

PRINCIPE DE SECURITE DANS LOTUS DOMINO

LOTUS DOMINO 6.X

Dans n'importe quelle structure (entreprise, administration, association,...) la sécurisation de l'environnement Informatique est une question essentielle, voir même de survie. Il est important de connaître le détail de l'utilisation des ressources informatiques.

La configuration de la sécurité de votre organisation est une tâche délicate. L'infrastructure de sécurité joue un rôle primordial dans la protection des ressources Domino de votre organisation. En tant qu'administrateur, vous devez analyser avec précision les exigences en matière de sécurité de votre organisation avant de configurer des serveurs Domino ou des utilisateurs Notes. Une planification efficace en amont prévient les risques générés par un système de sécurité défaillant.

Évaluez les points suivants :

Seriez-vous amené à gérer plusieurs domaines Domino ?

Vos données seront-elles accessibles depuis internet ?

Qui devra disposer de quel type d'accès à l'annuaire domino, cœur de votre système ?

Quelle est la criticité de vos données ? Ceci devra prendre en compte, les intrusions dans votre système informatique, les interactions avec d'autres applications, les erreurs humaines (utilisateurs et administrateurs), les effets turnOver.

1. Modèle de sécurité Domino

Le modèle de sécurité Domino est basé sur la protection des ressources, tels que le serveur Domino, les bases, les données du poste de travail et les documents. Les ressources, du serveur sont configurées de sorte à définir les droits d'accès et de modification, accordé à des utilisateurs et des serveurs. Les informations sur les droits d'accès et les privilèges sont enregistrées dans chaque ressource protégée. Ainsi, un utilisateur ou un serveur donné peut disposer de jeux de droits d'accès différents selon les ressources auxquelles cet utilisateur ou ce serveur requièrent l'accès.

Voici les ressources qu'il faut absolument protéger dans un environnement Domino :

- Le serveur physique (crash disque, dégât des eaux, incendie....)
- Le système d'exploitation : limitez les droits d'accès système, évitez de faire tourner le service FTP sur le serveur Domino, n'installez pas votre serveur Domino sur un serveur de fichiers, évitez également les liens repertoire vers des serveurs de fichiers.
- Sécurité du réseau en prenant en compte tous les protocoles réseau activés dans votre environnement.
- Enfin insistez auprès des utilisateurs sur le fait que la sécurité relève de la responsabilité de chacun d'eux. Vous devez former les utilisateurs aux notions suivantes, en adaptant ces dernières aux besoins de l'entreprise :
 - Authentification Domino
 - Sécurité dans les applications utilisées
 - Sécurité de la messagerie qui reste néanmoins une des briques principales de Lotus.

2. Différents niveaux de planification de la sécurité Domino

Domino offre la possibilité de contrôler les accès au système à cinq niveaux différents : Fig.1

- ☒ sécurité au niveau du serveur : elle permet au serveur de contrôler l'authenticité des utilisateurs et des serveurs qui tentent d'accéder à ses ressources par processus basé sur jeux de clés et de certificats.
- ☒ sécurité au niveau des ressources et applications : une Liste de Contrôle d'Accès (L.C.A.) autorise différents droits d'accès et manipulation des ressources et applications.
- ☒ sécurité au niveau des éléments de conception d'une application.
- ☒ sécurité au niveau des ID : pièce d'identité des utilisateurs et des serveurs
- ☒ sécurité aux niveau des postes de travail utilisateurs, car ceux-ci peuvent stoker des applications qui seront deversées ultérieurement sur le serveur; leur accès doit être également sécurisé. De même une application ne doit pas mettre en péril la sécurité du poste de travail.

