**DOSSIER SOLUTION**
CA IDENTITY SUITE

# Gestion et gouvernance des identités au service des utilisateurs métier

Comment combler le fossé entre l'IT et les utilisateurs métier

ca technologies

# Résumé

## Défi

En tant que leader IT, responsable de la sécurité ou dirigeant d'entreprise, vous évoluez dans un contexte à la fois changeant et exigeant. Les environnements IT sont de plus en plus distribués, complexes et hétérogènes. Cela dit, l'instauration de règles d'accès et leur application fiable représentent un défi aux multiples facettes, qui devrait impliquer les trois acteurs concernés : IT, sécurité et métier.

L'équipe IT se voit souvent allouer moins de budget et de ressources pour assumer ses responsabilités. Vous avez donc besoin d'une solution à la fois fiable et économique pour relever ces défis critiques de gestion des identités :

- Prise en main rapide par les nouveaux utilisateurs pour qu'ils deviennent productifs le plus rapidement possible
- Garantie que tous les utilisateurs disposent exclusivement des droits d'accès correspondant à leurs rôles actuels
- Automatisation des principaux processus d'identification pour une efficacité accrue et une réduction des coûts
- Identification et prévention des potentielles infractions aux règles (comptes orphelins, droits inappropriés, etc.) avant qu'elles ne se produisent
- Satisfaction des exigences d'audit en termes de suivi des droits attribués

Enfin, l'une des principales clés dans le contexte actuel :

- L'offre d'une expérience simple et intuitive permettant aux utilisateurs métier d'accéder facilement à vos services clés de gestion des identités.

## Solution

L'accent largement mis sur les utilisateurs métier a créé de nombreux défis pour les utilisateurs de la plupart des solutions de gestion des identités actuelles. Malheureusement, les quelques rares solutions qui offrent une expérience utilisateur acceptable manquent généralement d'envergure en termes de provisioning, de gestion des rôles et de gouvernance. Par ailleurs, elles ne sont pas suffisamment évolutives pour supporter la gestion des identités si l'entreprise est vaste. Vous êtes donc contraint de choisir entre fonctionnalités étendues et simplicité d'utilisation.

CA Identity Suite offre un moyen unique de combler le fossé entre les technologies IAM actuelles et les utilisateurs métier. Cette suite intégrée de fonctions de gestion et de gouvernance des identités combine des fonctionnalités robustes et une expérience orientée métier, intuitive et pratique. Elle peut simplifier vos processus de gestion des identités, améliorer la satisfaction utilisateur, supporter les applications aussi bien sur site que dans le Cloud, ainsi qu'offrir une réelle évolutivité au niveau des consommateurs. Qui plus est, elle peut être déployée facilement et rapidement.

# Les enjeux majeurs de la réussite de la gestion et de la gouvernance des identités

Ce document identifie les principaux défis liés à la gestion des identités que doivent aujourd'hui relever les entreprises ouvertes. Il décrit en quoi ces défis peuvent accélérer ou ralentir votre activité et présente un aperçu des fonctionnalités CA Identity Suite qui peuvent aider votre organisation à les surmonter.

Chacun des défis ci-dessous revêt à la fois un aspect métier et un aspect IT. Par le passé, l'expérience utilisateur pour les services de gestion des identités se focalisait surtout sur l'aspect IT, compliquant ainsi les interfaces et réduisant la satisfaction. Pour généraliser l'utilisation des services de gestion des identités et améliorer l'expérience utilisateur globale, l'environnement actuel nécessite un rapprochement entre les services IT et les utilisateurs métier. Nous allons donc explorer l'aspect métier et l'aspect technique de ces défis.

