RAC/M IDENTITY

# REPRENEZ LE CONTRÔLE DE VOS IDENTITÉS

## Atteignez la conformité, réduisez les coûts et les risques

Comme lorsqu'elles tentent de suivre les poissons dans l'océan, les organisations sont confrontées au défi de la validation et du contrôle de l'accès au système et ce, dans une mer de complexité.

RAC/M Identity™ est une solution GIA simple et efficace qui permet aux entreprises, grandes et petites, de comprendre et de gérer les relations complexes entre les utilisateurs et leurs accès aux ressources physiques et numériques, que ce soit sur site ou en mode infonuagique.

RAC/M Identity™ est la pierre **angulaire** sur laquelle bâtir un programme GIA capable de transformer vos défis les plus redoutables en un avantage concurrentiel. Ces défis comprennent le manque de ressources, les budgets limités, les échéanciers stricts et la transformation rapide alimentée par l'accélération de l'adoption des nuages et de l'Internet des objets.

RAC/M Identity™ s'attaque également à l'un des défis les plus difficiles auxquels sont confrontés les programmes de GIA - le maintien de l'engagement continu des cadres supérieurs. Il génère automatiquement un score de santé composite qui reflète la maturité et l'efficacité des processus clés de la GIA, permettant à la direction exécutive d'évaluer les progrès réalisés ainsi que le chemin qui reste à parcourir.

## Simplifiez votre programme de gouvernance des identités et des accès

Au fur et à mesure que les organisations grandissent, il devient de plus en plus complexe de comprendre qui a accès à quoi et de garder le contrôle en raison de défis tels que la fragmentation des populations d'utilisateurs, la complexité et l'évolution rapide du paysage technologique et les pratiques de gestion incohérentes.

En simplifiant la gouvernance de l'identité, RAC/M Identity permet à une organisation d'obtenir et de démontrer rapidement le contrôle de l'accès aux informations critiques, comme l'exigent les différents cadres réglementaires tels que GDPR, SOX, PCI, NERC, HIPAA, etc.

### Réduisez vos coûts avec la GIA en mode Service

Vous pouvez réaliser des économies substantielles et éviter de maintenir un personnel hautement qualifié en déployant RAC/M Identity en tant que Service. RAC/M Identity peut être déployé en mode infonuagique, éliminant ainsi le besoin d'une infrastructure coûteuse et complexe sur place, tandis qu'OKIOK fournit des services de gestion quotidienne tels que la surveillance, la mise à jour, la mise à niveau, les correctifs de sécurité et les évolutions.

D'autres économies sont réalisées en évitant la personnalisation et le codage grâce à la configuration de modules préconstruits et à l'utilisation de processus et de flux de travail GIA standardisés mais flexibles.

### Obtenez des résultats rapidement

RAC/M Identity est conçu autour d'un référentiel de données qui fournit une vue complète de tous les comptes, accès et droits détenus par tous les utilisateurs sur tous les actifs concernés. La réconciliation en temps quasi réel du référentiel avec toutes les sources d'identité et tous les systèmes cibles, qu'ils soient sur site ou en infonuagique, associée à de puissantes fonctions d'analyses et de rapports, offre une visibilité immédiate après le déploiement. Le référentiel permet de détecter et de corriger immédiatement les situations à risque ainsi que de lancer rapidement des examens périodiques de l'accès, améliorant ainsi la maturité et l'efficacité des processus de la GIA.

### Réduisez le risque

Le risque est réduit en identifiant et en remédiant en permanence aux situations à risque telles que les comptes orphelins ou malicieux, ainsi qu'en révoquant rapidement les accès inutiles lorsque les personnes quittent l'organisation ou changent de rôle. De plus, des examens périodiques de l'accès permettent aux gestionnaires et aux propriétaires de biens de valider l'accès aux biens essentiels.

### Engagez vos employés

RAC/M Identity améliore l'expérience utilisateur et la productivité en fournissant une authentification unique (Single Sign-On (SSO)) avec des domaines Active Directory ainsi qu'un portail libre-service qui permet d'effectuer des opérations clés telles que les demandes d'accès, les approbations et la réinitialisation des mots de passe depuis n'importe quel appareil doté d'un navigateur compatible.

## Une approche différente, axée sur la gouvernance des identités

RAC/M Identity diffère des suites traditionnelles de gouvernance et d'administration de l'identité (GIA) par le fait qu'elle est proposée dans le cadre d'une offre de services complète, soutenue par une méthodologie de déploiement éprouvée et sans risque.

Notre approche est centrée sur la mise en œuvre d'une base solide, axée sur l'amélioration des processus de gouvernance de l'identité avant l'automatisation de l'approvisionnement.

