- *Accès serveur*
- *Agent d'absence*
- *Agent de prédistribution*
- *Agent Web*
- *Débogage*
- *Délais*
- *Pour le compte de*
- *Signature*

10

@Les agents

Objectifs

Ce module décrit les agents du point de vue de l'administration. Les connaissances apportées doivent permettre à l'administrateur de comprendre les instructions de mise en production d'une base et de définir en connaissance de cause les paramètres d'exécution du gestionnaire d'agents et les restrictions de programmabilité.

Connaissances

- Fonctionnement des agents

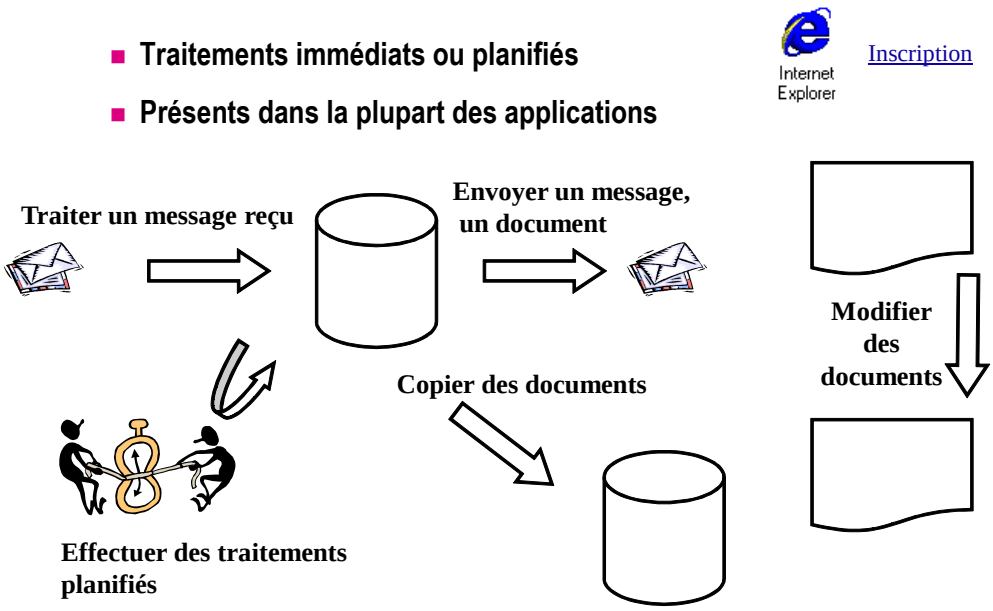
Savoir-faire

- Définir les restrictions de programmabilité
- Définir un serveur d'exécution
- Paramétrer le gestionnaire d'agents

Progression

Rôle des agents
Paramétrage du gestionnaire d'agents
Serveur d'exécution d'un agent
Atelier 1
Modèle de sécurité des agents
Agent accédant à un serveur distant
Agent Web planifié sur serveur
Agent d'absence
Atelier 2
Restrictions de programmabilité
Atelier 3
Débogage distant d'un agent

Rôle des agents



Les agents effectuent des traitements sur un document ou un ensemble de documents. Ils sont une pièce maîtresse des applications de workflow, des applications Web.

Les agents sont exécutés sur l'initiative de l'utilisateur ou non.

– L'utilisateur Notes lance un agent, par exemple en cliquant sur un bouton depuis un document affiché en modification ou non, ou bien dans une vue. L'agent archive des documents, publie le document en cours, envoie un message contenant un lien vers le document en cours aux membres d'une liste de diffusion…
– L'utilisateur d'un navigateur lance un agent en cliquant sur une URL ou sur un bouton. L'agent vérifie les informations saisies sur un formulaire, affiche une page sur le navigateur… L'agent peut aussi activer un autre agent planifié.

Les agents sont aussi des automates, déclenchés par des événements ou planifiés, qui effectuent des traitements variés tels que :

– Examiner les messages déposés par le routeur de messagerie dans une base,
– Envoyer un message – un rappel automatique – à un ou plusieurs utilisateurs en fonction de la date du jour et d'une date butoir dans un document,
– Prévenir les expéditeurs que le destinataire est absent,
– Copier des documents d'une base vers une autre à des fins d'archivage par exemple.

L'administrateur procède à des vérifications au moment de la mise en production d'une application comportant des agents :

– Ressources : le gestionnaire d'agents doit disposer de suffisamment de ressources pour éviter des files d'attente importantes et réduire les délais.
– Réplication : lorsque la base est répliquée sur plusieurs serveurs, les agents sont également répliqués. La plupart ne devront s'exécuter que sur un seul serveur s'ils modifient des documents afin d'éviter les conflits de réplication.
– Signature et droits : les agents sont signés au moment de la mise en production d'une base ce qui leur donne normalement les droits nécessaires pour fonctionner.

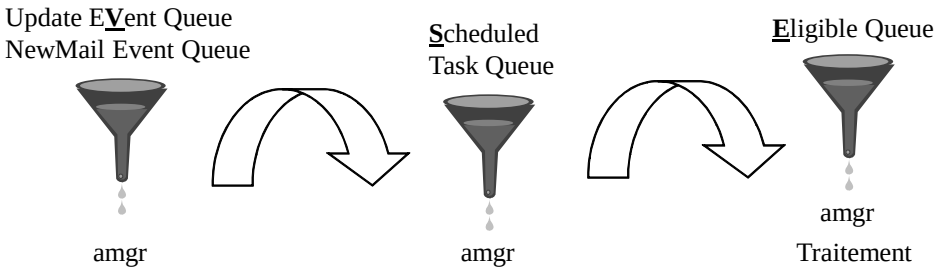
Interview de l'Expert

Imaginons que les cerveaux de Nietzsche et d'Einstein aient été passés au mixeur, nous n'aurions jamais obtenu qu'un ensemble de composés lipidiques et quelques protéines de structure. C'est la preuve qu'un comportement complexe peut émerger d'un ensemble de composants simples et coopératifs. Les agents, autant que possible, ne négligeront jamais les « actions simples » et seront d'autant plus efficaces que chacun d'entre eux sera simple.

Ils sont l'outil idéal de l'administrateur qui souhaite simplifier ses tâches quotidiennes et pallier les rares erreurs qui peuvent subsister dans la documentation, lorsqu'une tâche ne se déroule pas exactement telle que son comportement a été décrit.

Paramétrage du gestionnaire d'agents

- **Trois files d'attente pour les agents planifiés**



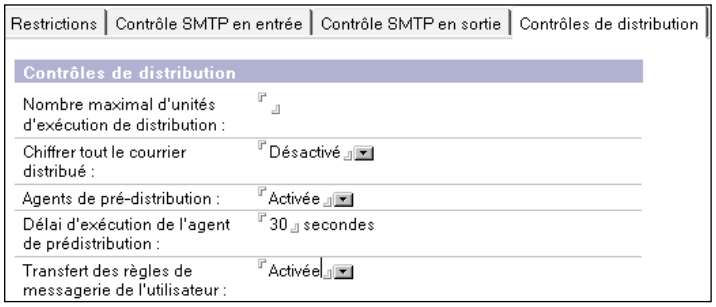
- **Document du serveur : nombre d'agents simultanés**
- **NOTES.INI : délais liés aux files d'attente**
- **Document de configuration du serveur : agents courrier**

Le gestionnaire d'agents prend en charge les agents planifiés sur le serveur. Il gère des files d'attente, le passage de l'une à l'autre se faisant après un délai. Il ne gère pas les agents s'exécutant sur le poste de travail, qui sont lancés par le routeur de messagerie ou depuis le Web.