Les défis suivants requièrent une planification approfondie et devraient faire partie intégrante des plans de lancement :

- **Adoption par les utilisateurs** : amélioration et simplification de l'expérience utilisateur globale pour favoriser l'adoption des processus de gestion des identités par les utilisateurs
- **Demandes d'accès** : simplification du processus permettant aux utilisateurs d'obtenir l'accès aux applications dont ils ont besoin
- **Gestion des risques liés aux droits** : prévention des infractions aux règles d'attribution des droits
- **Certifications des accès** : hausse de productivité chez les responsables
- **Accès aux applications utilisateur** : accès pratique des utilisateurs à leurs applications phares
- **Analyse des identités en temps réel** : efficacité garantie des services clés de gestion des identités
- **Défis de déploiement** : amélioration du ROI et du délai de rentabilisation

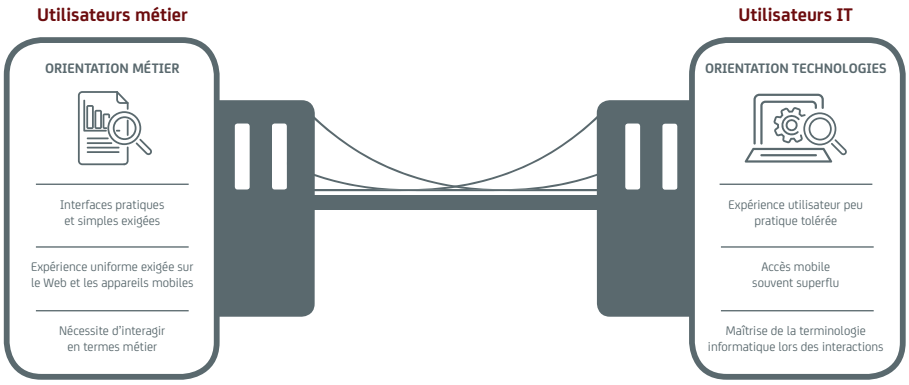
## Le défi : l'adoption par les utilisateurs

*« Les utilisateurs sont déçus du manque de convivialité de la plupart des fonctions de gestion des identités qu'ils doivent utiliser dans l'interface utilisateur. Nous ne pouvons dès lors décemment pas proposer ces services à un plus grand nombre d'utilisateurs au sein de l'entreprise. »*

L'un des défis majeurs de la réussite du déploiement des services de gestion des identités est que l'expérience utilisateur de ces services soit essentiellement centrée sur l'aspect IT. Par le passé, cela aurait pu convenir, mais étant donné que la gestion des identités dépasse désormais le domaine de l'utilisateur IT proprement dit, cette approche n'est plus envisageable. La terminologie et les procédures si évidentes pour un utilisateur IT averti peuvent se révéler déroutantes et frustrantes pour la plupart des utilisateurs métier. Cela se traduit par un faible taux d'adoption des processus de gestion des identités, une charge accrue pour les services IT, un non-respect des exigences réglementaires et une frustration des utilisateurs. Ces derniers ont besoin d'applications métier simples, rapides, ne nécessitant aucune formation et disponibles sur le périphérique de leur choix. Ils doivent être inclus dans les processus basiques de gestion des identités, mais cela n'est possible que s'ils trouvent l'expérience simple, intuitive et surtout uniquement aux professionnels qu'ils sont et non spécialistes IT.

## La solution CA Identity Suite

CA Identity Suite offre un moyen unique de combler le fossé entre les technologies IAM actuelles et les utilisateurs métier. Cette suite intégrée de fonctions de gestion et de gouvernance des identités combine des fonctionnalités robustes et une expérience orientée métier, intuitive et pratique. En améliorant la productivité et la satisfaction des utilisateurs métier, l'expérience utilisateur offerte par la solution CA Identity Suite entend accroître considérablement la proposition de valeur de la solution IAM pour les grandes entreprises, tout en allégeant les charges administratives de l'organisation IT.




Voici quelques-uns des nombreux avantages offerts par cette suite en termes d'expérience utilisateur :

- Un catalogue de droits pertinents, compréhensible par les professionnels
- Un tableau de bord et un outil de lancement pour les applications Web et mobiles
- Un référentiel unique : accès centralisé et facile à tous les services de gestion des identités pour les utilisateurs métier
- Une expérience de type panier virtuel pour les demandes et le suivi des accès
- Une expérience de type réseaux sociaux pour le suivi des demandes d'accès
- Des outils d'aide proactifs
- Une application mobile permettant à l'utilisateur de gérer les identités où qu'il soit et à tout moment

CA Identity Suite simplifie également la génération de tableaux de bord spécifiques et personnalisés, adaptés aux besoins uniques de rôles donnés, tels que dirigeants, agents de sécurité et partenaires commerciaux. Les administrateurs peuvent configurer l'interface en fonction du rôle utilisateur et des services auxquels ils ont accès. L'interface de la suite peut également être entièrement personnalisée pour respecter l'identité visuelle de votre marque, en intégrant par exemple le logo, la couleur, la police, les images d'arrière-plan souhaitées, et bien plus encore. Votre portail sera le fidèle reflet de l'identité de votre entreprise.

