.3 Installation ou mise à niveau d'Identity Manager

Une fois le plan créé et les données préparées, vous pouvez installer Identity Manager. Si votre environnement informatique est de taille réduite ou moyenne et que vous n'avez jamais utilisé Identity Manager, il est préférable de recourir au programme d'installation intégré. Celui-ci installe et configure tous les composants fournis avec Identity Manager. Pour plus d'informations, reportez-vous au manuel *Identity Manager 4.0 Integrated Installation Guide* (Guide du programme d'installation intégré d'Identity Manager 4.0).

Si vous avez un système Identity Manager existant ou si votre environnement informatique est vaste, utilisez le manuel *Identity Manager 4.0 Framework Installation Guide* (Guide d'installation du moteur Identity Manager 4.0) pour installer ou mettre à niveau les différents composants d'Identity Manager. Chacun d'eux étant installé et configuré séparément, vous pouvez personnaliser votre solution Identity Manager.

- Pour des instructions concernant l'installation, reportez-vous à la section « Installation » du manuel *Identity Manager 4.0 Framework Installation Guide* (Guide d'installation du moteur Identity Manager 4.0).
- Pour des instructions concernant la mise à niveau, reportez-vous à la section « Performing an In-place Upgrade » (Exécution d'une mise à niveau directe) du manuel *Identity Manager 4.0 Framework Installation Guide* (Guide d'installation du moteur Identity Manager 4.0).
- Si vous migrez un système existant vers un nouveau matériel, reportez-vous à la section « Performing a Migration » (Exécution d'une migration) du manuel *Identity Manager 4.0 Framework Installation Guide* (Guide d'installation du moteur Identity Manager 4.0).
- Si vous devez migrer le module de provisioning basé sur les rôles, reportez-vous au manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide* (Guide de migration de l'application utilisateur du module de provisioning basé sur les rôles d'Identity Manager 4.0).

## 5.4 Configuration d'Identity Manager

Une fois Identity Manager installé, vous devez configurer les différents composants afin de disposer d'une solution pleinement fonctionnelle.



### 5.4.1 Synchronisation des données

Identity Manager utilise des pilotes pour synchroniser les données entre plusieurs applications, bases de données, systèmes d'exploitation et répertoires. Dès lors, après avoir installé Identity Manager, vous devez créer et configurer un ou plusieurs pilotes pour chaque système avec lequel vous souhaitez synchroniser les données.

Pour chaque pilote, un guide explique les conditions requises et les étapes de configuration nécessaires à la synchronisation des données. Ces guides sont disponibles sur le site Web de documentation des pilotes Identity Manager 4.0 (http://www.novell.com/documentation/idm40drivers/index.html).

Utilisez le guide spécifique pour chaque système géré afin de créer un pilote pour synchroniser les données d'identité.

## 5.4.2 Assignation de rôles

En cas de synchronisation d'informations entre les différents systèmes, utilisez l'administrateur d'assignation de rôles (RMA) pour gérer les rôles dans ces systèmes. Pour plus d'informations, reportez-vous au manuel *Novell Identity Manager Role Mapping Administrator 2.0 User Guide* (Guide de l'utilisateur de la version 2.0 de l'administrateur d'assignation de rôles de Novell Identity Manager).

## 5.4.3 Configuration de l'application utilisateur

L'étape suivante consiste à ajouter une perspective d'entreprise à la solution Identity Manager grâce à l'application utilisateur. L'application utilisateur permet de répondre aux besoins suivants de votre entreprise :

- proposer un moyen pratique d'effectuer des opérations de provisioning basées sur les rôles ;
- garantir que votre organisation dispose d'une méthode permettant de vérifier que le personnel est parfaitement au courant des stratégies organisationnelles et qu'il prend les mesures appropriées pour les respecter ;
- fournir un self-service utilisateur qui permet à un nouvel utilisateur de s'enregistrer lui-même et qui autorise l'accès par des utilisateurs anonymes ou invités ;
- assurer que l'accès aux ressources de l'entreprise respecte les stratégies organisationnelles et que le provisioning s'opère dans le cadre de la stratégie de sécurité de l'entreprise ;
- réduire la charge administrative que supposent la saisie, la mise à jour et la suppression d'informations utilisateur dans l'ensemble des systèmes de l'entreprise ;
- gérer le provisioning manuel et automatisé des identités, services et ressources ;
- prendre en charge des workflows complexes.

Le manuel *Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide* (Guide d'administration de l'application utilisateur de la version 4.0 du module de provisioning basé sur les rôles d'Identity Manager) explique comment configurer ces fonctions de l'application utilisateur.

## 5.4.4 Configuration des fonctions d'audit, de création de rapports et de conformité

La dernière étape de la création de votre solution Identity Manager, la plus importante, est la configuration des fonctions d'audit, de création de rapports et de conformité de manière à pouvoir vérifier que votre solution est en accord avec les stratégies de votre entreprise. Pour installer et configurer ces fonctions, reportez-vous aux guides suivants :

- **Audit :** reportez-vous au manuel *Identity Manager 4.0 Reporting Guide for Novell Sentinel* (Guide de création de rapports d'Identity Manager 4.0 pour Novell Sentinel).
- **Création de rapports :** reportez-vous aux manuels *Identity Reporting Module Guide* (Guide du module Identity Reporting) et *Using Identity Manager 4.0 Reports* (Utilisation des rapports Identity Manager 4.0).
- **Conformité :** reportez-vous à la section « Utilisation de l'onglet Conformité » du *Guide d'utilisation de l'application utilisateur du module de provisioning basé sur les rôles Identity Manager version 3.7.0*.

## 5.5 Administration d'Identity Manager

Une fois votre solution Identity Manager complète, il existe de nombreux guides qui peuvent vous aider à l'administrer, la tenir à jour et la modifier en fonction de l'évolution de votre entreprise. Les différents guides d'administration sont disponibles sur le site Web de documentation d'Identity Manager 4.0 (http://www.novell.com/documentation/idm40/index.html), sous l'intitulé Administration.