En fait, les projets de déploiement trébuchent souvent lorsqu'il s'agit d'essayer d'automatiser à la hâte des processus GIA sans avoir une compréhension claire des pratiques obscures, sans prendre le temps de nettoyer les données d'accès et d'établir une vision claire et partagée des objectifs finaux.

RAC/M Identity met de l'avant l'établissement d'une stratégie de gouvernance d'identité claire, adaptée aux besoins réels de votre organisation, en vous fournissant les capacités critiques qui vous permettront d'y parvenir :

- Comprendre rapidement les identités et la structure des droits d'accès de votre organisation pour l'ensemble des sources d'identités intégrées, des systèmes cibles et des applications
- Identifier et révoquer les identités et les comptes inutiles
- Gérer les comptes des employés, des utilisateurs privilégiés, des entrepreneurs et des utilisateurs externes.
- Gérer les comptes de services, partagés, génériques et techniques.
- Affecter les propriétaires, les approbateurs, les examinateurs et les fiduciaires aux actifs, aux comptes et aux rôles.
- Définir un modèle d'accès structuré basé sur les rôles métier et applicatifs et les règles d'affectation.
- Définir, surveiller et appliquer des règles de séparation des tâches (SOD) pour prévenir la fraude et les erreurs.
- Mettre en œuvre un processus souple de certification des accès pour les identités, les rôles, les droits et les conflits de ségrégation des tâches.
- Promouvoir la gestion des accès en libre-service et la réinitialisation des mots de passe grâce à des flux d'approbation automatisés.
- Automatisez l'arrivée, le départ et le mouvement des utilisateurs en approvisionnant et en dé-provisionnant automatiquement les comptes, les membres de groupes et les droits dans les systèmes cibles connectés.
- Fournir tous les artefacts requis à l'appui des exigences en matière de conformité et de vérification.
- Générer automatiquement des métriques pour maintenir le support exécutif du programme GIA.

## Flexibilité par la configuration

RAC/M Identity s'adapte facilement à n'importe quel contexte technologique et commercial en s'intégrant aux systèmes et processus d'affaires existants grâce à la configuration d'un riche éventail de modules intégrés. Pour réduire le temps et les efforts d'intégration, RAC/M Identity peut traiter tout type de données de référence représentant votre structure organisationnelle, vos flux de travail (workflows), votre nomenclature ou votre logique métier.

L'expérience utilisateur peut être améliorée en personnalisant les étiquettes dans les formulaires d'affichage pour correspondre à la nomenclature propre de votre organisation. Cette approche élimine les efforts coûteux de personnalisation, réduit les coûts de déploiement et permet d'obtenir de meilleurs résultats plus rapidement.

## Modèle de données sans limite

Une caractéristique clé de RAC/M Identity est la capacité d'étendre dynamiquement le modèle de données pour représenter et gérer n'importe quel nombre d'attributs spécifiques remplis à partir des sources de données des clients. Ces attributs étendus sont définis par le client et peuvent être attachés à des éléments d'information tels que les identités, les rôles, les comptes, les groupes et les organisations. Ces attributs étendus peuvent être invoqués tout comme les attributs d'objet de base standard pour mieux définir la logique métier ou filtrer les résultats de recherche.

## Des résultats rapides et convaincants

Chaque implémentation de RAC/M Identity commence par le mappage, la consolidation et l'analyse des données d'identité. Ces premières étapes catalysent une transformation organisationnelle qui apporte des améliorations immédiates et durables aux pratiques de gestion de l'accès à l'information. En fait, RAC/M Identity a permis à nos clients d'analyser, de détecter et de révoquer les comptes et les droits inutiles, en quelques jours après la mise en œuvre.

## Puissants algorithmes d'appariement

Les données d'identité du monde réel ne sont jamais propres, complètes ou fiables. Demandez à toute personne qui a essayé de faire correspondre manuellement plusieurs comptes système à des identités uniques. Pour aider et supporter dans ce défi, RAC/M Identity inclut un ensemble d'algorithmes d'appariement puissants.

Ces algorithmes permettent aux utilisateurs de résoudre rapidement de nombreuses conditions d'appariement complexes telles que :

- collisions de noms
- fautes d'orthographe
- orthographes alternatives
- ordre différent des composants d'appellation
- et encore davantage de situations.

La logique d'appariement peut être affinée de façon itérative pour atteindre un appariement automatisé de plus de 80 % des comptes, en fonction de la qualité des données source. Tous les comptes ou identités non appariés restants peuvent être appariés à l'aide d'outils simples.

## Forage de rôles et modélisation

RAC/M Identity comprend un puissant outil d'exploration et de modélisation des rôles.

Des règles de filtrage sont définies pour déterminer le sous-ensemble d'identités et d'actifs à analyser (ou à extraire) pour les similitudes. Ces règles peuvent utiliser n'importe quel attribut de base ou étendu pour déterminer les identités et les actifs à analyser.

