Livre blanc

LA BONNE GOUVERNANCE EN GIA ... RBAC ET PLUS ENCORE

Version 2014-10

Date de publication : Octobre 2014

Auteur : Guy Paris

SUJET

Les organisations tentent successivement d'implémenter le modèle Role-Based Access Control (RBAC) pour faciliter leur gestion des identités et des accès. Le succès de ces initiatives est généralement mitigé et le retour sur investissement reste marginal. Au final, la pérennité de cette approche est assurée seulement pour quelques secteurs ; ceux à haut taux de roulement et dont la mission est très stable.

Ce livre blanc expose d'abord les principaux écueils rencontrés par les professionnels qui tentent d'implémenter RBAC. Ensuite, il propose un concept qui supporte RBAC mais qui n'est pas limité à celui-ci. En effet, le concept proposé supporte efficacement plusieurs autres contextes d'utilisation et complémente ainsi la couverture de RBAC à proprement dit. Enfin, ce document propose une approche de gouvernance simple mais rigoureuse et sans compromis sur la sécurité. Cette approche favorise l'évolution de la **G**estion des identités et des accès (GIA) au rythme souhaité par les organisations.

AUDITOIRE CIBLE

Ce livre blanc s'adresse à un public désireux d'améliorer la GIA dans son organisation. L'auteur présume que le lecteur possède déjà des connaissances de base de la GIA. De même, une connaissance générale de la gouvernance en GIA et de RBAC est recommandée mais non essentielle.

REMERCIEMENTS

Ces idées et ce document n'auraient pu voir le jour sans la contribution de plusieurs collègues et amis. Sans tous les nommer, je tiens néanmoins à leur témoigner ma reconnaissance et mon amitié. Ce sont tous ces débats intellectuels qui ont permis de consolider ces idées et de confirmer leurs valeurs.

INTRODUCTION

Le Role-Based Access Control (RBAC) est un modèle de contrôle d'accès à un système d'information. Le principe de base est simple : chaque décision d'accès est basée sur le rôle de l'utilisateur. Beaucoup d'organisations ont investi des sommes importantes et des efforts imposants pour « implémenter RBAC ». Ainsi, on définit de nouveaux processus, de nouveaux rôles et des nouvelles responsabilités. On acquiert de nouveaux outils : un outil pour aider à la conception des rôles, un outil pour faire le provisionnement des rôles, etc. On effectue des analyses méticuleuses des accès pour déceler des assemblages constituant des rôles. On ajuste et confirme ces rôles avec les lignes d'affaires, on les codifie et on les documente dans l'outil retenu. On les teste et on les met en production pour finalement réaliser qu'ils sont déjà obsolètes, et ce, malgré tous les efforts et le bon travail. Dès leur mise en production, la constitution des rôles ne colle plus parfaitement avec les besoins il faut donc les réviser.

Force est de constater que les approches d'implémentation retenues sont à la base même du problème puisqu'elles ne permettent pas d'évoluer à la vitesse requise. La GIA est un écosystème en mouvance continue. Malheureusement, ces implémentations sont tellement sclérosées à la base qu'elles ne peuvent soutenir le rythme d'évolution de cet écosystème. Disons le simplement, ces « assemblages d'accès » qu'on a mis tant d'efforts à créer sont difficiles à faire vivre. Devant ce constat et pour pouvoir ajouter un peu d'agilité à notre GIA, on va même jusqu'à accepter des passe-droits à la bonne gouvernance des accès.

C'est d'ailleurs là que devrait reposer le principal malaise des spécialistes en GIA. Ces implémentations introduisent des failles dans la gestion des identités et des accès. Parfois, on va même jusqu'à présenter ces lacunes comme « le prix à payer ». La question de fonds revient donc à savoir s'il est possible et comment obtenir les bénéfices liés à l'utilisation de ces concepts tout en respectant les besoins d'agilité d'une organisation; et ce, sans fragiliser la bonne gouvernance des accès.

LES CONCEPTS…

Qu'on les appelle "Rôles" ou "Profils" ou quoi que ce soit d'autre, on les aborde généralement sous l'angle qu'ils sont des assemblages d'accès. Pour les décrire, on retrouvera des définitions qui ressemblent généralement à « Assemblage ou regroupement structuré de tâches ou de privilèges d'accès reflétant les besoins d'accès partagés par un ensemble d'utilisateurs ». On observe aisément que la définition même de ces "assemblages" est plutôt de nature mixte. Qu'est-ce que c'est finalement? De l'organisation du travail? Un regroupement d'accès? Parfois l'un, parfois l'autre ? Un heureux mélange de tout ça? Comment peut-on espérer que l'évolution d'une telle chose soit simple? La nature même de la bête n'est pas claire. On établira néanmoins des règles de gouvernance et des processus de gestion des rôles qui s'inspirent fortement de la gestion des accès.