« Dans une enquête réalisée par un cabinet d'analystes, 97 % des clients interrogés ont signalé que l'expérience utilisateur offerte par Identity Suite était supérieure à celle des solutions concurrentes ».

Source : Enquête TechValidate

## Le défi : les demandes d'accès

*« Mes utilisateurs rencontrent des difficultés lors des demandes d'accès aux applications et systèmes dont ils ont besoin pour exercer leur fonction. La procédure est fastidieuse et les noms de ressources prêtent souvent à confusion pour mes utilisateurs métier. »*

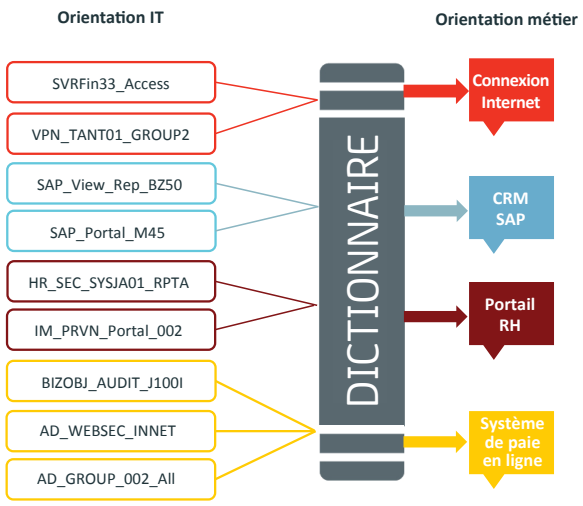
Les utilisateurs doivent pouvoir accéder rapidement et facilement aux applications et données dont ils ont besoin, tout en respectant les exigences réglementaires. Les systèmes de demande d'accès étaient souvent basés sur un ensemble de droits conçus pour des administrateurs qui comprenaient leur signification, puis imposés à des utilisateurs qui devaient quasiment apprendre un nouveau langage, pour ne pas dire un jargon IT. Alors qu'un nombre croissant d'utilisateurs métier sont impliqués dans les processus de gestion des identités au sein de leur entreprise, cette expérience loin d'être intuitive freine l'adoption, réduit la satisfaction et nécessite malgré tout l'intervention du personnel IT pour répondre aux questions d'utilisateurs déroutés.

Un nouveau mode d'interaction avec ces professionnels est nécessaire, et le domaine des demandes d'accès constitue un exemple parfait de l'intérêt de cette nouvelle approche. Il ne faut toutefois pas négliger le fait que les services IT ont également de réels besoins dans ce domaine, notamment pour automatiser les procédures basiques de demandes d'accès et pour simplifier l'audit des demandes et approbations. Ainsi, des fonctionnalités qui répondent aux besoins d'automatisation de l'IT tout en restant simples d'emploi pour les professionnels sont essentielles.

### La solution CA Identity Suite

CA Identity Suite offre une expérience simple et intuitive, ressemblant un peu à un « panier virtuel », qui simplifie considérablement la procédure de demande d'accès. Inspirée des sites de vente en ligne, la solution permet aux utilisateurs de mettre dans leur panier les rôles et droits dont ils ont besoin pour accomplir leurs tâches, de visualiser leurs droits actuels et de vérifier l'état de leurs demandes précédentes.