Agents de prédistribution

Ces agents sont lancés par le routeur au moment où il écrit un document dans une base Courrier en arrivée. L'unité d'exécution de distribution – thread d'exécution – est mobilisée par l'exécution de l'agent. Pour paramétrer ce type d'agent :

- Modifier le document de configuration du serveur
- Cliquer sur l'onglet (Routeur/SMTP), puis sur (Restrictions et contrôles), puis sur (Contrôles de distribution)



– <Agents de prédistribution> : sélectionner *Activée*.
– <Délai d'exécution de l'agent de prédistribution> : laisser 30 secondes ou modifier ce paramètre en accord avec les concepteurs.
– <Nombre maximal d'unités d'exécution de distribution> : taper une valeur entre 1 et 25 pour limiter les unités d'exécution si le serveur est chargé (option).

Agents Web

Ces agents sont lancés par l'utilisateur qui clique le plus souvent sur un lien URL ou bien qui enregistre un formulaire. L'agent est pris en charge par le moteur HTTP de Domino : le gestionnaire d'agents ne le connaît pas.

Agents planifiés

Les agents planifiés sur serveur sont activés par des événements – *Après l'arrivée de nouveaux messages* et *Après la création ou modification de documents* – ou prévus pour une exécution horaire, quotidienne, hebdomadaire ou mensuelle.

Le gestionnaire examine l'ensemble des bases du serveur au démarrage. Il répartit les agents planifiés dans deux files d'attente :

– File V (Update Event Queue et New Mail Event Queue) : les agents activés par un événement.
– File S (Scheduled Task Queue) : les agents horaires, quotidiens, hebdomadaires ou mensuels.

Lorsqu'un agent de la file V est réveillé par un événement, le gestionnaire d'agents le fait passer dans la file S. Lorsqu'un agent de la file S doit être exécuté, il passe dans la file E (Eligible Queue), où il attend une unité d'exécution disponible.
Les délais d'exécution proviennent clairement du passage d'une file d'attente à une autre et du nombre de processus disponibles pour exécuter les agents. Ces paramètres se règlent dans le NOTES.INI du serveur et dans le document du serveur.

Paramètres NOTES.INI

Les valeurs par défaut de ces paramètres doivent être modifiées pour que les agents s'exécutent dans des délais raisonnables. Ils ont été conçus à une époque où les serveurs étaient moins puissants d'une part, et où le gestionnaire d'agents était peu performant d'autre part.

Paramètre	Objet
AMgr_DocUpdateEventDelay	Défaut : 5 minutes. Temps minimum entre la mise à jour ou la création d'un document et l'exécution d'un agent déclenché par cet événement.
AMgr_NewMailEventDelay	Défaut : 1 minute. Temps minimum entre le dépôt d'un document par le routeur de courrier et l'exécution d'un agent déclenché par cet événement.
AMgr_DocUpdateAgentMinInterval	Défaut : 30 minutes. Temps minimum entre deux exécutions successives d'un agent déclenché par l'événement *Après la création ou modification de documents*.
AMgr_NewmailAgentMinInterval	Défaut : 0 minute. Temps minimum entre deux exécutions successives d'un agent déclenché par l'événement *Après l'arrivée de nouveaux messages*.

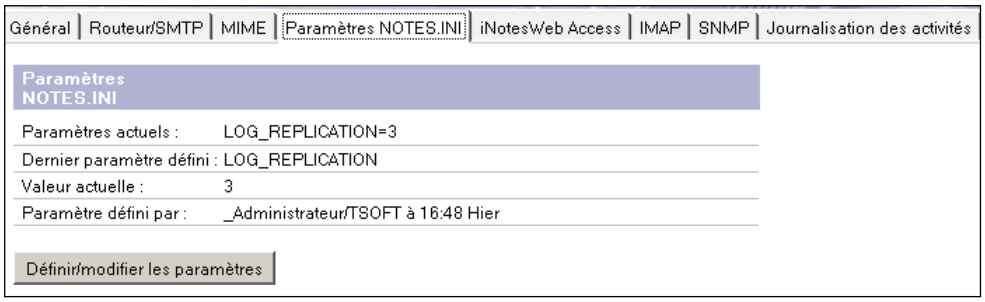
Paramètre	Objet
AMgr_SchedulingInterval	Défaut : 1 minute. Temps entre deux consultations de la file d'attente « Event Queue » par l'agent manager.

Supposons que les valeurs par défaut soient conservées. Un agent réveillé par l'événement *Après la création ou modification de documents* sera activé dans la file d'attente V au bout de cinq minutes (AMgr_DocUpdateEventDelay). Le gestionnaire d'agents examine une file d'attente toutes les minutes (AMgr_SchedulingInterval). L'agent passe donc dans la file d'attente S au bout de 5 à 6 minutes. Il peut s'écouler 1 minute avant qu'il passe dans la file d'attente V où il attendra une unité d'exécution disponible. Au total il s'est écoulé 7 minutes ou plus entre l'événement et l'exécution de l'agent. Si le même agent est réveillé par un deuxième événement, un nouveau délai est ajouté (AMgr_DocUpdateAgentMinInterval) qui fait qu'il s'écoulera 30 minutes supplémentaires.

Les délais supportés par les agents de type *Après l'arrivée de nouveaux messages* sont moins longs mais le délai au final sera de l'ordre de 4 minutes ou plus.

Les paramètres du NOTES.INI du serveur sont écrits de préférence dans le document de configuration du serveur.

- Cliquer sur l'onglet (Configuration), puis sur la vue *Serveur/Configuration*
- Ouvrir le document de configuration du serveur en modification
- Cliquer sur l'onglet (Paramètres NOTES.INI)

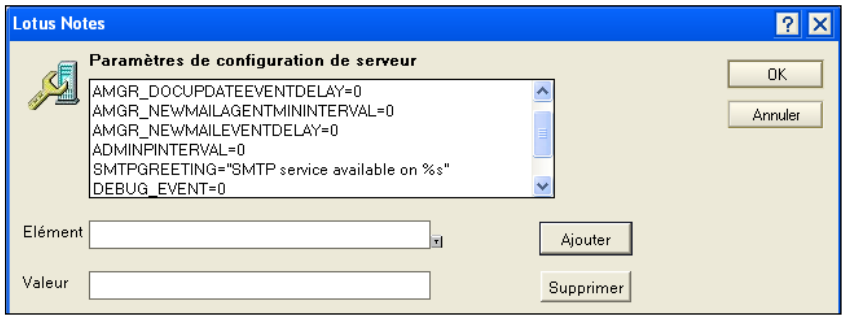


- Cliquer sur (Définir/modifier les paramètres)

- <Elément> : sélectionner *AMGR_DOCUPDATEAGENTMININTERVAL*
- <Valeur> : taper 0 pour supprimer le délai
- Cliquer sur (Ajouter)

Le paramètre apparaît dans l'espace supérieur.

