TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

IDENTITY ACCESS MANAGER (IAM)

DANS LA PRATIQUE, RARES SONT LES DÉPLOIEMENTS DE SOLUTIONS DE GESTION DES IDENTITÉS ET DES ACCÈS QUI S'EFFECTUENT EN SEULE ET UNIQUE OPÉRATION, ON PROCÈDE GÉNÉRALEMENT PAR ÉTAPES, UNE APPROCHE BIEN PLUS PRAGMATIQUE SI L'ON SOUHAITE PARVENIR AU RÉSULTAT ESCOMPTÉ. AINSI, IAM PREND EN CHARGE CETTE MÉTHODE D'IMPLÉMENTATION PAR PHASES, AU MOYEN DE DIFFÉRENTS MODULES. CES MODULES PEUVENT ÊTRE IMPLÉMENTÉS INDIVIDUELLEMENT ET SUIVANT UN ORDRE ALÉATOIRE.

LES MODULES PROPOSÉS PAR IAM SONT LES SUIVANTS :

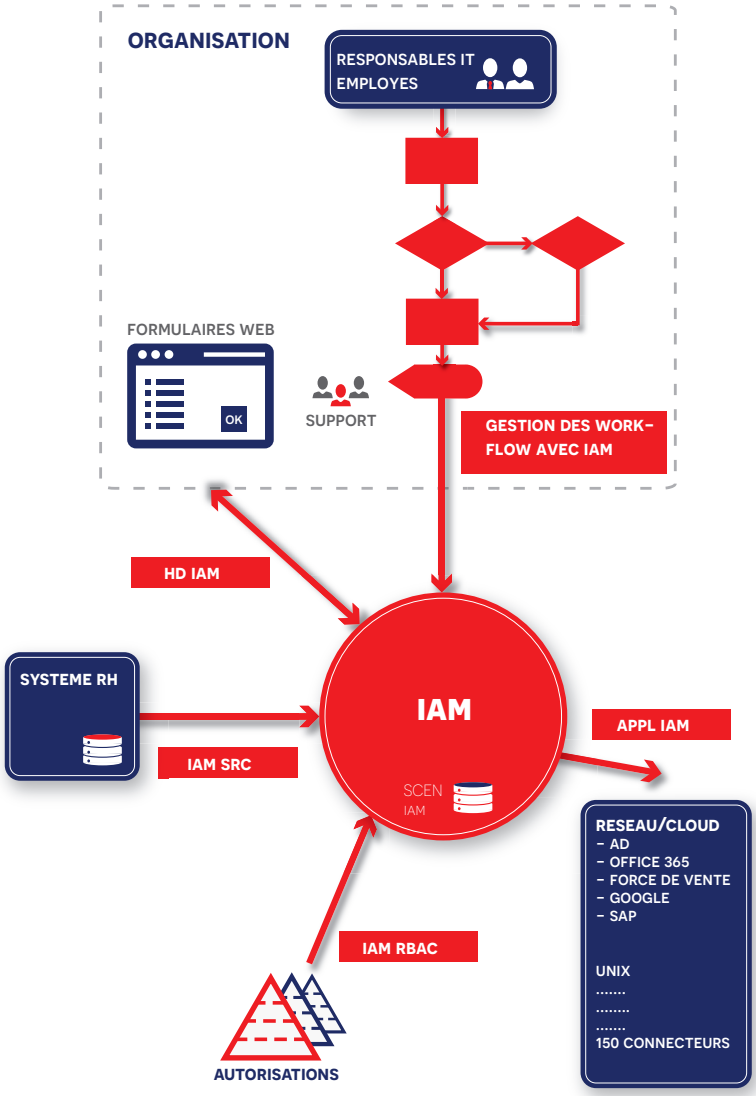
LE PROVISIONING IAM-PROV

Grâce à ce module de Provisioning, toutes les tâches d'administration (semi-)manuelles des utilisateurs sont enregistrées au sein de scénarios électroniques dans IAM. Des scénarios informatisés déterminent en détail la façon dont les comptes utilisateurs doivent être gérés au sein des différentes applications et systèmes. Par exemple, IAM possède des scenarios pour les cas de figure suivants : pour l'arrivée d'une nouvelle ressource, lorsqu'un employé change de service, obtient une promotion ou lorsqu'il quitte l'entreprise. Pour couvrir l'ensemble des changements inhérents aux cycles de vie d'un utilisateur, une moyenne de vingt scénarios est nécessaire pour une implémentation normale.
Ces dix dernières années, Tools4ever a mené à bien plusieurs centaines de déploiement, ce qui lui a permis de constituer au fil des ans, une base de données exhaustive des scénarios possibles, de sorte que quasiment n'importe lequel cas de figure touchant à la gestion des comptes d'utilisateurs peut être appréhendé directement et sans délai.