Le catalogue de droits pertinents joue un rôle central dans la qualité de l'expérience utilisateur offerte par CA Identity Suite. Il traduit des noms de ressources obscurs comme « TSS_MNG_per_view » en désignations plus explicites, telles que « Système de paie en ligne », ce qui permet aux utilisateurs métier de trouver plus facilement les ressources dont ils ont besoin. Pour encore simplifier l'accès, vous pouvez également regrouper les applications en catégories logiques, en créant par exemple un groupe nommé « Accès SRM » comprenant les applications SAP, les applications Oracle et les fonctionnalités SalesForce généralement utilisées par les professionnels, le tout en utilisant une terminologie compréhensible pour ces utilisateurs. L'illustration ci-contre représente le rapprochement opéré par le catalogue entre les termes orientés IT et ceux orientés métier.




Identity Suite inclut des outils d'aide proactifs qui permettent une simplification considérable de la procédure de demande d'accès. L'utilisateur peut afficher les rôles et les droits d'accès suggérés pour des utilisateurs similaires. Ces conseils proactifs permettent à l'utilisateur d'effectuer la demande appropriée à l'accès dont il a besoin. La suite fournit également un indice de risque, basé sur l'accès demandé et le degré de risque associé à ce type d'accès. L'utilisateur peut ensuite prendre une décision plus éclairée concernant l'accès qu'il doit demander.

## Le défi : la gestion des risques liés aux droits

*« Certains utilisateurs se voient parfois octroyer des droits par erreur, ce qui enfreint nos règles de sécurité. Je souhaite éviter ces infractions en amont. »*

Des attributions inappropriées de droits ont récemment été à l'origine de plusieurs divulgations de données. Ceci est d'autant plus vrai pour les utilisateurs à forts privilèges, car ils disposent souvent de droits très étendus. Toutefois, le principe est le même pour tous les utilisateurs : nous devons rectifier les attributions inadéquates de droits qui enfreignent les règles de sécurité avant que ceux-ci ne soient octroyés (« contrôle préventif ») et supprimer ceux potentiellement octroyés par erreur dans le passé (« contrôle réactif »). Si des contrôles efficaces ne sont pas mis en place dans les deux cas, le risque augmentera et les audits de conformité seront bien plus complexes.

Dans le même ordre d'idée, il arrive que les règles évoluent et que les accès octroyés par le passé ne soient plus conformes aux nouvelles règles. Lors des certifications d'accès de routine, il est important que le responsable puisse s'en rendre compte afin de suspendre la certification de cet utilisateur pour le droit d'accès en question.

### La solution CA Identity Suite

CA Identity Suite vous permet de formuler, d'appliquer et de valider des règles de processus métier pour implémenter la séparation des fonctions et d'autres contraintes logiques liées aux relations entre utilisateurs, rôles et droits. Par exemple, une règle de processus métier peut modéliser une contrainte, « les personnes autorisées à accéder à X ne sont pas autorisées à accéder à Y » ou une relation de dépendance, « seules les personnes ayant accès à A sont autorisées à effectuer l'action B ». Il est ainsi possible d'éviter en amont les instances susceptibles d'enfreindre ces règles de sécurité.

La suite peut également vous alerter si des droits conflictuels sont demandés (contrôles préventifs décrits plus haut). Elle assigne un indice de risque en fonction de l'accès demandé et de la règle associée. Cet indice se base sur l'utilisateur, ses autres droits et tous les facteurs contextuels potentiellement pertinents. Le demandeur est informé de ce niveau de risque lorsque la demande d'approbation est émise, afin de l'alerter d'une éventuelle demande inappropriée. De la même manière, l'approbateur voit cet indice de risque lors de la procédure d'approbation, ce qui garantit une visibilité totale et peut éviter l'octroi d'un accès à haut risque.

La suite propose également des contrôles réactifs pour remédier à des droits d'accès inadaptés déjà octroyés. Lors de la certification, la suite contrôle que les droits d'accès sont conformes aux règles et vous indique si un utilisateur dispose de droits inappropriés. Les infractions s'affichent clairement pour chaque utilisateur afin que le responsable puisse prendre des mesures sans tarder. Ces deux types de contrôles peuvent considérablement réduire le risque d'octroi ou de maintien de droits inadaptés.