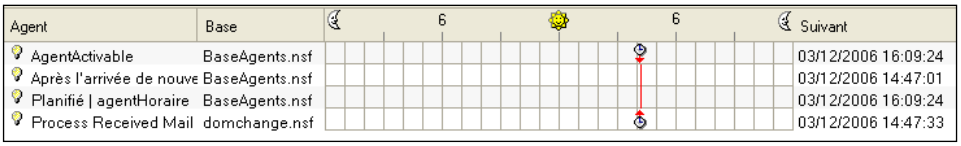
- Répéter l'opération pour les paramètres suivants



- Cliquer sur (OK)
- Cliquer sur (Enregistrer et fermer)
- Redémarrer le serveur Domino pour une prise en compte immédiate

Liste des agents planifiés

- Cliquer sur l'onglet (Serveur), puis sur (Etat), puis *Planifications/Agents*



- Placer le curseur sur un agent : la prochaine planification est indiquée, ou bien la mention *L'agent n'a pas été exécuté*

ou

- Taper la commande `TELL AMGR SCHEDULE` sur la console Domino

Les messages d'anomalie sont envoyés par le gestionnaire d'agents dans le journal du serveur log.nsf.

Document du serveur

Il contient les paramètres pour le gestionnaire d'agents. Les paramètres pour les agents Web correspondent à un mode de compatibilité version 5.

- Cliquer sur l'onglet (Configuration), puis *Serveur*, puis *Document Serveur courant*
- Cliquer sur l'onglet (Tâches serveur), puis sur (Gestionnaire d'agents)
- <Nombre maximal d'agents simultanés> : taper le nombre d'unités d'exécution disponibles pour la file Eligible Queue
- <Nombre maximal d'agents simultanés> : taper un nombre, par exemple *3*
- Cliquer sur l'onglet (Protocoles Internet), puis sur l'onglet (Moteur Web Domino)
- <Exécuter les agents Web simultanément> : sélectionner *Activé*

A partir de la version 6 de Domino, le paramètre se trouve de préférence dans un *site Internet*.

Interview de l'Expert

Les agents ne sont pas circonscrits par la page de paramétrage du document serveur.

Les administrateurs auront tout intérêt à ne pas négliger les variables telles qu'AMGR_DOCUPDATEMININTERVAL, afin de régler des temps entre la survenance d'un événement et le déclenchement de l'agent lui-même, ou entre deux exécutions successives d'un même agent.

Pensez à examiner quotidiennement les statistiques du serveur afin de connaître le nombre d'exécutions d'agents planifiées ainsi que les erreurs d'exécution.

La commande console TELL AMGR SCHED sera également utile avant tout arrêt du serveur afin de déterminer si ce dernier n'est pas sur le point de lancer une exécution.

Lors de la mise en production d'une application Notes, vérifiez également que cette dernière comporte obligatoirement une vue par défaut. L'absence de vue par défaut est susceptible d'entraîner des erreurs d'exécution lorsque les agents doivent effectuer des traitements sur des sous-ensembles de documents.

Serveur d'exécution de l'agent

- **Agent menu Actions ou «Lorsque vous collez des documents»**
  - Sur le client Notes
- **Agent Courrier (avant et après dépôt du message)**
  - Dépend du signataire de l'agent
- **Agent Après la création ou modification de documents ou planifié**
  - Activer l'agent puis sélectionner le serveur
  - Local
  - -Tout serveur-
  - Un serveur

Un agent s'exécute sur le client Notes ou sur serveur. Le choix du serveur d'exécution obéit à des règles dépendant de son type :

– Agent courrier (les deux types) : le serveur de messagerie du signataire,
– Agent lancé manuellement : le client Notes,
– Agent planifié ou réveillé par l'événement *Après la création ou modification de documents* : choix du concepteur ou à la première utilisation.

Si la base est répliquée sur plusieurs serveurs, un agent qui modifie des documents ne peut s'exécuter que sur un seul serveur, faute de quoi des conflits de mise à jour se produiront. Le choix du serveur sera fait au moment de la mise en exploitation.

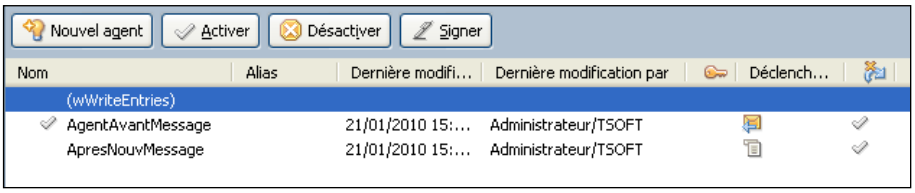
Agent courrier

Le serveur d'exécution de l'agent courrier dépend du serveur de messagerie du signataire, par exemple le serveur de messagerie du « super administrateur » dont l'identifiant sert à signer les bases.

Agents planifiés

L'activation de l'agent détermine le serveur d'exécution la plupart du temps.

- Ouvrir la base dans Designer, puis cliquer *Code partagé/Agents*



- Sélectionner l'agent à activer, puis cliquer sur (Rendre actif)
- <Choisissez le serveur sur lequel exécuter cet agent> : sélectionner un serveur

Interview de l'Expert

La première chose que fera un agent sera de rechercher l'adresse de son serveur d'exécution. Dans le cas où un agent ne s'exécute pas, la première chose à faire est de vérifier que la DNS contient bien le nom (ou l'alias) de ce serveur, afin que son adresse puisse être déterminée.

Modèle de sécurité des agents

- **Modèle version 5 : le signataire de l'agent détermine les droits d'exécution**
  - Sur le serveur : restrictions d'exécution
  - Sur le client Notes : LCE, Liste de Contrôle d'Exécution
- **Modèle version 6 et suivantes : une autorité donne une délégation**
- **Trois scénarios de délégation**
  - Accéder à une base sur un autre serveur depuis un agent
  - Sauvegarder un agent sur serveur sans modifier le signataire
  - Activation d'un agent par un utilisateur ayant l'accès Éditeur

Le modèle de sécurité de la version 5 est actif par défaut : ceci assure une compatibilité ascendante et correspond aussi au cas le plus fréquent de la programmation des agents. Ce modèle de sécurité repose sur la confiance accordée au signataire de l'agent. La version 6 a introduit le concept de délégation dont le principe est le suivant : une autorité de confiance se porte garante du signataire d'un agent, de l'identité d'un utilisateur. Les droits de l'autorité de confiance interviennent de différentes manières selon les scénarios.

Modèle de sécurité version 5

La sécurité s'applique à l'invocation de l'agent et pendant l'exécution de l'agent.

	Client		**Serveur**		
Exécuté par	Utilisateur	Planifié	HTTP Identité utilisateur Web	HTTP Identité signataire	Planifié
Restrictions	LCE du poste		Document du serveur		
	Signataire	Signataire	Signataire	Signataire	Signataire
LCA	Invoqueur	Invoqueur	Invoqueur	Signataire	Signataire

La signature d'un agent et l'explication des postes du tableau suivent maintenant.

Signature de l'agent

La dernière personne qui modifie un agent le signe électroniquement de son nom à l'aide des informations de son fichier ID à la façon dont un message envoyé est signé. Par exemple, un utilisateur qui active l'agent d'absence le signe de son nom.