Prenons un peu de recul et revenons à la base : dans un modèle discrétionnaire, la dynamique entre le gestionnaire responsable de l'identité visée et le détenteur du bien informatique à accéder est gérée très simplement. Dans le cas d'un accès qui serait autorisé, le processus se résume en trois petites étapes : 1- le gestionnaire demande l'accès pour une identité, 2- le détenteur autorise l'accès, 3- l'accès est octroyé à l'identité. On peut souvent percevoir des cas qui semblent différents. Par exemple, on trouvera des cas où l'accès a été « pré autorisé » si certaines conditions sont respectées. Mais, quand on y regarde de plus près, tous ces cas sont des variantes plus ou moins automatisées respectant cette dynamique de base : l'accès est demandé par une personne autorisée à poser cet acte, l'accès est autorisé par une personne autorisée à poser cet acte, et finalement l'accès est octroyé. Dans l'exemple précédent, une pré autorisation demeure tout de même une autorisation du détenteur.

Pour illustrer cette dynamique, j'utilise souvent l'analogie de l'établissement d'un contrat. Le gestionnaire et le détenteur sont les deux parties en cause et la personne qui octroie l'accès est le notaire (le tiers de confiance qui matérialise l'entente entre les deux parties).

Examinons maintenant le rôle au sens RBAC; et surtout la nature même de celui-ci.

Quand on présente le rôle au sens usuel RBAC, on le définit d'abord sous l'angle de l'organisation du travail. Le rôle apparaît donc comme un ensemble d'identités qui font un certain travail; qui accomplissent une certaine tâche. Avec une telle définition, on se retrouve face à un concept dont la nature est claire et qui est facilement gérable. Les rôles sont des regroupements d'identités. Donc, ils relèvent et sont sous le contrôle d'une unité administrative (comme les identités). Dès lors, le gestionnaire (celui à qui on a confié cette unité administrative) jouit de toute la légitimité requise pour définir ses rôles ; et surtout pour gérer les affectations à ces regroupements d'identités dont il est responsable. L'affectation de personnel à des tâches tombe parfaitement dans le champ d'intervention normale du gestionnaire.

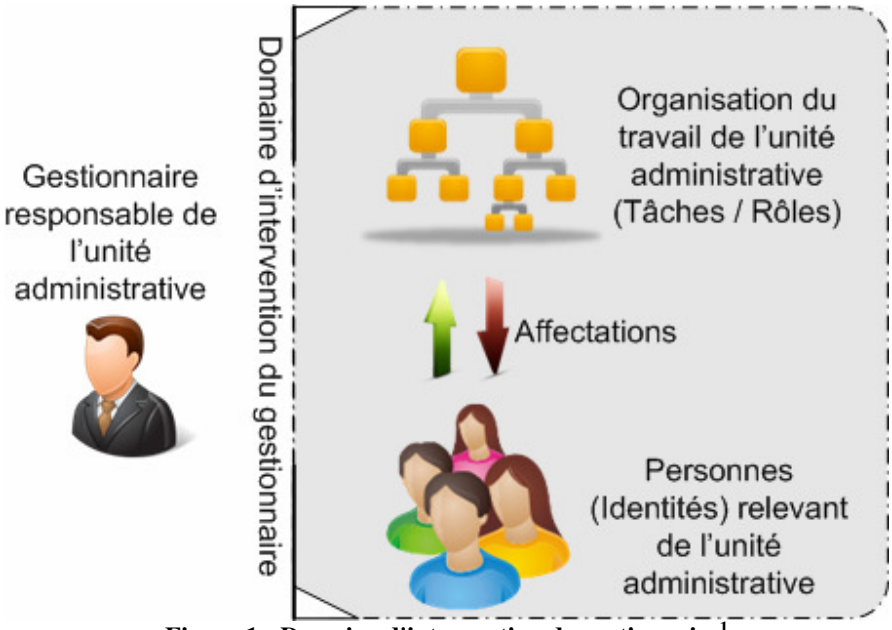

Figure 1 - Domaine d'intervention du gestionnaire[1]

[1] Certains icônes utilisés dans les diagrammes de ce document sont libres de droits mais un lien vers le site de l'auteur est requis. Merci donc aux designers suivants : http://www.dezinerfolio.com/ , http://www.icons-land.com/ .

« C'est bien mais je n'ai toujours pas octroyé d'accès ! Le problème reste entier ! ». Qu'à cela ne tienne ! Un regroupement d'identités a besoin d'un accès? Pas de problème! Comme il s'agit là d'un rassemblement d'objets de même nature (i.e. : des identités), je peux appliquer le même processus simple que celui utilisé pour une seule identité : 1- le gestionnaire demande l'accès pour le regroupement d'identités, 2- le détenteur autorise l'accès, 3- l'accès est octroyé au regroupement d'identités. Dans le processus « standard », seule la cible a changé !