Les blocs constitutifs sur la base desquels les différents scenarios sont élaborés sont un élément standard de IAM et font partie intégrante du produit. Dans l'éventualité où de nouvelles applications viendraient à apparaître, comme ce fut le cas par exemple avec l'apparition des applications Cloud, ou si des applications existantes venaient à être changées, une nouvelle version des actions destinées aux bases de données serait alors éditée.

PROVISIONING EN AVAL IAM-APPL

Le module de provisioning en aval d'IAM édité par Tools4ever permet de fournir une connexion vers plus de 150 systèmes. La solution utilise un connecteur pour stocker et gérer l'ensemble des comptes utilisateurs et les droits d'accès associés dans un système cible. IAM peut se connecter à un large éventail de systèmes et d'applications, y compris aux applications du Cloud, aux applications sur site standards, aux applications virtuelles, aux emails, aux bases de données, aux systèmes d'exploitation et aux répertoires.



TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

HELPDESK DELEGATION IAM-HD

Grâce au module Helpdesk Delegation, la gestion des comptes utilisateurs peut être facilement déléguée à du personnel autre que purement informatique (personnel de bureau, personnel RH, secrétaires, coordinateurs techniques spécialisés, etc). Le dispositif de Helpdesk Delegation est un ensemble de formulaires électroniques reliés au service central de IAM. Dans ces formulaires, le membre du personnel mandaté peut saisir les données relatives à la demande de gestion de l'utilisateur (ex : prénom, nom, titre, poste et service pour créer un nouveau compte d'utilisateur), puis il clique sur OK pour terminer l'opération.

Ainsi, le service IAM met en œuvre les changements au sein du réseau conformément au scénario éligible (IAM-PROV). L'employé mandaté n'a besoin d'aucun droit d'administration particulier, sachant que le processus de mise en place des changements est strictement identique à chaque fois. Chaque changement est également consigné, pour qu'il soit possible par la suite, notamment en cas d'audit, d'identifier l'employé ayant initié cette demande, la date et enfin l'heure de cette demande.

CONNEXION AVEC LE SYSTÈME RH IAM-SRC

Le système RH constitue une très bonne source d'informations pour gérer les comptes utilisateurs. Grâce au module IAM-SRC, Tools4ever peut obtenir des connexions avec les systèmes RH disponibles. Le module IAM-SRC récupère des informations issues du système RH sur les membres du personnel (identité complète), sur leur contrat de travail (poste, service, missions), ainsi que sur leur hiérarchie (savoir qui est le responsable de tel ou tel employé). Tout changement enregistré dans le système RH est relié aux scénarios indexés.

Le module IAM-SRC est capable de détecter un changement immédiatement et est en mesure de l'appréhender comme une connexion directe entre le système RH et l'Active Directory, et ce n'est là qu'un exemple parmi tant d'autres. Il est également possible de synchroniser les annuaires via un outil Identity Vault (base de données). Un dispositif d'ID Vault est déployé lorsqu'il n'existe pas de système RH capable de tenir lieu de système d'enregistrement source, c'est notamment le cas lorsque l'information source est répartie au sein de différents systèmes RH, des systèmes flexipool, des enregistrements externes, etc.

GESTION DES WORKFLOW ET SELF-SERVICE IAM-WFM

Le module IAM-WFM est un niveau de délégation externe d'IAM-HD. Grâce au module IAM-WFM, les responsables et les employés peuvent demander, approuver et mettre en place directement des changements concernant les comptes utilisateurs, sans intervention du département informatique. Le module IAM-WFM propose une interface facile à utiliser, affichant ainsi uniquement les icônes (formulaires) que les employés habilités peuvent activer. La plupart des actions sont répercutées immédiatement dans le réseau, mais les actions nécessitant des approbations spéciales sont d'abord acheminées vers les responsables mandatés. Pour permettre le traitement adéquat de ces demandes, les responsables reçoivent aune notification mail automatique des tâches en attente.

GOUVERNANCE DES ACCÈS IAM-RBAC

Le module IAM-RBAC régule les droits d'accès d'un employé sur le réseau, en se basant sur une matrice d'autorisation. Par ailleurs, en fonction du rôle d'un employé, la matrice détermine les ressources auxquelles un ou une employé(e) peut avoir accès. Il peut s'agir : de la capacité à effectuer certaines transactions, de l'accès à un système (partiel) ou d'un certain type de téléphone mobile, ainsi que de l'accès à certaines zones physiques.

La gestion de la matrice peut être déléguée à un responsable de la sécurité, à l'administration informatique ou à un agent gestionnaire de services.

Le module IAM-RBAC s'assure également que l'accès aux ressources est correct. Il peut également fournir un support au niveau de la configuration initiale de la matrice d'autorisation.