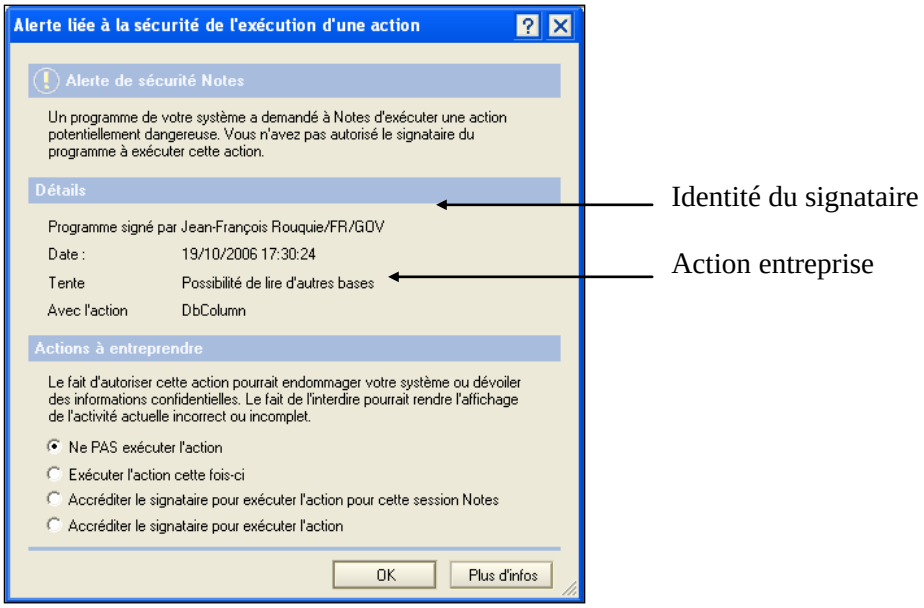
L'administrateur dispose d'un outil de signature dans Domino Administrator qui signe l'ensemble – ou une partie – des notes de conception d'un modèle ou d'une base avec son ID ou celui d'un serveur.

La signature utilisée se fait souvent avec un identifiant réservé à cet effet. Lotus signe ses modèles avec *Lotus Notes Template Development/Lotus Notes*.

Agent exécuté sur un poste client Notes

Il s'agit d'agents lancés manuellement depuis le menu Actions ou planifiés pour s'exécuter localement sur le poste.

Le signataire de l'agent est comparé aux signatures enregistrées dans la LCE (Liste de Contrôle d'Exécution) du poste : si le signataire est absent ou si l'agent utilise des instructions non autorisées, le propriétaire du poste reçoit un message d'avertissement qui lui demande la conduite à tenir.



Les bases en exploitation sur serveur sont habituellement signées avec un identifiant approprié qui est également défini dans la LCE d'administration par l'administrateur. Cette LCE sert de standard aux postes clients et les utilisateurs ne voient pas ce type de message, sauf accident bien sûr.

Une fois que l'identité du signataire de l'agent est validée, le droit de faire ce que fait l'agent dans la base est déterminé par l'identité de l'utilisateur qui invoque l'agent et la LCA de la base.

Agent exécuté en arrière-plan sur le serveur

Le signataire de l'agent est considéré pour vérifier le droit d'exécuter l'agent d'après les informations du document du serveur : droit d'exécuter un agent en langage de formules, en LotusScript/Java non restrictif ou restrictif (utilisant ou non toutes les possibilités du langage).

Le signataire de l'agent est aussi pris en compte pour vérifier le droit de faire ce que fait l'agent dans la base : le signataire doit être dans la LCA – directement ou par son appartenance à un groupe – avec un niveau d'accès suffisant. Une exception à cette règle : un agent exécuté depuis le Web peut le faire avec l'identité de l'utilisateur. Il faut noter que ceci s'applique uniquement à l'accès à la base. Le droit d'exécuter le type auquel appartient l'agent reste déterminé par le signataire.

Scénarios de délégation (version 6, 7, 8)

Les trois scénarios exposés correspondent à des demandes de clients auxquelles Lotus a répondu sans sacrifier le modèle de sécurité. Le principe retenu consiste à passer par une autorité de confiance lorsque le modèle de sécurité de la version 5 n'est pas applicable.

Accès à une base sur un autre serveur

Un agent ne peut pas ouvrir une base se trouvant sur un autre serveur. Lotus estime que le serveur distant n'a pas les moyens de savoir si le signataire de l'agent a un ID fiable :

- Si le signataire est un utilisateur, son ID n'est normalement pas disponible sur le serveur distant et il est protégé par un mot de passe, donc ne pourrait pas être ouvert.
- Si le signataire est un serveur, l'identité de la personne physique qui a procédé à la signature est incertaine puisque l'ID serveur n'est généralement pas protégé par mot de passe.

Sauvegarder un agent sur serveur

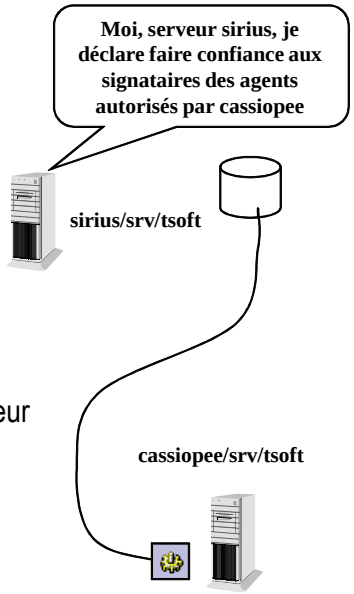
Un utilisateur qui ne dispose pas d'un client Notes ne peut pas signer un agent. C'est le cas des utilisateurs Web. Si un utilisateur Web devait activer ou désactiver un agent, il pourrait le faire en lançant l'exécution d'un agent *supplétif* dont la mission est d'activer ou de désactiver l'agent visé. La question posée est alors : comment signer cet agent modifié ? L'authentification Web est peu fiable comparée à l'authentification Notes : un identifiant et un mot de passe qui peuvent circuler en clair et l'utilisateur Web n'a pas de clé publique (sauf s'il a un certificat SSL individuel, ce qui n'est pas le plus courant). L'autre solution consisterait à signer l'agent avec l'ID de serveur ce qui aboutirait à donner à cet agent les droits du serveur qui sont très étendus. Le modèle de sécurité de la version 5 est dans l'impasse.

Activation par l'utilisateur

L'utilisateur d'une base Courrier a besoin d'être Concepteur dans sa base pour pouvoir activer l'agent d'absence. S'il est Éditeur – sur un serveur 5 et une base courrier 5 –, il ne peut pas activer cet agent. L'accès Éditeur évite notamment que l'utilisateur puisse – intentionnellement ou non – indexer sa base Courrier, ce qui génère de la consommation de ressources disque et processeur sur le serveur.

Agent accédant à un serveur distant

- **Un serveur ne fait pas confiance au signataire de l'agent qui s'exécute sur un autre serveur**
  - L'authentification de la signature n'est pas fiable
- **Modèle de délégation**
  - Le serveur fait confiance au serveur distant d'exécution de l'agent
  - Accréditation dans le document serveur
- **Le signataire de l'agent**
  - Détermine l'accès à la base d'après sa LCA



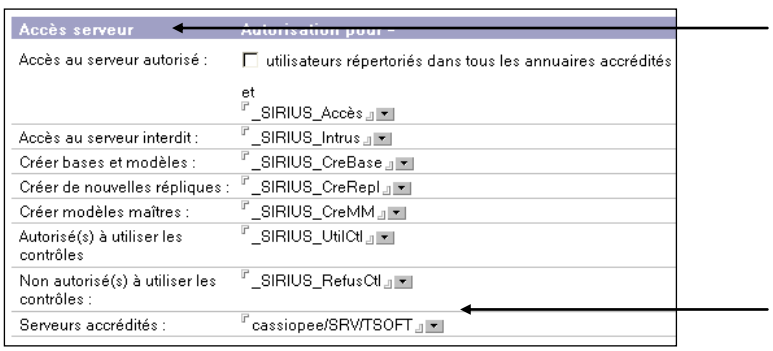
Un agent planifié sur un serveur ne peut pas ouvrir une base se trouvant sur un autre serveur. Lotus estime que le serveur distant n'a pas les moyens de savoir si le signataire de l'agent est effectué avec un ID fiable.