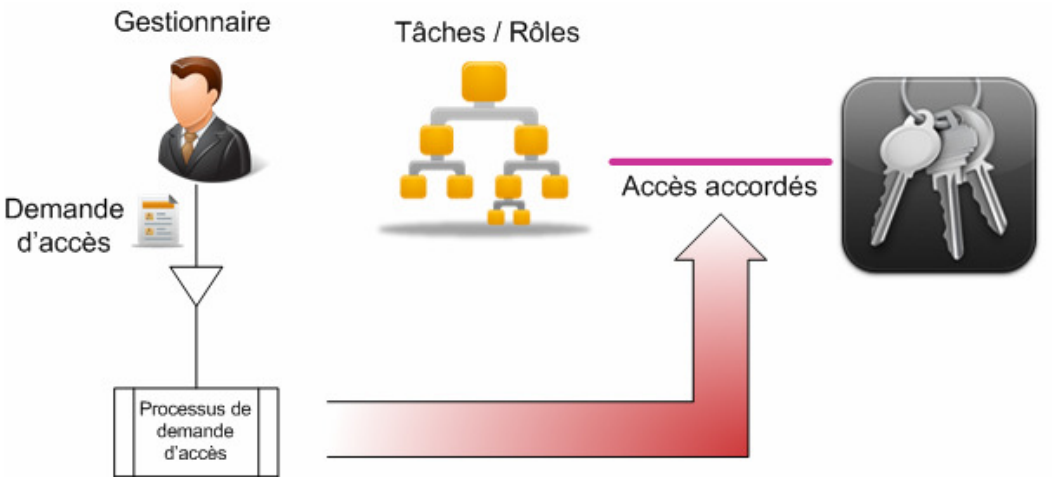

Figure 2 - Demande d'accès visant une tâche/un rôle

À partir de ce point, et c'est là que toute la magie doit opérer. L'effet sur les accès est pris en compte automatiquement au fil des affectations de personnel qui vise ce regroupement d'identités. L'avantage c'est que le gestionnaire est autonome dans la définition de ses rôles et dans ses affectations, ce qui est tout à fait légitime. Il est responsable de ses identités, de son organisation du travail, et de l'affectation des tâches à ses employés. Cette dernière n'est pas un acte d'octroi d'accès, mais bien une affectation de personnel à des tâches.

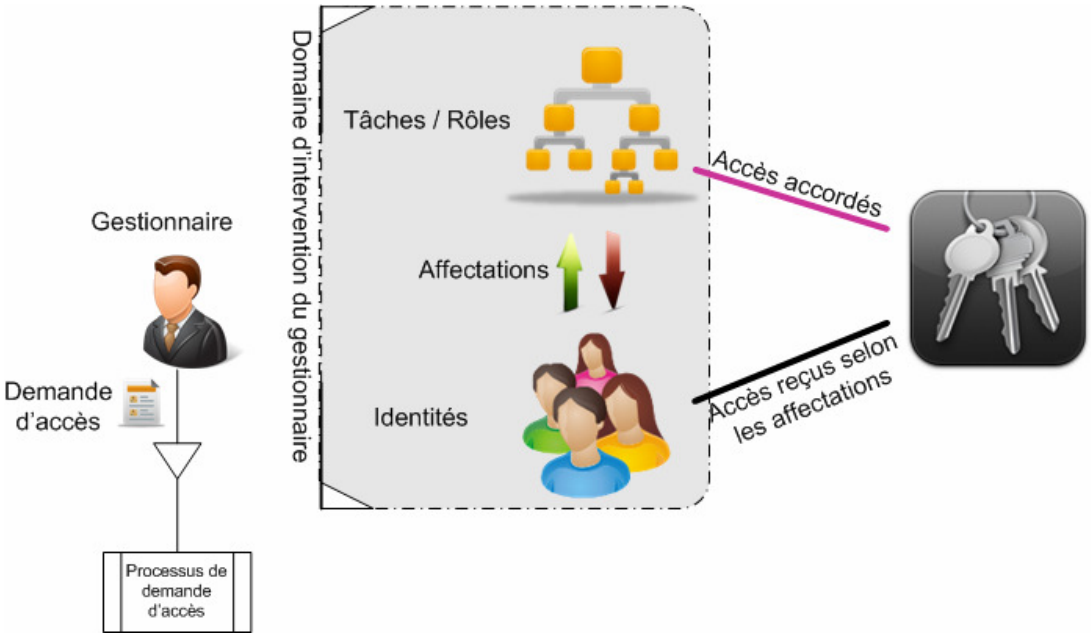

Figure 3 - Accès des identités suite à une affectation à un rôle

Dans mes conférences, c'est à ce moment précis que j'observe un phénomène très intéressant chez les participants. L'auditoire se divise habituellement en 2 camps. Il y a ceux qui acceptent d'emblée cette vision comme répondant parfaitement aux besoins. Et il y a ceux, voyant les paradigmes appris tombés, qui se disent qu'il y a sûrement une erreur; que c'est trop simple pour fonctionner. Le débat qui suit est toujours passionnant et, trois fois sur quatre, à la fin c'est le premier groupe qui défend directement la vision simple auprès du deuxième groupe; sans que j'intervienne. Ensuite, je leur explique jusqu'où cette idée simple peut bien répondre à d'autres besoins.

Revenons maintenant à RBAC.

L'objectif de RBAC se résume généralement comme suit : « chaque décision d'accès est basée sur le rôle de l'utilisateur ». Dans le modèle que je propose, cette décision d'accès (au sens humain du terme) a été appliquée par le détenteur (Figure 2 - Demande d'accès visant une tâche/un rôle) au moment d'autoriser ou non l'accès à ce regroupement d'identités (ex : à ceux qui font la tâche X). Ici, le principe est parfaitement respecté. Le détenteur a exercé son pouvoir discrétionnaire au moment opportun et il a appuyé sa décision sur des bases solides : « Est-il légitime que les personnes qui font cette tâche aient accès à mon bien informatique ? ».