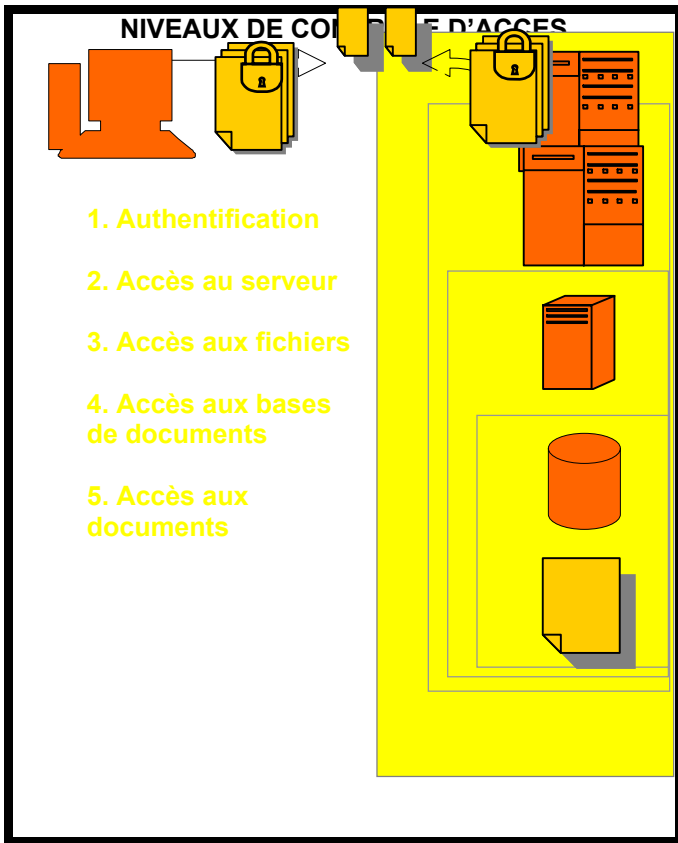
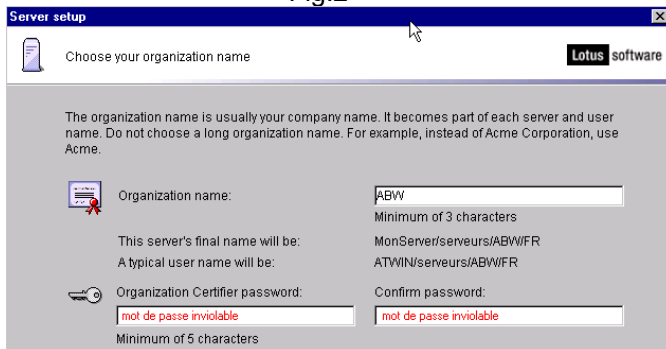


Fig.1

2.1. La sécurité d'accès au serveur

Elle est basée sur un principe de certificats. Un certificat est un tampon électronique unique qui identifie un utilisateur ou un serveur et est stocké dans le fichier ID. Il contient la signature (nom) du certificateur (accréditeur) qui l'a délivré et le nom du bénéficiaire; il contient également une clé publique enregistrée aussi bien dans l'ID que dans l'annuaire Domino, une signature électronique et les dates de validité. Lorsque que vous installez et enregistrez votre premier serveur Domino, vous créez en même temps le premier certificateur de votre domaine Domino qui engendrera certainement d'autres certificateurs. Ainsi veuillez à sécuriser au maximum ce certificateur (fichier ID cert.id). Donnez lui un mot de passer incassable et mettez ce fichier en lui sûr. Il ne faudra ni le perdre ni l'endommager. Il sera de même pour tous vos ID certificateurs.

Fig.2



Après l'installation du serveur Domino, avant de créer des utilisateurs ou des serveurs supplémentaires, créez en fonction de votre politique d'organisation, autant de subordonnés certificateurs que de groupes de politique de sécurité à appliquer. Ceci vous simplifiera énormément vos tâches d'administration par la suite.

- Exemple de subordonnés :
- DEVELOPPEMENT/ABW/FR
- TECHNIQUE/ABW/FR
- COMMERCIAL/ABW/FR
- DIRECTION/ABW/FR

La sécurité d'accès au serveur commence au moment de l'authentification du client Notes (utilisateur ou serveur). Après la saisie du mot de passe d'identification, le serveur vérifie si le client et lui ont en commun un certificateur parent (certificat Notes ou certificat Notes croisé). Sinon, ce client n'aura aucun droit d'accès au serveur et se fera rejeté. Si oui le serveur établit la communication avec le client et se réfère ensuite à la sécurité en vigueur paramétrée dans le document serveur pour vérifier ses droits d'accès effectifs.

2.1.1 Paramétrage de la sécurité d'accès au serveur.

Le serveur regarde en priorité la section Accès au serveur du document serveur, une fois le client authentifié.