La solution consiste à utiliser le serveur comme autorité de confiance, plus prosaïquement à faire confiance aux choix faits par l'administrateur du serveur : gestion de la sécurité des agents et signataires acceptés.

Le signataire de l'agent doit avoir les droits suffisants dans la base accédée.

Accréditation de serveur

- Ouvrir l'annuaire, puis la vue *Serveurs*/*Serveurs*
- Ouvrir le document du serveur distant en modification
- Cliquer sur l'onglet (Sécurité)



- <Serveurs accrédités> : sélectionner le serveur sur lequel s'exécute l'agent accédant à une base sur le serveur auquel correspond le document

Agent Web planifié sur serveur

- **Un agent activé – ou désactivé – est modifié, donc signé**
- **Un agent ne peut être modifié par un autre agent sur serveur**
  - Il serait signé avec l'ID du serveur
  - Cet ID n'est pas fiable car sans mot de passe
- **Application Web version 6 et suivantes : l'utilisateur lance un agent *supplétif* qui active ou désactive un autre agent**
- **Modèle de délégation**
  - Séparer signataire et modificateur de l'agent
  - Le signataire agit *pour le compte de* celui qui modifie l'agent
  - L'agent et son agent supplétif ont le même signataire

Un utilisateur Web doit activer un agent de l'application qui exécute un traitement planifié, par exemple une clôture d'exercice, un archivage, une récupération de données DB2… L'utilisateur Web ne peut pas signer l'agent d'application puisqu'il ne dispose pas d'un fichier ID Notes. Pour contourner l'absence de fichier ID, il est prévu qu'il lance agent *supplétif* dont la mission est d'activer ou de désactiver l'agent d'application avec la garantie d'une autorité dont la signature est reconnue. Le modèle de sécurité appliqué ici est le suivant :

– L'autorité est signataire des deux agents mis en œuvre.
– L'agent supplétif s'exécute avec l'identité de l'utilisateur Web.
– L'autorité exécute l'agent activé pour le compte de l'utilisateur Web.

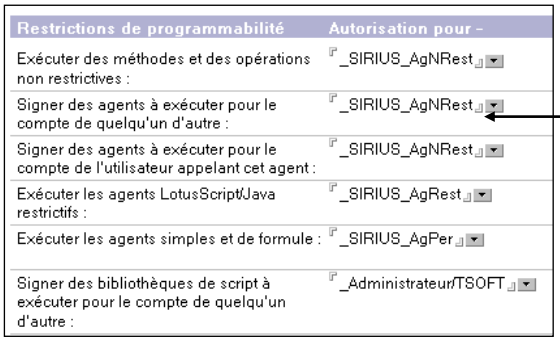
Le modèle s'exprime aussi de la façon suivante : une autorité se porte garante que le couple (agent supplétif, agent activé) est valide pour un utilisateur Web déterminé. L'autorité agit au nom d'un utilisateur Web en apportant sa garantie matérialisée par les informations de son fichier ID Notes et les restrictions portées par l'administrateur dans le document du serveur.

Droits de l'autorité signataire

Les droits sont dans le document du serveur. L'autorité doit avoir le droit de :

– Signer des agents à exécuter pour le compte de quelqu'un d'autre – ici, un utilisateur Web.
– Exécuter les agents *LotusScript/Java restrictifs, simples et de formules* ou des *méthodes et des opérations non restrictives* selon le style de programmation de l'agent.

- Cliquer sur l'onglet (Configuration), puis sur la vue *Serveurs*/*Serveurs*
- Ouvrir le document du serveur distant en modification
- Cliquer sur l'onglet (Sécurité)



Signer des agents à exécuter pour le compte de quelqu'un d'autre

- <Signer les agents à exécuter pour le compte de quelqu'un d'autre> : sélectionner le ou les signataires, ici le groupe *_SIRIUS_AnNRest* qui contient *_Administrateur/TSOFT*

Le signataire est celui des bases mises en production dans cet exemple, ce qui simplifie considérablement la vie.

Droits de l'utilisateur Web

L'utilisateur Web doit avoir l'accès *Concepteur* dans la base où réside l'agent à activer. Ce droit est nécessaire car l'activation – ou la désactivation – d'un agent le modifie. La LCA de la base accepte Concepteur pour *Accès maximum au nom et mot de passe Internet*.

Conclusion

Ce scénario est le plus complexe car il enchaîne en fait deux délégations :

– Une délégation pour activer un agent depuis le Web,
– Une délégation pour exécuter un agent planifié.

Il est clair que la deuxième délégation n'est possible que parce que la première a pu s'exécuter. Ce modèle repose sur le couple signataire et utilisateur tout comme les autres modèles de sécurité.

Activation d'un agent depuis le Web

Signataire : une autorité qui a le droit de *Signer des agents à exécuter pour le compte de quelqu'un d'autre*.

Utilisateur : les deux agents – l'agent supplétif et l'agent activé – s'exécutent tous les deux pour le compte de l'utilisateur Web.

Résultat : l'agent activé est signé par le serveur et s'exécutera pour le compte de l'utilisateur Web.

Délégation pour exécuter un agent

Signataire : le serveur. Cette autorité a le droit d'exécuter des agents *LotusScript/Java restrictifs* ce qui correspond au style de programmation de l'agent activé.

Utilisateur : l'utilisateur qui est dans le champ $OnBehalfOf de l'agent. Le droit d'accès de cet utilisateur dans la LCA de la base est pris en compte pour ce que fait l'agent, par exemple ajouter un document dans la base courante.

Agent d'absence

Configuration compatible version 5

- **Droits de l'utilisateur**
  - Concepteur ou Gestionnaire de sa base Courrier
  - Droit d'exécuter des agents LotusScript/Java restrictifs

Configuration versions 6, 7, 8

- **Droits de l'utilisateur**
  - Éditeur de sa base Courrier
  - Adminp rend l'agent automatiquement *activable par l'utilisateur*
  - Non requis : droit d'exécuter des agents LotusScript/Java restrictifs

Nouveautés version 8 : le Service Absence

L'utilisateur de messagerie qui déclare une absence active l'agent OutOfOffice. Cette opération fonctionne correctement pourvu que les règles de sécurité soient respectées :

– L'utilisateur modifie l'agent en l'activant.
– L'agent planifié doit pouvoir démarrer sur le serveur de messagerie.
– L'agent planifié doit pouvoir faire ce qu'il fait : envoyer des messages.

Les contraintes de la version 5.x de Lotus Domino disparaissent depuis la version 6 :

– Le niveau d'accès Éditeur dans la LCA de la base Courrier est suffisant pour que l'utilisateur déclare une absence.
– L'agent d'absence peut être activé depuis un navigateur Web.
– Le droit d'exécuter des agents LotusScript/Java restrictifs n'a pas besoin d'être donné aux utilisateurs de messagerie ayant le niveau Éditeur.

Ce paragraphe rappelle le mode de fonctionnement et les réglages en version 5.x et qui sont utilisables en version 6 et 7, puis montre comment configurer le fonctionnement de l'agent d'absence en tenant compte des nouveautés de la version 6.