Si on observe maintenant l'angle technologique de la décision d'accès, le contrôle d'accès est basé sur l'appartenance à un groupe d'accès qui a été octroyé à cause de l'appartenance au regroupement d'identités (Figure 3 - Accès des identités suite à une affectation à un rôle). On constate qu'ici aussi le principe est parfaitement respecté.

En appliquant ce modèle, la gouvernance des accès et la gouvernance des identités sont simples puisque la portée de chaque concept est bien délimitée et le sujet de chaque gouvernance est clairement défini. Ainsi, le gestionnaire gère ses identités et son organisation du travail tandis que le détenteur gère les accès à ses biens informatiques. Chacun est roi dans son royaume. Le processus usuel encadre la zone d'entente entre ces deux acteurs : la frontière entre les deux royaumes.

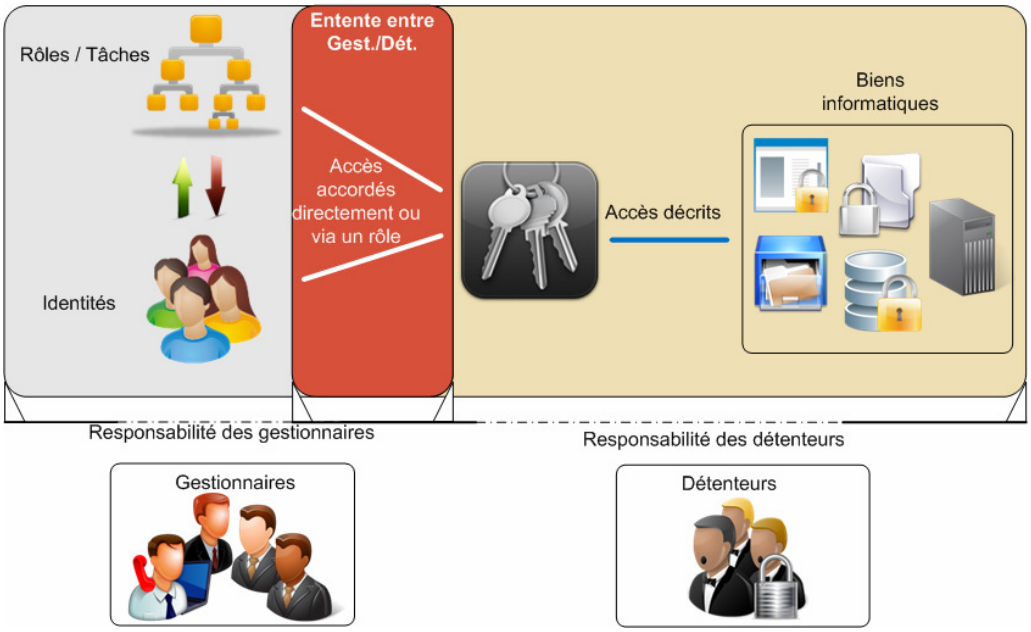

Figure 4 - Gestionnaires et Détenteurs

GÉNÉRALISATION DES CONCEPTS…

L'organisation du travail n'est toutefois qu'une forme de regroupements d'identités parmi tant d'autres. Dans nos organisations, on retrouve ces regroupements d'identités sous beaucoup d'autres formes. Certaines cadrent assez bien avec « l'organisation du travail » (ex : structures de projet, comités). En revanche, d'autres ne collent pas bien (voire même : pas du tout) avec une logique de « tâches ».

Un exemple qui cadre mal serait un regroupement basé sur la localisation géographique. Combien de fois ais-je entendu un gestionnaire dire « Je ne gère pas mon équipe de Montréal de la même façon que mon équipe de Québec… D'ailleurs, ils n'ont pas tout à fait les mêmes besoins au niveau des accès! »? Que faire aussi des premiers répondants en cas d'urgence, des secouristes, du club social, etc. Autant d'assemblage d'identités qui ont des besoins d'accès mais qui ne collent pas très bien avec une logique de travail.

En y regardant attentivement, on constate que la structure administrative n'est pas non plus un regroupement lié à l'organisation du travail. Il suffit d'observer une réorganisation administrative pour s'en convaincre. Rares sont les réorganisations administratives qui résultent en l'élimination d'une tâche ou d'une mission. Un déplacement de ceux-ci : oui leur élimination : rarement ! D'un autre côté, les accès pour des besoins administratifs (ex : saisie des feuilles de temps, accès à l'intranet du secteur) collent bien avec la structure administrative.

Comment faire pour supporter tous ces types de regroupements d'identités? La réponse est encore aussi simple : de la même façon!

> *Dans mes conférences, c'est ici que l'auditoire réalise l'énorme potentiel de l'usage des structures d'identités.*

On peut appliquer la même logique à autant de formes de regroupements d'identités qu'il y a de façons d'organiser celles-ci. C'est ce concept générique que l'on peut appeler « Structures d'identités ».