Les rôles peuvent également être affectés de haut en bas. Les ingénieurs de rôle ou les experts en la matière peuvent définir l'appartenance à un groupe et d'autres droits à accorder comme une seule unité. Les rôles prennent en charge simultanément l'affectation dynamique aux membres par le biais de règles d'affectation, ainsi que l'affectation statique à des membres spécifiques.

La combinaison des approches ascendante et descendante constitue une conception puissante et flexible des capacités et met en œuvre un modèle de rôle à deux niveaux où les rôles métier et applicatif sont liés et assignés dynamiquement par des règles et politiques.

## Capacité d'intégration

RAC/M Identity s'intègre facilement à pratiquement n'importe quel système source et cible d'identité. Il le fait avec des connecteurs ICF (Identity Connector Framework) et des collecteurs de fichiers plats flexibles et conformes aux normes de l'industrie. Ces connecteurs ainsi que la logique métier prédéfinie sont intégrés dans de nombreux modèles prédéfinis pour les applications sur site et les systèmes existants tels que Active Directory (AD), les répertoires LDAP, les bases de données SQL, SAP BW, les fichiers IDoc, AS/400 et les applications infonuagiques telles que Office 365.

Cette architecture flexible permet à RAC/M Identity de s'adapter facilement à tout environnement technique existant et futur.

## Réduction des risques

RAC/M Identity réduit les surfaces d'attaque en éliminant systématiquement les comptes et droits inutiles, en contrôlant les comptes sur privilégiés, en effectuant des rapprochements en temps quasi réel entre les sources d'identité et tous les systèmes cibles, en renforçant les flux d'approbation des demandes d'accès et en permettant des revues périodiques et ad hoc.

## Évolutivité

RAC/M Identity est évolutive et peut être déployé dans une organisation de toute taille. Le modèle unique de gouvernance d'identité en tant que service et le faible coût total de possession font de RAC/M Identity une solution viable lorsque les autres solutions GIA sont trop coûteuses ou ne peuvent répondre aux exigences fonctionnelles. Il est conçu pour gérer un nombre illimité d'identités dans des scénarios complexes de gestion des effectifs et des utilisateurs externes.

## EXPÉRIENCE UTILISATEUR

| Caractéristiques | Avantages |
|---|---|
| Interface Web | Les administrateurs peuvent facilement effectuer toutes les tâches de configuration et de gestion à partir de n'importe quel navigateur. |
| Interface web réactive | Des tâches telles que les révisions des accès, les approbations de demandes d'accès et la réponse aux notifications peuvent être effectuées à partir de n'importe quel navigateur et des appareils mobiles pris en charge. |
| Portail libre-service intégré entièrement personnalisable | Les demandes d'accès peuvent être émises par les utilisateurs finaux, les gestionnaires ou les super utilisateurs à travers le portail libre-service inclus qui peut être personnalisé. |
| Intégration avec le portail libre-service GSTI | La fonctionnalité libre-service peut être mise en œuvre par l'intégration avec un portail libre-service existant ou GSTI tel que Service Now. |
| SOAP et REST APIs pour les fonctions administratives | Les fonctions de libre-service et d'administration peuvent être exécutées via les API REST et SOAP. |
| Champs personnalisables | Améliorer l'expérience utilisateur en personnalisant les champs dans l'interface utilisateur pour correspondre à la nomenclature spécifique à l'organisation. |

## CAPACITÉS

| Caractéristiques | Avantages |
|---|---|
| Connecteurs bidirectionnels ICF pour l'intégration des sources d'identités et des systèmes cibles | Intégration bidirectionnelle de pratiquement n'importe quel système cible, application SaaS ou source d'identité, tels que:<br>•Active Directory<br>•Annuaires LDAP<br>•Bases de données SQL<br>•SAP BW<br>•SAP IDocs<br>•Serveur Windows 2008/2012/2016<br>•*NIX systems (*Linux/Unix)<br>•Microsoft Graph API (Office 365, Azure, etc.)<br>•AS/400<br>•Tout système cible, application SaaS ou source d'identité via un connecteur de script |
| Connecteurs unidirectionnels | Les collecteurs unidirectionnels peuvent importer et traiter des données à partir de n'importe quelle source d'identité, système cible ou application qui peut exporter des données d'accès vers un fichier plat tel que CSV, XLS, XLSX, IDOC, etc. |
| Algorithmes d'appariement automatisé | Des algorithmes d'appariement automatisés tels que soundex, soundex multiple, permutations ainsi qu'une logique d'affaires flexible peuvent faire correspondre un pourcentage élevé de comptes aux identités sans intervention de l'utilisateur. |