Configuration en version 5

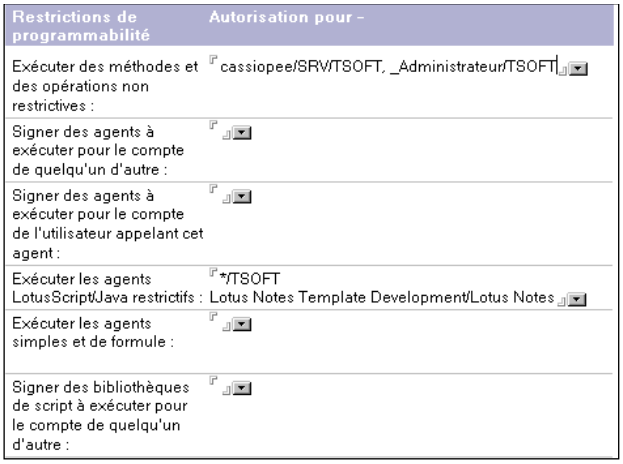
Niveau d'accès des utilisateurs à la base Courrier

Un utilisateur doit avoir le niveau d'accès Gestionnaire ou Concepteur à sa base Courrier pour activer l'agent d'absence OutOfOffice : l'activation de l'agent se fait par modification de cet élément de structure. Le choix de *Editeur* – proposé à l'enregistrement – est insuffisant.

Restrictions du document serveur

L'onglet (Sécurité) du document du serveur gère les règles d'exécution des agents. L'agent d'absence OutOfOffice est du type *LotusScript/Java restrictif* planifié et s'exécute normalement à 1 heure du matin.

Les noms de tous les utilisateurs de messagerie doivent être présents : l'utilisation du nom de l'organisation et du caractère joker étoile – */TSOFT – simplifie l'écriture.



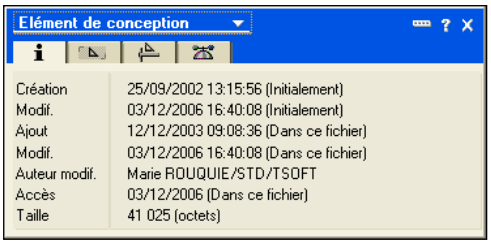
L'utilisateur Claude GAUTIER/SEC/TSOFT a le droit d'exécuter l'agent OutOfOffice du fait de son appartenance à */TSOFT.

Signature des bases

Les bases Courrier sont signées par *Lotus Notes Template Development/Lotus Notes*. L'agent d'absence est signé du nom de l'utilisateur lorsqu'il est modifié par activation ou désactivation. La signature de Lotus est en standard dans la LCE des clients Notes et est normalement conservée : les bases Courrier ne sont pas signées avec un autre identifiant.

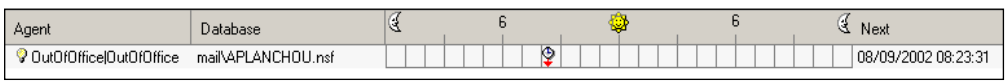
Le nom du signataire est inscrit dans l'agent d'absence. Pour le vérifier :

- Ouvrir la base Courrier de l'utilisateur dans Designer
- Ouvrir la vue *Code partagé/Agents*, puis clic droit sur OutOfOffice, puis commande *Propriétés de la structure…*



- <Modifié par> : contient le nom du propriétaire de la base Courrier après la première activation de l'agent

Suivi dans Domino Administrator



L'agent d'absence planifié apparaît dans la liste *Planification/Agents* sur le serveur de messagerie.

Si le propriétaire de la base Courrier n'a pas le droit d'invoquer des agents de type *LotusScript/Java restrictifs*, un message est envoyé dans le journal du serveur.

```
08/09/2006 08:19:31   AMgr: Agent 'OutOfOffice|OutOfOffice' in
'mail\APLANCHOU.nsf' does not have proper execution access,
cannot be run
```

Configuration en versions 6, 7 et 8

L'agent d'absence utilise deux nouvelles fonctions de la version 6 :

- Le concept d'une autorité de délégation qui agit au nom d'un utilisateur et dont les droits sont pris en compte pour lancer l'exécution de l'agent. Les droits de l'utilisateur sont pris en compte pour l'accès à sa base Courrier.
- L'activation de l'agent d'absence par un utilisateur disposant d'un niveau d'accès *Éditeur* à la base.

Ces deux fonctions couplées ont été implémentées dans le masque à partir duquel est activé l'agent d'absence. Lorsque le niveau d'accès de l'utilisateur à sa base de messagerie passe au niveau *Editeur*, la configuration de l'agent d'absence se fait automatiquement pour bénéficier des fonctions de la version 6.x. Inversement, si le niveau d'accès de l'utilisateur passe de *Editeur* à *Concepteur* ou *Gestionnaire*, la configuration de l'agent d'absence repasse automatiquement dans le mode version 5.x.

Niveau d'accès des utilisateurs à la base Courrier

L'utilisateur a le niveau d'accès *Éditeur* à sa base Courrier. Il pourra gérer son courrier et son agenda mais ne pourra pas indexer sa base pour une recherche documentaire, modifier les paramètres de réplication ou supprimer sa base.

Si l'utilisateur de messagerie n'a pas le niveau d'accès *Gestionnaire* à sa base Courrier – il est *Concepteur* ou *Éditeur* –, il est nécessaire qu'il ait le niveau d'accès *Auteur* assorti du privilège de Création de documents dans la LCA de la base de *Requêtes administratives* – admin4.nsf – pour qu'il puisse utiliser la délégation de courrier et d'agenda. En effet, la modification d'une délégation crée une requête dans la base admin4.nsf, puis la requête est exécutée par le serveur qui modifie la LCA de la base Courrier. Ce mode de fonctionnement est apparu en version 5.

La première activation de l'agent d'absence de l'utilisateur de niveau d'accès *Éditeur* crée aussi une requête administrative.

Autorité de délégation

Le client Notes génère automatiquement une requête administrative qui modifie l'agent d'absence OutOfOffice. Le serveur de messagerie qui exécute la requête signe l'agent d'absence. Le lancement de l'exécution de l'agent se fait avec les droits du serveur – le serveur joue le rôle d'autorité de délégation – alors que les droits de l'utilisateur dans la LCA de sa base Courrier sont pris en compte pendant l'exécution de l'agent.

Restrictions du document serveur

L'onglet (Sécurité) du document du serveur qui gère les règles d'exécution des agents n'a pas besoin de contenir les noms des utilisateurs dont le niveau d'accès à leur base Courrier est *Éditeur*.

- <Exécuter les agents LotusScript/Java restrictifs> : la signature générique */NomOrganisation, par exemple **/TSOFT* n'est plus nécessaire

Dans la pratique, si le serveur de messagerie héberge aussi des utilisateurs ayant le niveau d'accès *Gestionnaire* ou *Concepteur*, il faudra quand même que le champ contienne la liste de ces utilisateurs abrégée en utilisant le caractère joker * et le nom de l'organisation, par exemple **/TSOFT*, ou alors le groupe de ces utilisateurs.