D'emblée, on reconnaît l'utilité d'une structure d'identités pour refléter la structure administrative. Ainsi, l'octroi des accès pour des besoins administratifs (exemple : la saisie du temps) se fera sans problème via l'appartenance à la structure d'identités reflétant la structure administrative.

On pourra tout aussi bien créer une structure d'identités correspondant à la localisation géographique des identités. On pourrait aussi imaginer une structure d'identités reflétant à la fois une logique liée à la tâche et une logique de localisation géographique. La seule limite quant aux formes que peuvent prendre ces structures est votre imagination. Observez autour et vous trouverez aisément des exemples aussi variés les uns que les autres.

Imaginons de plus qu'une structure d'identités offre la capacité de propager, si désiré, un accès à toutes les identités des structures subordonnées à la structure ayant reçu cet accès. Dès lors, au moment de faire la demande d'accès vers une structure d'identités, le gestionnaire pourrait spécifier que l'accès sera octroyé à toutes les identités affectées à la structure d'identités ou à l'une de ses structures subordonnées.

Pour illustrer ce propos, la figure suivante présente ce que pourrait être une structure d'identités qui supporterait une réalité mixte tâche/localisation physique et exploitant aussi la notion de propagation des accès aux identités des structures subordonnées.

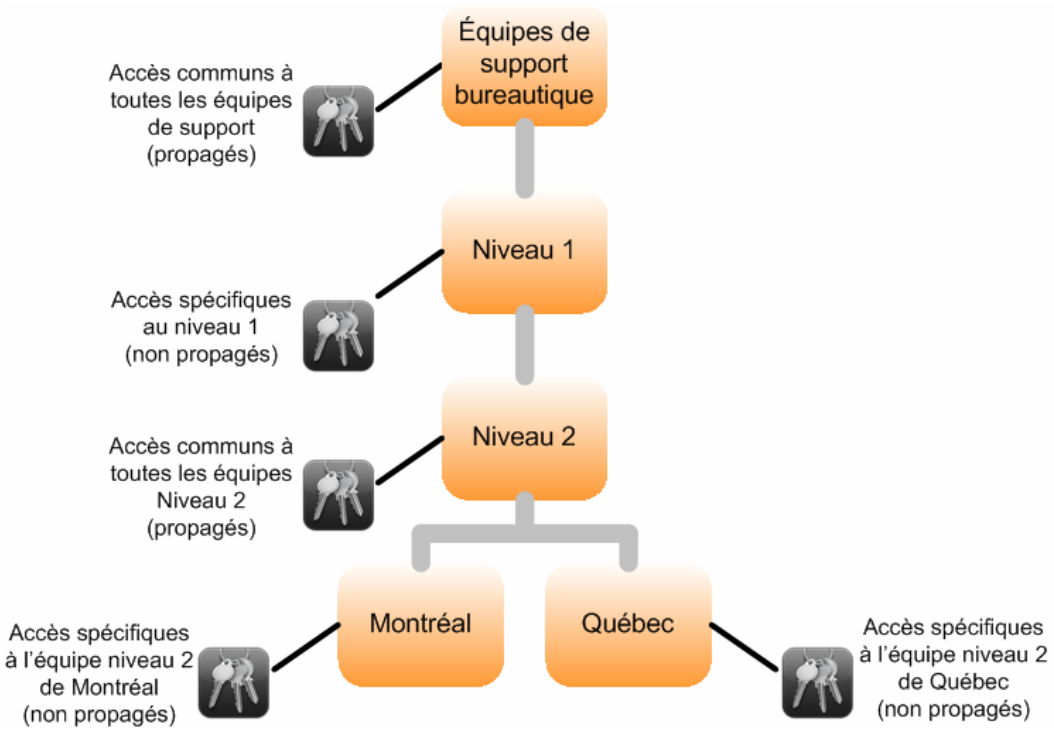

Figure 5 - Structure d'identités mixte avec propagation des accès

On peut aussi imaginer à quoi pourrait ressembler l'utilisation d'une structure d'identités reflétant la « Structure administrative » :