## Le défi : la certification des accès

*« J'aimerais simplifier les certifications et les rendre intuitives, afin de pouvoir améliorer la productivité de mes responsables et faciliter mes audits de conformité. »*

Nous avons déjà vu l'importance d'une fonction automatisée assurant la traduction des informations d'accès des utilisateurs en un langage et un format appropriés à chaque type de campagne de certification que vous menez. Si les noms des accès sont explicites et orientés métier, si un workflow flexible peut être conçu pour répondre à vos besoins spécifiques, et si le suivi et le statut de chaque campagne sont facilement disponibles, votre programme de certification a plus de chances de réussir.

### La solution CA Identity Suite

Les fonctionnalités de certification de CA Identity Suite s'appuient sur le catalogue de droits pertinents, ce qui permet aux responsables de comprendre très facilement les droits d'accès de chaque employé, puis de les approuver, refuser ou déléguer. En outre, un indice de risque est disponible si un droit d'accès donné, ou une combinaison de droits d'accès, est particulièrement risqué(e). En accordant de la visibilité à ces évaluations des risques, la certification n'est plus seulement une proposition à laquelle il convient de répondre par oui ou non, mais une opportunité de mettre en évidence des risques qui n'auraient pas pu être repérés par un autre biais.

CA Identity Suite est suffisamment flexible pour supporter de nombreux types de campagnes de certification et notamment les suivantes :

- **Certification d'entités :** permet de certifier les droits d'accès associés aux entités d'utilisateurs, de rôles ou de ressources sélectionnées par les responsables, les propriétaires de rôles et les responsables de ressources.
- **Recertification :** permet de répéter le processus de certification en se basant sur une campagne précédente.
- **Différentiel :** amorce une campagne de certification qui repose uniquement sur les droits ayant changé depuis une campagne précédente.
- **Auto-attestation :** permet à chaque utilisateur (par opposition aux responsables ou propriétaires de ressources) de certifier ses propres privilèges. Ce type de campagne peut satisfaire à certaines exigences juridiques pour la certification de sécurité des données.

Les campagnes de certification peuvent être fastidieuses, chronophages et finalement inefficaces en termes de réduction des risques. Non seulement CA Identity Suite renforce l'efficacité de ce processus d'un point de vue sécurité et conformité, mais elle s'inscrit dans le contexte d'une expérience utilisateur facile et hautement intuitive, plébiscitée par les responsables.

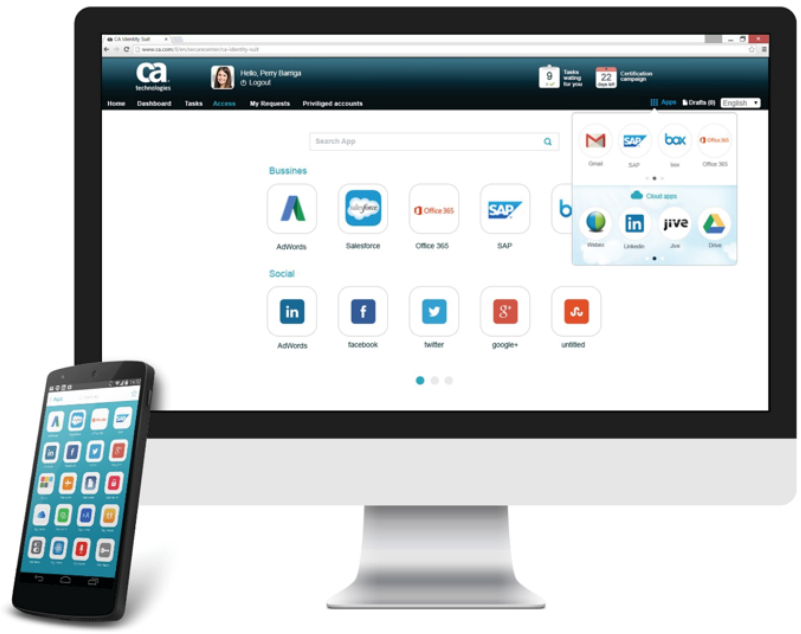
## Le défi : la facilité d'accès aux applications

*« Je voudrais que mes utilisateurs aient très facilement accès à toutes les applications pour lesquelles ils disposent de droits d'accès, et ce aussi bien dans le Cloud que sur site. L'accès doit aussi être possible sur l'ensemble de leurs appareils. »*