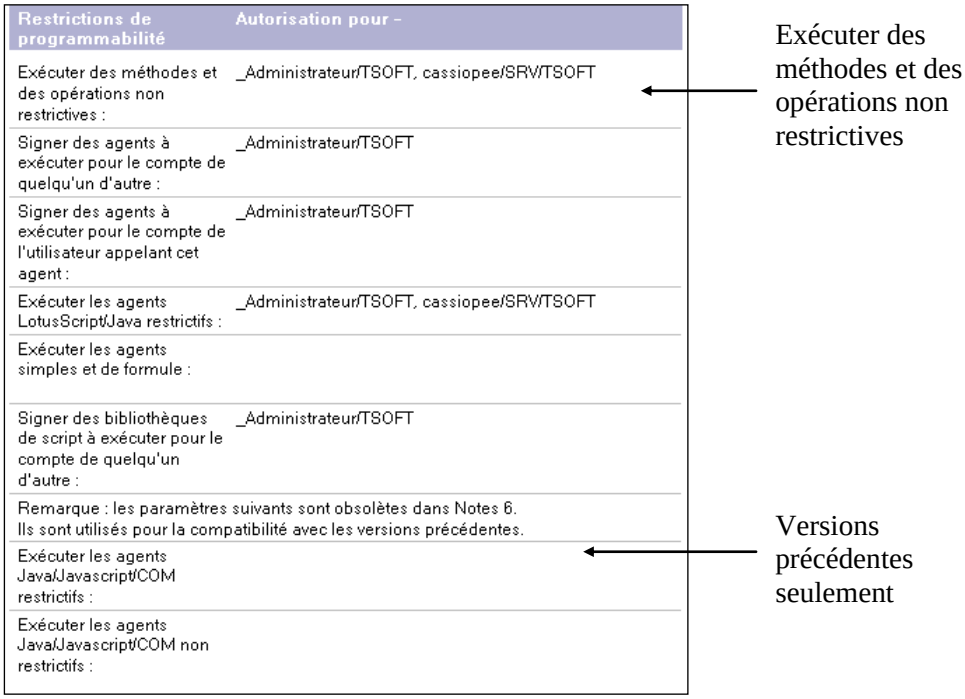
Remarque

Ce manuel traite également du Service Absence (chapitre 7) qui est une nouveauté de la version 8.

Restrictions de programmabilité

- **Restrictions de programmabilité**
- **Droits d'exécution, y compris Java, JavaScript/COM, CORBA**
  - Opérations non restrictives
  - Opérations restrictives
  - Agents simples et formules
- **Droits de signer «pour le compte de»**
  - Des agents
  - Des agents *supplétifs* qui activent/désactivent d'autres agents
  - Des bibliothèques de scripts
- **Droits d'exécution des agents Java/JavaScript COM : applicables aux serveurs 5**

Les restrictions d'exécution des agents sont réunies dans le document du serveur, dans l'onglet (Sécurité) et le paragraphe *Restrictions de programmabilité*.



Restrictions de programmabilité	Autorisation pour :
Exécuter des méthodes et des opérations non restrictives :	_Administrateur/TSOFT, cassiopee/SRV/TSOFT
Signer des agents à exécuter pour le compte de quelqu'un d'autre :	_Administrateur/TSOFT
Signer des agents à exécuter pour le compte de l'utilisateur appelant cet agent :	_Administrateur/TSOFT
Exécuter les agents LotusScript/Java restrictifs :	_Administrateur/TSOFT, cassiopee/SRV/TSOFT
Exécuter les agents simples et de formule :	
Signer des bibliothèques de script à exécuter pour le compte de quelqu'un d'autre :	_Administrateur/TSOFT
Remarque : les paramètres suivants sont obsolètes dans Notes 6. Ils sont utilisés pour la compatibilité avec les versions précédentes.	
Exécuter les agents Java/Javascript/COM restrictifs :	
Exécuter les agents Java/Javascript/COM non restrictifs :	

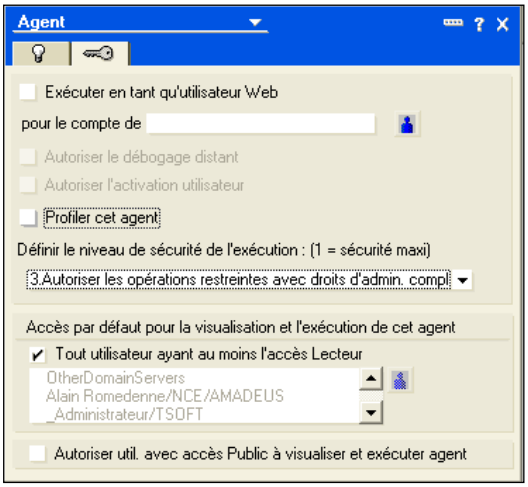
– <Exécuter des méthodes et des opérations non restrictives> : regroupe les champs <Exécuter les agents Java/JavaScript/COM non restrictifs> et <Exécuter les agents LotusScript/Java non restrictifs> de la version 5.
– <Exécuter les agents LotusScript/Java restrictifs> : regroupe les champs <Exécuter les agents Java/JavaScript/COM restrictifs> et <Exécuter les agents LotusScript/Java restrictifs> de la version 5.

Exécuter des méthodes et des opérations non restrictives	
	Signataires autorisés à signer des agents avec les trois niveaux : 1. Ne pas autoriser les opérations restreintes 2. Autoriser les opérations restreintes 3. Autoriser les opérations restreintes avec droit d'admin. complet Le choix du niveau (1) ne requiert pas la présence dans ce champ. Ce signataire peut modifier/supprimer une base sans être listé dans la LCA s'il est Administrateur de bases. Le serveur et la signature *Lotus Notes Template Development/Lotus Notes* ont ce droit par défaut. L'administrateur complet doit être aussi présent dans ce champ si le mode (3) est sélectionné pour l'agent.
Signer des agents à exécuter pour le compte de quelqu'un d'autre	
	Signataires autorisés à signer des agents *Exécuter pour le compte de*. Le nom de la personne pour le compte de laquelle l'agent a été signé est utilisé pour vérifier l'accès dans la LCA de la base.
Signer des agents à exécuter pour le compte de l'utilisateur appelant cet agent	
	Signataire autorisé à signer des agents exécutés au nom de celui qui lance l'exécution et qui n'est pas le signataire. Agents Web uniquement. Le défaut – champ non rempli – donne l'autorisation à tous (compatibilité avec les versions précédentes).
Exécuter des agents LotusScript/Java restrictifs	
	Signataires pouvant exécuter des agents LotusScript/Java restrictifs.
Exécuter les agents simples et de formules	
	Signataires pouvant exécuter des agents privés ou partagés écrits avec des actions simples ou des formules. Le défaut – champ non rempli – donne l'autorisation à tous (compatibilité avec les versions précédentes).
Signer des bibliothèques de scripts à exécuter pour le compte de quelqu'un d'autre	
	Signataires pouvant signer des bibliothèques de scripts utilisées par des agents signés par d'autres. Le défaut – champ non rempli – donne l'autorisation à tous (compatibilité avec les versions précédentes).

<Exécuter les agents LotusScript/Java restrictifs> : ne contient que deux signatures. Les utilisateurs du serveur ne peuvent pas avoir directement ce droit. Sur un serveur de messagerie, ceci suppose que tous les utilisateurs sont *Éditeurs* ce qui permet à l'agent d'absence signé par le serveur de s'exécuter.

Le tableau indique comment se déterminent les droits et démontre que le nombre de signataires doit être réduit au minimum. C'est d'ailleurs ce que propose la copie d'écran qui se limite à *_Administrateur/TSOFT* ce qui est suffisant pour une organisation n'ayant que quelques serveurs Domino.

Signature des agents au cas par cas



Lorsque le signataire d'une base veut imposer à un agent de ne pas pouvoir exécuter des opérations restreintes, il doit :

- Ouvrir l'agent dans Designer
- Afficher les propriétés de l'agent

 Cliquer sur l'onglet (Sécurité).