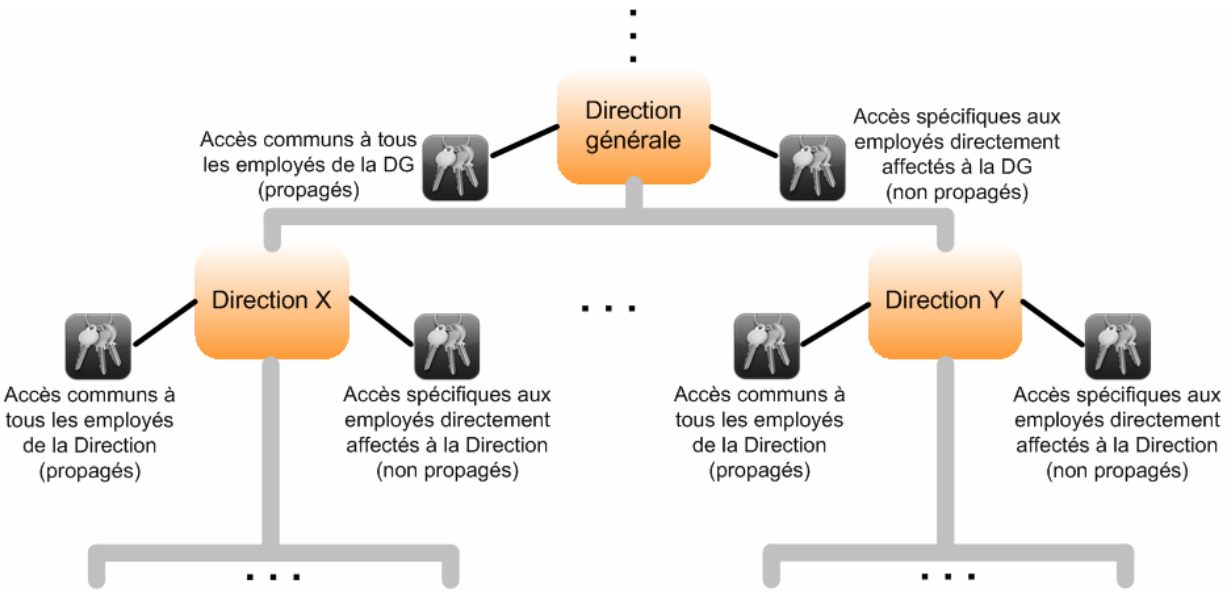

Figure 6 - Utilisation de la Structure d'identités reflétant la structure administrative

REGARDONS LES ACCÈS

Quand on adopte cette vision, on découvre un avantage supplémentaire. Les accès sont beaucoup plus simples à documenter, et à gérer par le fait même. De fait, la documentation d'un accès pourra dorénavant se résumer à décrire « Accès à quoi et comment! ». En effet, toutes les informations contextuelles qu'on retrouve régulièrement (ex : « accès pour telle clientèle ») n'ont plus d'utilité. Ici encore, on peut se concentrer sur la nature spécifique de l'objet considéré; à son rôle dans l'écosystème de GIA. Ses relations avec les autres objets sont inutiles pour le décrire.

De plus, quand on voudra connaître tous ceux qui ont un accès donné, le résultat sera beaucoup plus facile à interpréter puisqu'il sera possible de grouper des masses d'identités sous des étiquettes plus éloquentes : les structures d'identités par lesquelles elles ont reçu cet accès.

Accès aux biens informatiques "Serveurs d'installation logiciel"

octobre 24, 2014

	Nbr d'identités	Lecture	Écriture
Répertoires des logiciels corporatifs			
Groupe d'accès "Repertoire-Log-Corpo-tous-Lect"		X	
Équipes de support Niveau 2	42		
Jean Gabin	1		
Rock Voisine	1		
Groupe d'accès "Repertoire-Log-Corpo-tous-Maj"			X
Équipe de normalisation des applications	4		
Équipe de mise en production des applications	6		
Administrateurs des serveurs de fichiers	4		
Patrick Bruel	1		
Céline Dion	1		
Véronique Dicaire	1		
Nbre d'utilisateurs par type d'accès		**44**	**17**
Répertoires des logiciels libres			
Groupe d'accès "Repertoire-Log-libres-tous-Lect"		X	

Figure 7 - Illustration d'un rapport d'accès incluant des structures d'identités

QUESTIONS ET RÉPONSES

Faut-il arrêter de concevoir des profils et des rôles?
Pour bien répondre à cette question, il faut d'abord savoir qui la pose ?

Si c'est le gestionnaire qui pose la question, je lui rappellerai qu'une bonne organisation du travail dans son secteur est une preuve de saine gestion. Dans la mesure où cette organisation du travail existe déjà, les profils (ou rôles) de son secteur sont connus et la construction des structures d'identités ne sera qu'un jeu de traduction de cette organisation du travail. Restera, au moment utile, à faire les demandes d'accès applicables pour tirer profit de ces structures. Sur ce dernier point, la suggestion est d'attendre l'arrivée d'une nouvelle identité à affecter à la structure pour faire les demandes d'accès. Il suffira de faire les mêmes demandes qu'on aurait faits pour l'identité affectée mais on visera la structure d'identités comme bénéficiaire de l'accès (i.e. : on vise la structure d'identités au lieu de la nouvelle identité). Et voilà, le tour est joué. Les demandes d'accès pour que l'identité soit fonctionnelle devaient être faites de toute façon. En choisissant ce moment pour faire les demandes, aucun effort supplémentaire n'est requis.