Server Access	Who can -
Access server:	All users can access this server
Not access server:	
Create databases & templates:	Administrateur, LocalDomainServers, Support et Maintenance
Create new replicas:	Administrateur, LocalDomainServers, Support et Maintenance, Support Niveau 1, OtherDomainServers,
Create master templates:	Administrateur, LocalDomainServers, Support et Maintenance
Allowed to use monitors:	*
Not allowed to use monitors:	
Trusted servers:	

Fig.3

Soit vous autorisez l'accès à tous dans le champ **Acces server** (tout client authentifié) et vous gerez ensuite la liste des indesirables dans le champ **Not access server**. Fig.3

Si tel est le cas nous vous conseillons de créer un groupe **Intrus** de type Deny dont les membres seront les personnes non autorisées (anciens employés de la société par exemple, ou toute personne qui pourrait mettre en péril les données présentes sur ce serveur...) Soit vous pouvez aussi, si vous êtes en environnement multi-domaine, n'autoriser l'accès qu'aux utilisateurs répertoriés dans vos différents Annuaire. Toutefois vous devriez mettre en place une accréditation par assistance d'annuaire. Fig.4

Server Access	Who can -
Access server:	<input checked="" type="checkbox"/> users listed in all trusted directories
	and
	<input type="checkbox"/> []
Not access server:	<input type="checkbox"/> []
Create databases & templates:	<input type="checkbox"/> Administrateur, LocalDomainServers, Support et Maintenance
Create new replicas:	<input type="checkbox"/> Administrateur, LocalDomainServers, Support et Maintenance, Support Niveau 1, OtherDomainServers
Create master templates:	<input type="checkbox"/> Administrateur, LocalDomainServers, Support et Maintenance
Allowed to use monitors:	<input type="checkbox"/> []
Not allowed to use monitors:	<input type="checkbox"/> []
Trusted servers:	<input type="checkbox"/> []

Fig.4

Mise en place d'une assistance d'annuaires accrédités

Depuis Domino Administrator ou depuis le client notes, créez une base avec le modèle da.ntf (directory Assistance).

Déclarez la base créée dans le document serveur, onglet Basic, section Directory information.

Ensuite créez autant de documents de configuration que vous aurez d'annuaires à accréditer, hors mis votre annuaire du Domaine (names.nsf).

Vous pouvez prendre en compte aussi bien des annuaires Domino que des annuaires de type LDAP.

Attention, si vous aviez déjà une ligne Names=names.nsf, names1.nsf, names2.nsf, names3.nsf.... supprimez la.

Ainsi toutes les personnes et serveurs figurants dans ces différents annuaires seront accrédités aussi bien en accès notes que Internet.

2.1.2 Limitation des opérations sur le serveur.

Limitation dans l'administration du serveur et de ses ressources

Il est désormais possible de définir à la manière d'Unix un root dans l'administration du serveur domino. Donner le droit full access à une personne lui permet de passer outre toutes les restrictions, dès lors qu'elle a accès au serveur. Elle obtient un contrôle total sur toutes les ressources du serveur. Ne donnez pas ce droit à un utilisateur. Par contre vous pouvez créer un utilisateur spécial que vous mettez dans le champ correspondant (**Full Access Administrators**) pour des fins de dépannage.

Exemple: Root DOMINO/TECHNIQUE/ABW/FR

Son ID doit être en lieu sûr. Vous pouvez même pour plus de sécurité, affecter plusieurs mots de passe à cette ID.

Nous allons maintenant faire le tour des autres options de la partie Administration de l'onglet security du document serveur.

• Le champ **Administrators** est l'équivalent de la version 5 de Domino (onglet general, puis Administrateurs) avec une extension implicite de certains droits.

Entrez les noms des administrateurs autorisés à administrer le serveur. La valeur par défaut de ce champ

est le nom de l'administrateur qui a configuré le serveur. Ils bénéficieront alors des droits suivants :

1. Droits d'accès Gestionnaire à la base de documents Web Administrator (WEBADMIN.NSF) ;
2. Droits de création, de mise à jour et de suppression de liens vers un dossier ou une base ;
3. Droits de création, de mise à jour et de suppression des LCA de lien de répertoire ;
4. Droits de compression et de suppression des bases de documents ;
5. Droits de création, de mise à jour et de suppression des index documentaires ;
6. Droits de création de bases de documents, de répliques et de modèles maîtres ;
7. Droits d'obtention et de définition de certaines options de base (par exemple, en/hors service, quotas de base, etc.) ;
8. Droits d'utilisation du suivi des messages et des objets ;
9. Droits d'utilisation de la console pour administrer à distance les serveurs UNIX ;
10. Droits d'émission de commande de console à distance.

• Les personnes dont les noms figureront dans le champ **Database Administrators** bénéficieront de tous les droits ci-dessus à l'exception des droits 1,8,9 et 10.

• Dans le champ **Full Remote Console Administrators**, entrez les noms des administrateurs autorisés à utiliser la console à distance pour émettre des commandes au serveur.