| Caractéristiques | Avantages |
|---|---|
| Interface d'appariement manuel | Les comptes restants et les identités peuvent être appariés manuellement en utilisant n'importe quelle combinaison d'algorithmes et de facteurs multiples pour maximiser la vitesse et la fiabilité. |
| Étiquettes de compte et catégories | Le traitement et la catégorisation des comptes permettent un suivi et un contrôle efficace de tous les types de comptes, y compris les comptes personnels, génériques, techniques, privilégiés et autres. |
| Extraction de rôles | Les rôles peuvent être extraits des accès existants en utilisant des règles de filtrage puissantes pour les actifs et les identités. Les rôles peuvent également être construits et réglés manuellement. |
| Attribution dynamique et statique des rôles | Les rôles peuvent être attribués automatiquement en fonction des règles et des attributs (ABAC). Les rôles peuvent également être attribués statiquement à des identités spécifiques. |
| Réconciliation du référentiel | Le référentiel est automatiquement maintenu en pleine synchronisation avec toutes les sources d'identité et les systèmes et application cibles, offrant ainsi une visibilité complète et fiable des identités et des accès. |
| Configuration des éléments de logique d'affaires | Obtenir des résultats beaucoup plus rapides en éliminant la longue et fastidieuse programmation et le scriptage. |
| Métriques, tableaux de bord et aperçus | Fournir une visibilité immédiate de l'efficacité et de l'efficience des processus de GIA ainsi que de l'état du référentiel. Les aperçus offrent une visibilité immédiate des situations à risque classées par criticité pour une résolution rapide. |

| Caractéristiques | Avantages |
|---|---|
| Bilan de santé du programme de GIA | Maintenir l'appui de la haute direction au programme de GIA et maintenir l'engagement de la direction en exprimant la maturité et l'efficacité des processus clés de GIA via un indicateur unique pour l'analyse comparative et le suivi de la posture de GIA. |
| Affichages personnalisés | Optimiser l'expérience utilisateur en fournissant un affichage de la console d'administration adapté à la responsabilité de l'utilisateur et au niveau de privilège. |
| Rapports exhaustifs | Effectuer des analyses puissantes et générer des rapports à partir d'une multitude de rapports intégrés. Au besoin, la configuration de rapport personnalisés est possible. |
| Campagne de révision des accès flexible | Les campagnes entièrement configurables et les flux de travail de suivi permettent au chef de campagne d'exercer un contrôle total sur la gouvernance en se concentrant sur les ressources critiques et en assurant leur exécution en temps voulu. Les requêtes automatisées garantissent que les actions correctives sont prises en charge rapidement tout au long de la campagne. |
| Password management | Les utilisateurs peuvent réinitialiser leurs mots de passe via le portail libre-service. |
| Password synchronization | Les changements de mots de passe peuvent être propagés du Active Directory vers les systèmes cibles compatibles. |

## RAC/M IDENTITY EST OFFERT EN DEUX MODÈLES POUR ASSURER LE MAXIMUM DE FLEXIBILITÉ

**Sur site**
Vous gérez et exploitez la solution dans votre centre de données

**En mode infonuagique (SaaS)**
OKIOK fournit le nuage et gère pendant que vous exploitez la solution.

| | SUR SITE | MODE INFONUAGIQUE |
|---|---|---|
| **Configuration matérielle et logicielle requise** | Veuillez communiquer avec un revendeur autorisé OKIOK pour connaître les exigences les plus récentes. | Aucune configuration matérielle ou logicielle requise. Connectivité avec Microsoft Azure active par VPN. |
| **Modèle de souscription** | Annuel, selon le nombre d'identités<br>Inclus un environnement limité de préproduction | Annuel, selon le nombre d'identités<br>Inclus un environnement limité de préproduction |
| **Modèle en service géré** | Réalisé par le client | Réalisé par OKIOK:<br>• Dimensionnement & gestion de la charge de travail<br>• Suivi de la disponibilité et de la performance<br>• Mise à niveau, correctifs, mise à jour<br>• Sauvegardes & reprise après sinistre<br>• Enquêtes sur les questions opérationnelles |
| **Configuration logicielle requise pour le client** | Windows: Microsoft Internet Explorer 11, Microsoft EDGE, version actuelle de Firefox et Chrome<br>Mac OS X: Safari, Opera, tout navigateur compatible | |

Veuillez contacter un revendeur agréé pour plus d'informations et pour les prix.

OKIOK

**OKIOK est un chef de file en matière de sécurité informatique.** Depuis 1973, OKIOK se démarque par l'excellence de ses produits et la qualité de ses services. OKIOK offre une vaste gamme de solutions intégrées conçues pour répondre aux besoins des entreprises de toutes tailles.

www.okiok.com | info@okiok.com | 1 877 561-1681
Dernière mise à jour: Septembre 2019 