Si c'est une personne mandatée pour implémenter RBAC, je répondrai sans hésiter qu'il faut arrêter de concevoir des profils et des rôles. Tel que mentionné au point précédent, l'organisation du travail relève directement du gestionnaire et cette organisation du travail est déjà implémentée dans son secteur. Votre travail devrait plutôt être orienté afin d'offrir un service d'accompagnement pour aider les gestionnaires qui désire utiliser ces concepts et traduire leur organisation du travail en structure d'identités. Offrir ce service permettra aux gestionnaires de frapper à votre porte pour avoir l'aide requise pour traduire en structures d'identités leur façon de gérer leurs identités. Le bon usage des structures d'identités offrira à l'organisation une grande pérennité aux résultats des efforts investis puisqu'ils seront investis dans les secteurs où cela est utile ; ceux-là même qui le demandent. Et surtout, n'oubliez pas de considérer les structures d'identités qui ne sont pas liées à l'organisation du travail. Le retour sur investissement pour le gestionnaire est parfois très bon pour celle-ci. Par expérience, un atelier dirigé d'une durée d'environ une (1) heure suffit généralement pour offrir à un gestionnaire les structures d'identités de base qui reflètent sa façon d'organiser ses identités. Un gestionnaire qui maîtrise son secteur s'est doté d'une organisation de son personnel. Il faut simplement la comprendre et la transcrire. Il n'est même pas nécessaire que cette première version de son secteur soit parfaite. Il est autonome dans l'évolution de ses structures d'identités. Il pourra donc la faire évoluer à sa guise. Face à un gestionnaire, concentrons nous donc sur l'idée d'offrir une vision réaliste et surtout une vision utile de sa réalité. L'utilisation provoquera naturellement les ajustements requis. Les structures inutiles seront abandonnées alors que les structures utiles évolueront au rythme requis, des structures à utilisation ponctuelle (ex : projet) apparaîtront et disparaîtront selon les besoins de l'organisation, etc. C'est ici que le dynamisme de ce modèle prend toute son importance.

Comment faire pour concevoir toutes les structures d'identités d'une organisation ?
On ne le fait pas!!! Pour qu'une organisation tire la pleine valeur de ces outils et concepts, il est important qu'elle les utilise là où c'est réellement utile. Si les gestionnaires comprennent le concept, les gestionnaires pour qui ce sera utile,auront vite fait de cogner à votre porte pour l'utiliser dans leur secteur. L'implémentation de ce concept dans une organisation passera donc par un bon service d'accompagnement (guide, formation, support direct, etc.), une bonne visibilité (on ne peut espérer que quelqu'un utilise quelque chose dont il ignore l'existence) et une bonne publicité. Pour cette dernière, on pourrait tabler sur les secteurs très opérationnels, surtout ceux ayant un fort roulement de personnel. On créera ainsi des pôles d'évangélisation à partir desquels la bonne nouvelle se répandra naturellement. Ces secteurs deviendront aussi des exemples que l'on citera aussi souvent que nécessaire pour démontrer le bon usage de ces concepts. Je suggère aussi de mettre des « automatismes administratifs » pour créer systématiquement certaines structures d'identités. Par exemple, le lancement d'un projet s'accompagnerait de la création systématique d'une structure d'identités équivalente. Le même

automatisme pourrait apparaître à la création d'un comité ou d'un groupe d'intérêt. Une valeur ajoutée évidente pour tous les gestionnaires sera la capacité de lier une liste de distribution de courriels à une structure d'identités. À elle seule, cette fonctionnalité suffira parfois à faire adhérer des gestionnaires.

Comment les gestionnaires peuvent-ils éviter d'être submergés par les tâches de GIA ?
Cette question est à la fois simple et délicate. Elle met le doigt sur le principal facteur derrière bon nombre de compromis à la bonne gouvernance de la GIA. En effet, particulièrement dans les grandes organisations, les tâches entourant les demandes d'accès (demander les accès, autoriser les accès, etc.) auraient tôt fait de monopoliser une partie significative d'une semaine de travail d'un gestionnaire ou d'un détenteur. Sans compter que ces acteurs n'ont pas nécessairement toutes les habilités requises pour maîtriser les objets concernés. Qu'on pense simplement au détenteur du parc informatique : être détenteur du parc ne fait pas de lui un spécialiste de tous les composants technologiques présents dans celui-ci. Cette préoccupation est donc bien réelle et répondre exhaustivement pourrait faire l'objet d'un livre blanc séparé (qui viendra peut-être dans un avenir prochain). Pour ce document, je vais tout de même tenter de répondre succinctement. Pour cela, il faudra aborder le tout selon deux axes distincts et complémentaires.

Premièrement, tant les détenteurs que les gestionnaires doivent avoir la capacité d'utiliser les personnes de leur entourage pour les assister dans ces tâches. En résumé, ils doivent être à même de déléguer leurs pouvoirs en matière de GIA. Par exemple, un détenteur pourra déléguer son pouvoir d'autorisation d'un accès au chef d'équipe administrant la ressource informatique visée. Aussi, un gestionnaire pourra déléguer son pouvoir d'affectation à une structure d'identités de type « projet » au chef du projet en question. De même, certains pouvoirs de gestion des identités d'un secteur pourraient être délégués à l'adjoint administratif de ce secteur. La délégation des pouvoirs est essentielle à une saine gestion des identités et des accès d'une organisation. Évidemment, ces délégations doivent être formelles et documentées. On se rappellera également que le pouvoir de déléguer ne peut être délégué (i.e. un pouvoir reçu par délégation ne peut être délégué à quelqu'un d'autre par le délégué).

Deuxièmement, on aura probablement remarqué l'utilisation de l'expression « délégation de pouvoir » et non « délégation de responsabilité ». La nuance est fondamentale. La responsabilité doit demeurer sur les épaules des gestionnaires et des détenteurs. Pour ceux-ci, les délégations de pouvoir permettent à un tiers de confiance d'agir en leur nom ; mais elles n'affectent en rien leurs responsabilités. Ils demeurent totalement responsables des identités et des accès qu'on leur a confiés. Il est donc primordial que la capacité de déléguer soit accompagnée par un retour vers les gestionnaires et les détenteurs de toutes ces actions qui sont faites en leur nom par les délégués. C'est grâce à ce retour vers les responsables qu'on peut espérer les maintenir en contrôle.