• Les **View-Only Administrators** ne pourront que envoyer à la console que des tâches de visualisation (Show task, Show Server, Show user. Affectez ce droits à des développeurs non administrateurs qui pourront vérifier d'eux même que certaines tâches tournent sur le serveur, au lieu de faire systématiquement la demande à l'administrateur.

Ils ne pourront lancer aucune commande susceptible de mettre le serveur en péril.

• Les **system Administrators** seront autorisés à exécuter un ensemble de commandes de système d'exploitation sur le serveur.

Les personnes déclarées dans ce champ, si elles ont également les droits dans la LCA de la WEBADMIN.nsf pourront de ce fait arrêter et redémarrer des services NT depuis un navigateur Web. Nous en reparlerons. Vous pouvez donner ce droit à des administrateurs système, mais connaissant peu domino.

• Vous pouvez également lister un certain nombre de commandes système et ne donner que les droits d'exécution de ces commandes aux personnes dont les noms figurent dans le champ **Restricted System Administrators**. Fig.5

Attention: Les administrateurs enregistrés dans les champs Full Access Administrators, Administrators et Databases Administrateurs sont autorisés à supprimer n'importe quelle base de ce serveur, même s'ils ne sont

pas répertoriés comme gestionnaires dans la LCA de la base.

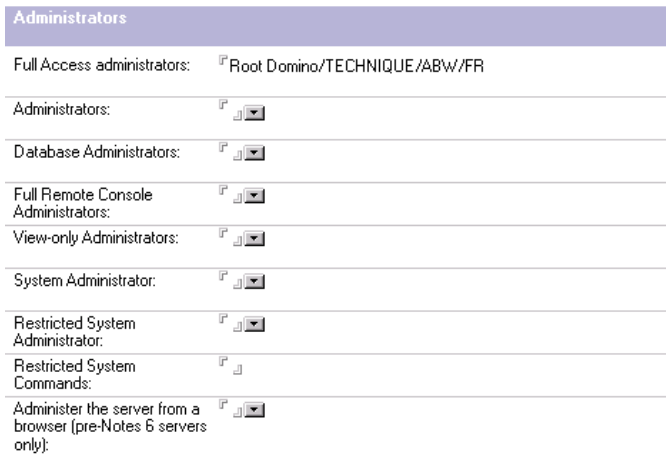


Fig.5

Limitation dans les programmes et exécution automatique

L'exécution d'un programme Notes/Domino appelé agent Notes se fait avec les droits de celui qui l'a créé ou qui l'a modifié la dernière fois. On dit que l'agent porte sa signature. Ainsi est contrôlé tout programme s'exécutant sur un serveur Domino. Tout le monde n'aura donc pas la possibilité de faire exécuter tel ou tel type de programme. Et maintenant avec la version 6.x de Domino, il est possible de signer un agent qui s'exécutera sous le nom de quelqu'un d'autre. Ces points sont traités dans le N°3 de nsfmag.

Cependant nous vous conseillons de créer un utilisateur spécial, pour signer vos bases.

Ex : Admin SIGN/TECHNIQUE/ABW/FR. Au moins il ne risque ni de changer de nom, ni de quitter la société.

2.2. Sécurité des ressources et applications

Chaque base de documents possède une liste de contrôle d'accès (LCA) qui permet de gérer l'accès des utilisateurs Notes et Internet/intranet, et des serveurs Domino à une application. Bien que les noms des niveaux d'accès pour les utilisateurs et les serveurs soient identiques, ceux qui s'appliquent aux utilisateurs définissent des tâches qui leur sont spécifiques, tandis que ceux qui s'appliquent aux serveurs définissent le type d'informations de la base susceptible d'être répliqué par les serveurs. Nous vous conseillons de toujours spécifier le type des entrées de la LCA. Seuls les utilisateurs bénéficiant de l'accès Gestionnaire peuvent créer ou modifier une LCA.

Chaque fois qu'un utilisateur accède à une base de documents, Notes cherche son nom dans la LCA de la base en question et classe l'utilisateur dans l'un des sept niveaux d'accès suivants où sont déterminés ses droits.