Les utilisateurs sont agacés lorsque la procédure pour obtenir l'accès à l'une de leurs nombreuses applications est fastidieuse. La multiplicité des connexions et la complexité de lancement des applications constituent des plaintes récurrentes. Alors que la mobilité augmente et que les utilisateurs s'habituent à la facilité de ces interfaces, les défis liés à la frustration et à la productivité peuvent également se multiplier. Vous avez besoin d'un moyen plus pratique d'obtenir rapidement et facilement accès aux applications, qui applique l'authentification unique (SSO) en se limitant aux applications auxquelles chaque utilisateur est autorisé à accéder.

### La solution CA Identity Suite

CA Identity Suite inclut une plate-forme de lancement d'applications Web et mobiles qui propose aux utilisateurs un tableau de bord unique permettant d'accéder rapidement et facilement à toutes les applications Web, Cloud et mobiles pour lesquelles ils disposent d'autorisations. Cette plate-forme de lancement est accessible depuis tous les périphériques et offre des fonctionnalités de recherche avancée. Une fois les utilisateurs connectés à CA Identity Portal, toutes leurs applications Web sont accessibles en un clic et toutes les applications auxquelles ils accèdent sur leur bureau sont également toujours disponibles via CA Identity Portal Mobile. Cette plate-forme de lancement permet aux employés de rester productifs où qu'ils soient grâce au déploiement du SSO pour les applications Web et mobiles, dans un format mobile.



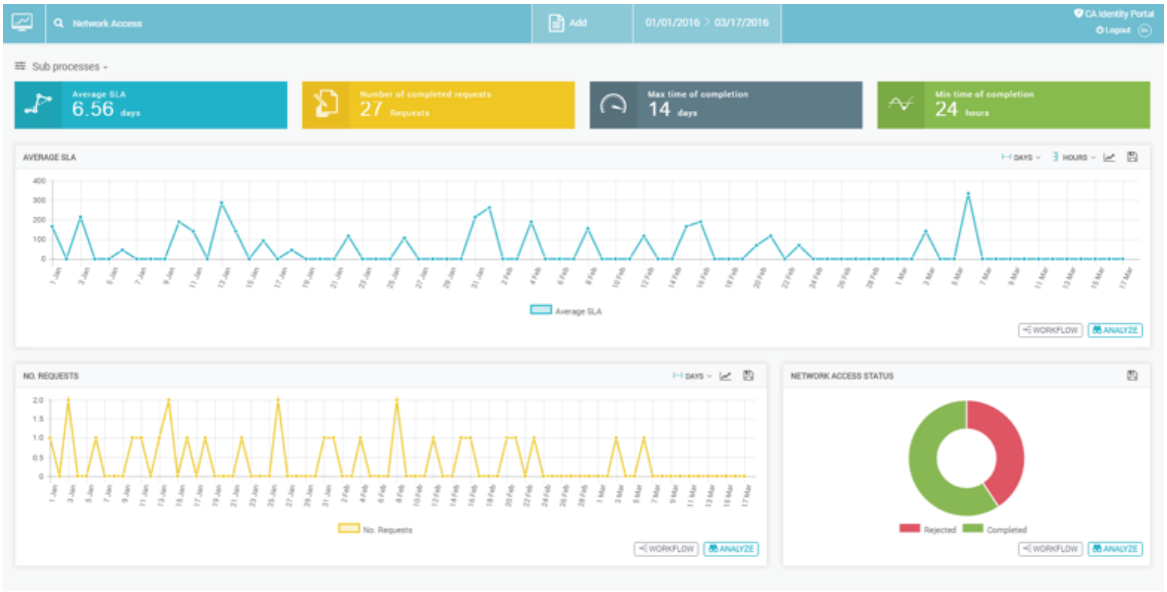
## Le défi : garantir l'efficacité des processus pour respecter les accords sur les niveaux de service

*« Mes processus de gestion des identités ne fonctionnent pas tous de manière optimale. D'autres responsables se plaignent des niveaux de service que je fournis. Je ne dispose toutefois pas d'informations suffisantes pour pouvoir identifier les goulets d'étranglement et les résoudre. »*