- <Définir le niveau de sécurité de l'exécution> : sélectionner une option
  – *1. Ne pas autoriser les opérations restreintes*
  – *2. Autoriser les opérations restreintes*
  – *3. Autoriser les opérations restreintes avec droits d'admin. complet*

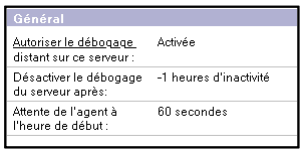
Dans la pratique, si un agent doit exécuter des opérations restreintes, il faut que la première option soit sélectionnée, faute de quoi l'agent de s'exécutera pas correctement.

Remarque

La nature du langage LotusScript – il est interprété – fait que le compilateur ne sait pas si des méthodes ou des instructions du langage sont utilisées et dans quelles conditions. Ceci explique cette intervention manuelle.

Débogage distant d'un agent

- **Déboguer un agent s'exécutant sur le serveur**
  - Tâche RDEBUG active sur serveur
  - Activer l'agent pour le débogage distant
  - Attraper l'agent lorsqu'il va s'exécuter
  - Fenêtre de mise au point LotusScript



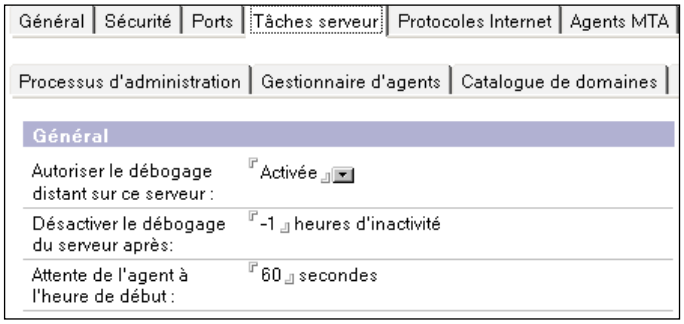
La tâche RDebug – apparue en version 6 – permet d'analyser l'exécution d'un agent planifié sur le serveur. Le serveur doit être configuré pour le débogage à distance ainsi que l'agent à déboguer.

Notes.ini

La ligne ServerTasks du NOTES.INI du serveur doit contenir Rdebug.

```
ServerTasks=Update,Replica,Router,AMgr,AdminP,CalConn,Sched,Statlog,DIIOP,DECS,HTTP,Rdebug
```

Document serveur



- Cliquer sur l'onglet (Tâches serveur), puis sur l'onglet (Remote Debug Manager)
- <Autoriser le débogage distant sur ce serveur> : sélectionner *Activée*

– <Désactiver le débogage du serveur après> : taper une valeur en heures, -1 signifiant jamais
– <Attente de l'agent à l'heure de début> : taper un nombre de secondes suffisant – 60 secondes – pour attraper au vol l'agent lorsqu'il débutera son exécution

Interview de l'Expert

Ne jamais oublier qu'il existe une commande TELL AMGR RUN, permettant de lancer un agent de force, sans devoir attendre à la console. Dans le cas d'un agent agissant sur le système de fichiers, le déverminage distant est le seul moyen d'avoir une vision claire de l'environnement du compte serveur. En effet, un disque mappé pour compte serveur n'aura pas forcément la même lettre pour le compte de celui qui ouvre la session sur ledit-serveur (par exemple).

Rappel des objectifs

- **Connaissances**
  - Fonctionnement des agents
- **Savoir-faire**
  - Définir les restrictions de programmabilité
  - Définir un serveur d'exécution
  - Paramétrer le gestionnaire d'agents

Ce module décrit les agents du point de vue de l'administration. Les instructions de mise en exploitation comprennent les procédures applicables aux agents.

Rôle des agents

Les agents effectuent des traitements sur un document ou un ensemble de documents. Ils sont une pièce maîtresse des applications de workflow, des applications Web.

L'exécution d'un agent est déterminée :

– Par une action de l'utilisateur Notes ou Web.
– Par l'événement *Après la création ou modification de documents* ou *Après l'arrivée de nouveaux messages*.
– Par planification sur le serveur.

L'exécution d'un agent est prise en charge par :

– Le client Notes.
– Le gestionnaire d'agents.
– Le service HTTP de Domino.
– Le routeur de courrier.

L'administrateur paramètre l'environnement d'exécution des agents : ressources, sécurité, serveur d'exécution.

Paramétrage du gestionnaire d'agents

Le gestionnaire d'agents prend en charge les agents planifiés sur le serveur – horaires, quotidiens, hebdomadaires, mensuels – et les agent activés par les événements *Après la création* et *modification de documents* ou *Après l'arrivée de nouveaux messages*. Il gère trois files d'attente : file **V** (Update Event Queue et New Mail Event Queue), file **S** (Scheduled Task Queue) et file **E** (Eligible Queue).

Les unités d'exécution prennent en charge les agents de la file E.

Le document du serveur et le document de configuration du serveur – onglet (Paramètres NOTES.INI) – déterminent les temps d'attente dans chaque file et le nombre d'unités d'exécution.

Paramétrage du routeur de messagerie

Le routeur de messagerie prend en charge l'exécution des agents de type *Avant l'arrivée de courrier*. Cette prise en charge est autorisée ou non et le temps maximum d'exécution est fixé.

Paramétrage du moteur HTTP

Les agents invoqués depuis un navigateur – par URL, à l'enregistrement de document ou à l'affichage d'un document – sont pris en charge par le moteur HTTP de Domino. Le paramétrage se fait :

- Dans le document du serveur : compatibilité avec la version 5 de Domino,
- Dans un document de site Internet : version 6, 7 et 8 de Domino.

Serveur d'exécution d'un agent

Un agent s'exécute sur le client Notes ou sur serveur. Le choix du serveur d'exécution obéit à des règles dépendant de son type :

- Agent courrier (les deux types) : le serveur de messagerie du signataire,
- Agent lancé manuellement : le client Notes,
- Agent planifié ou réveillé par l'événement *Après la création ou modification de documents* : choix du concepteur ou à la première utilisation.

Si la base est répliquée sur plusieurs serveurs, un agent qui modifie des documents ne peut s'exécuter que sur un seul serveur, faute de quoi des conflits de mise à jour se produiront. Le choix du serveur sera fait au moment de la mise en exploitation.

Modèle de sécurité des agents

Le modèle de sécurité de la version 5 est actif par défaut : ceci assure une compatibilité ascendante et correspond aussi au cas le plus fréquent de la programmation des agents. Ce modèle de sécurité repose sur la confiance accordée au signataire de l'agent. La version 6 introduit le concept de délégation dont le principe est le suivant : une autorité de confiance se porte garante du signataire d'un agent, de l'identité d'un utilisateur. Les droits de l'autorité de confiance interviennent de différentes manières selon les scénarios :

- Accès à une base sur un autre serveur
- Sauvegarde d'un agent sur serveur : utilisé pour l'activation d'un agent depuis le Web avec un agent *supplétif*
- Activation par l'utilisateur Éditeur : utilisé notamment avec l'agent d'absence.
- En version 8.5.1, il devient possible d'interdire à un agent d'exécuter des XPages.

Restrictions de programmabilité

Les restrictions d'exécution des agents sont réunies dans le document du serveur, dans l'onglet (Sécurité) et le paragraphe *Restrictions de programmabilité*. Une technique simple est de disposer d'une seule signature pour toutes les bases mises en exploitation et de donner à cette signature tous les droits dans le paragraphe de restrictions de programmabilité.