CONCLUSION

De tout temps, les initiatives d'amélioration en GIA ont souffert du faible retour sur investissement et de la complexité des processus résiduels. Les enseignements exposés dans ce document peuvent servir aux organisations pour favoriser une meilleure atteinte des objectifs visés par ces initiatives. Les idées novatrices avancées dans ce livre blanc offre aux organisations une nouvelle perception de l'écosystème de la Gestion des identités et des accès. Une perception simple et rigoureuse sur laquelle l'organisation peut donner une grande pérennité aux résultats de ses investissements.

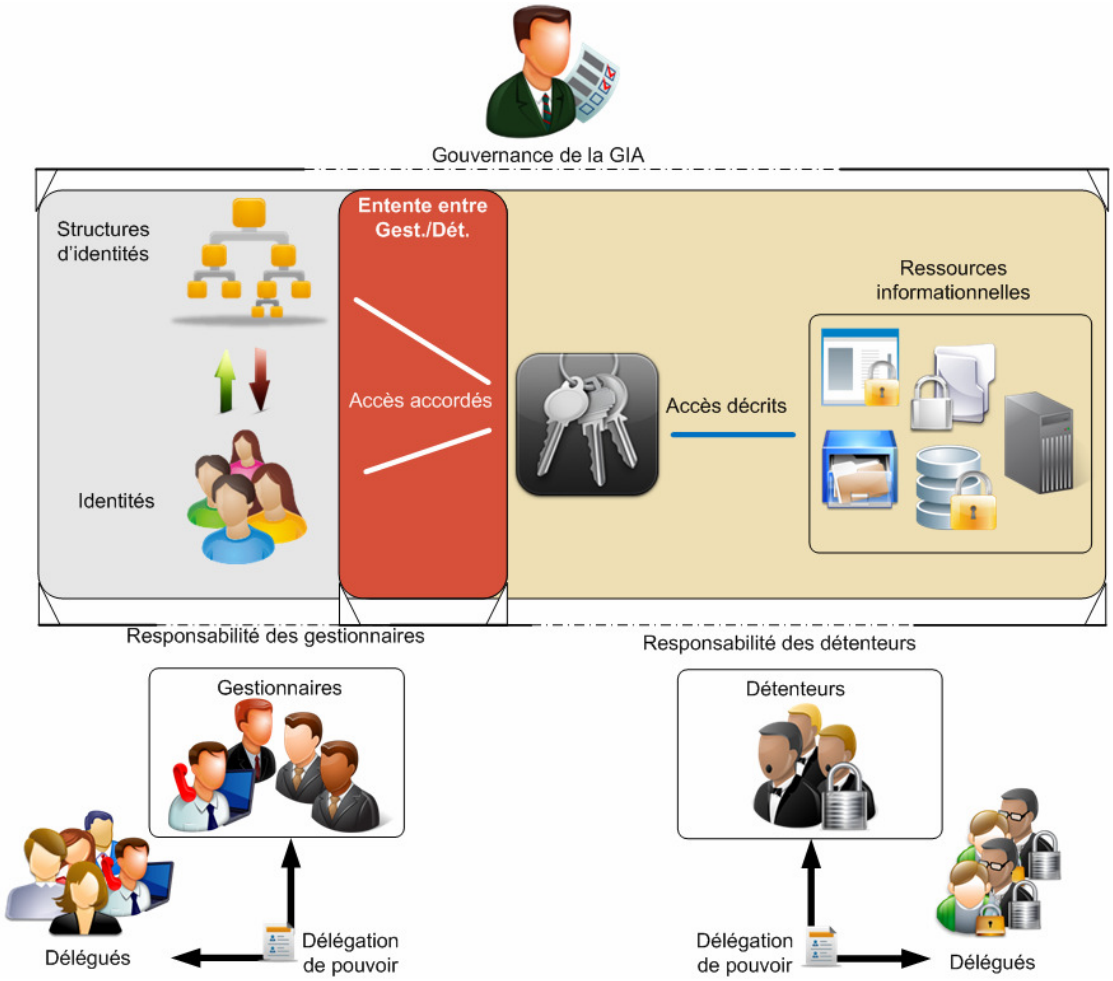

Figure 8 - L'écosystème revu et corrigé de la GIA

Lorsque bien appliqué dans les processus de GIA, cette vision offre un niveau de souplesse inégalée pour permettre à la GIA d'évoluer au même rythme que l'organisation. De plus, cette agilité d'évolution ne se fait pas au prix d'une perte de contrôle puisque ce contrôle demeure entre les mains des personnes responsables du résultat : les gestionnaires et les détenteurs. La gouvernance de la GIA s'en trouve mieux servie et les risques de sécurité des organisations mieux contrôlés.

Responsabilités, souplesse, rigueur et efficience n'auront jamais fait si bon ménage en GIA.

Guy Paris