Les processus liés à la gestion des identités sont souvent complexes et peuvent impliquer des workflows en plusieurs étapes. Lorsque ces processus ne fonctionnent pas efficacement, par exemple si un groupe d'utilisateurs ne terminent pas leurs tâches dans les temps, c'est l'ensemble du système qui risque d'être ralenti et les objectifs sur les niveaux de service (SLA) ne pourront pas être respectés. Lorsque des processus fondamentaux comme des certifications d'accès ne sont pas finalisés conformément aux objectifs de services convenus, cela génère des faiblesses d'audit ou augmente tout simplement l'inefficacité. Sans une visibilité adéquate du fonctionnement détaillé de ces processus, il n'est pas possible d'identifier la cause de ces problèmes, ni de la résoudre rapidement.

### La solution CA Identity Suite

CA Identity Suite propose des analyses en temps réel permettant de mieux comprendre le fonctionnement des processus clés de gestion des identités et de les optimiser. Vous pouvez ainsi identifier les goulets d'étranglement et garantir le respect de vos SLA essentiels. Prenons un exemple simple. Le graphique ci-dessous affiche une vue temporelle des accords sur les niveaux de service actuels au cours du mois précédent, ainsi que des valeurs clés, comme les accords sur les niveaux de service moyens, maximum et minimum pour un processus donné. Il indique aussi la fréquence d'arrivée de nouvelles demandes au cours de chaque jour du mois précédent, ainsi qu'un récapitulatif de l'état (terminé, rejeté) de toutes ces demandes. Cette fonctionnalité confère au responsable une bien meilleure visibilité et permet d'optimiser les processus et de voir très facilement l'état de ces processus.



## Le défi : la difficulté du déploiement

*« Le déploiement de ma solution de gestion des identités est chronophage et difficile. Dans un premier temps, le simple fait d'installer et de configurer les logiciels prend des journées entières. Ensuite, il faut parfois des semaines pour rendre opérationnels certains scénarios de base, car j'ai besoin d'un code personnalisé. Il faut aussi définir des workflows, des règles, sans oublier l'interface utilisateur. »*

Le déploiement d'une solution de gestion des identités robuste peut se révéler complexe et coûteux. Cela peut facilement prendre des semaines pour rendre opérationnelles certaines fonctionnalités de base. Par ailleurs, des exigences telles que des connecteurs pour applications personnalisées, peuvent monopoliser pas mal de ressources et de temps.

### La solution CA Identity Suite

La solution CA Identity Suite peut *considérablement* réduire le temps nécessaire avant d'être opérationnel, grâce aux fonctionnalités suivantes :

- **Appliance virtuelle (vApp).** vApp supprime la phase d'installation traditionnelle et fournit une image de machine virtuelle préinstallée et préconfigurée, prête à fonctionner dans des configurations de production sur des plates-formes de virtualisation courantes. vApp intègre un système d'exploitation renforcé, un serveur d'applications et le logiciel CA Identity Suite. Cette appliance inclut également un support intégré pour des procédures DevOps courantes, comme les configurations de haute disponibilité, les ajustements de capacité, les agrégations de journaux, les patchs applicables aux plates-formes et les mises à jour logicielles.

  Pour déployer des services de gestion des identités, faites simplement glisser le nom du service sur le nom de la machine concernée et l'installation sera effectuée automatiquement. En faisant glisser le même service sur plusieurs machines, tous les mécanismes de communication de haute disponibilité (équilibrage de charge, basculement, etc.) seront exécutés automatiquement. Aucune configuration manuelle, chronophage et propice aux erreurs n'est requise. Les gains de temps sont considérables.

  Cette approche entraîne une réduction spectaculaire du délai de rentabilisation et du coût total de possession. Vous obtenez plus de résultats avec la même équipe et le même budget. Cette méthode permet aussi d'économiser chaque année des milliers de dollars en frais de licences logicielles, car tous les composants système clés peuvent être déployés librement sans licence supplémentaire.
- **Deployment Xpress (Depx).** DepX représente une amélioration spectaculaire en termes de déploiement de logiciels de gestion des identités. Il s'agit d'un ensemble de scénarios préconfigurés pour les cas d'utilisation courants dont la plupart des organisations ont besoin, notamment l'intégration d'utilisateurs et de partenaires, la réinitialisation des mots de passe, les certifications d'accès, etc. Chaque scénario comprend tous les éléments nécessaires pour faciliter le déploiement, comme des modèles d'interface utilisateur, des workflows et des définitions de règles. Le responsable sélectionne simplement les scénarios dont vous avez besoin, les place dans le panier et procède au règlement. À ce stade, tous ces éléments clés sont automatiquement chargés dans Identity Suite et déployés. Vous pouvez personnaliser ces éléments (par exemple l'image de marque pour l'interface), mais aucun code personnalisé n'est requis. Ces scénarios accélèrent le processus de déploiement et peuvent considérablement réduire le délai de rentabilisation du déploiement de services classiques de gestion des identités.
- **Autres outils Xpress.** Identity Suite inclut d'autres outils qui simplifient nettement la gestion de votre environnement de déploiement, notamment :
  - Connector Xpress simplifie le processus de création de connecteurs pour les applications « maison » et facilite la connexion aux systèmes qui ne disposent pas de connecteurs OOTB.
  - Config Xpress vous permet de déplacer plus rapidement et facilement des composants entre différents environnements de simulation. Cela simplifie la gestion des configurations et vous donne plus de temps pour les tests de fonctionnement.
  - Policy Xpress vous permet de configurer les règles qui exécutent vos processus métier uniques et complexes. Cette étape nécessite généralement le développement d'un code personnalisé, mais cet outil basé sur un assistant vous permet de concevoir des règles en interne en quelques heures, au lieu de plusieurs semaines de programmation.

# Fonctionnalités clés

CA Identity Suite offre les principaux avantages suivants :

- Portail d'identité en self-service (référentiel unique) : centralise les données relatives aux droits et présente un « panier » intuitif de demandes d'accès.
- Réduction des délais de déploiement, de quelques jours à quelques minutes.
- Catalogue de droits pertinents : simplifie la compréhension des demandes d'accès et de la certification des droits pour les utilisateurs métier.
- Analyse proactive : conseille et avertit les utilisateurs métier des infractions potentielles des règles et empêche ces infractions.
- Provisioning des utilisateurs pour une multitude d'applications sur site, de services SaaS et de systèmes non connectés.
- Self-service des utilisateurs : leur permet de gérer leurs propres informations afin d'alléger la charge des départements IT.
- Deployment Xpress : des modèles de scénarios préconfigurés simplifient considérablement le déploiement initial et la gestion continue.
- Personnalisation sans codage personnalisé : des fonctionnalités puissantes telles que ConfigXpress, PolicyXpress et ConnectorXpress permettent de personnaliser l'infrastructure de gestion des identités sans codage personnalisé.
- Nettoyage des droits : analyse des droits systèmes existants et mise en évidence des droits superflus ou excessifs.
- Modélisation des rôles avec un moteur d'analyse de pointe : permet de trier efficacement des volumes importants d'informations sur les utilisateurs et les droits afin de détecter les rôles potentiels.

ca technologies

**Restez connecté à CA Technologies sur ca.com/fr**

CA Technologies (NASDAQ : CA) fournit les logiciels qui aident les entreprises à opérer leur transformation numérique. Dans tous les secteurs, les modèles économiques des entreprises sont redéfinis par les applications. Partout, une application sert d'interface entre une entreprise et un utilisateur. CA Technologies aide ces entreprises à saisir les opportunités créées par cette révolution numérique et à naviguer dans « l'Économie des applications ». Grâce à ses logiciels pour planifier, développer, gérer la performance et la sécurité des applications, CA Technologies aide ainsi ces entreprises à devenir plus productives, à offrir une meilleure qualité d'expérience à leurs utilisateurs et leur ouvre de nouveaux relais de croissance et de compétitivité sur tous les environnements : mobile, Cloud, distribué ou mainframe. Pour plus d'informations, rendez-vous sur **ca.com/fr**.



CS200-230014_1016