Opérations réalisables	Niveaux d'accès					
	Déposant	Lecteur	Auteur	Editeur	Concepteur	Gestionnaire
Lire des documents publics	◆	◆	◆	◆	◆	◆
Créer des documents	◆			◆	◆	◆
Supprimer des documents			◆	◆	◆	◆
Modifier des documents personnels			◆	◆	◆	◆
Modifier des documents publics	◆			◆	◆	◆
Créer des agents personnels		◆	◆	◆	◆	◆
Créer des vues/dossiers personnels		◆	◆	◆	◆	◆
Créer des vues/dossiers publics				◆	◆	◆
Créer des agents LotusScript		◆	◆	◆	◆	◆
Contrôler les accès						◆
Supprimer la base						◆

◆ : autorisation permanente
 ◆ : autorisation optionnelle (attribuée par le gestionnaire)

Un utilisateur peut être identifié en tant que personne ou bien faire partie d'un groupe. Tous les membres d'un groupe auront les mêmes droits. Cela permet de simplifier les contrôles d'accès pour certaines bases. Il en est de même pour les serveurs.

Attribuez des propriétaires aux groupes que vous créez si vous souhaitez déléguer leur administration à d'autres personnes. Un groupe possède un/des propriétaires, un/des administrateurs et des membres. Le propriétaire peut modifier le groupe et l'administrateur a un rôle de type éditeur. Les membres sont des personnes ou des groupes.

Une fois que vous avez défini les entrées de LCA correspondant à votre politique de sécurité, vous pouvez l'affiner par application de rôles.

Les rôles sont une autre possibilité pour regrouper des utilisateurs ayant les mêmes droits d'accès.

2.2. Sécurité dans les éléments de conception d'une application

La sécurité des éléments de structure d'une application est définie au moment de sa conception par le développeur. Domino ne tient compte de cette couche qu'au moment de l'accès à l'application. Nous conseillons de donner tous les droits à vos serveurs notamment le groupe LocalDomainServers de même qu'au groupe OtherDomainServers, mais il faut bien spécifier les membres de ce dernier groupe.

Le tableau suivant présente les différents contrôles qu'il est possible de planifier depuis le design d'une application. C'est pourquoi développeurs et administrateurs doivent travailler en concertation.

Mise en place	Effet
Liste de contrôle d'accès en lecture seule pour les vues	Définit les utilisateurs Notes et Internet/intranet qui peuvent afficher une vue.
Liste de contrôle d'accès en lecture et en écriture pour les dossiers	Définit les utilisateurs Notes et Internet/intranet qui peuvent afficher un dossier ou mettre à jour son contenu.
Liste de contrôle d'accès en lecture et en écriture pour les masques	Définit les utilisateurs Notes et Internet/intranet qui peuvent créer, modifier ou lire des documents créés à partir d'un masque.
Champ Lecteur et Auteur	Définit les utilisateurs Notes et Internet/intranet qui peuvent créer, modifier ou lire des documents spécifiés.
Champ signé	Vérifie si l'utilisateur Notes à l'origine des données en est l'auteur et qu'aucune falsification des données n'a eu lieu.
Champ chiffré	Permet de contrôler les utilisateurs Notes autorisés à accéder à un champ d'un masque.
Champ masqué	Contrôle les utilisateurs Notes et Internet/intranet autorisés à accéder à un champ d'un masque.
Liste de contrôle d'accès en lecture et en écriture pour les sections	Définit les utilisateurs Notes et Internet/intranet qui peuvent accéder à une section d'un document.

2.3. Sécurité des ID utilisateurs

L'ID est la carte d'identité d'un utilisateur, un serveur ou un certificateur, consignée dans un fichier d'extension .id.

Quand un client notes accède à un serveur c'est dans ce fichier que sont lus les éléments permettant de l'authentifier. Il contient un mot de passe dont la complexité est fixée par l'administrateur à l'enregistrement de l'utilisateur, du serveur ou du certificateur.

Sensibilisez vos utilisateurs à changer souvent de mot de passe pour ne pas se faire usurper leur identité, à ne pas laisser trainer des copies de leur ID.

Vous pouvez également configurer Domino pour qu'il fasse une vérification de mot de passe pour ne prendre en compte que le mot de passe le plus récent. Ainsi Si un utilisateur non autorisé réussit à obtenir un ID et son mot de passe alors que le serveur est configuré pour procéder à une vérification des mots de passe, l'utilisateur autorisé n'aura qu'à modifier le mot de passe de cet ID. La prochaine fois que l'utilisateur non autorisé tentera de s'authentifier, l'accès au serveur lui sera refusé pour raison de mot de passe erroné.

Pour activer la vérification du mot de passe pour une personne, ouvrez le document personne dans l'annuaire Domino, puis l'onglet Administration.

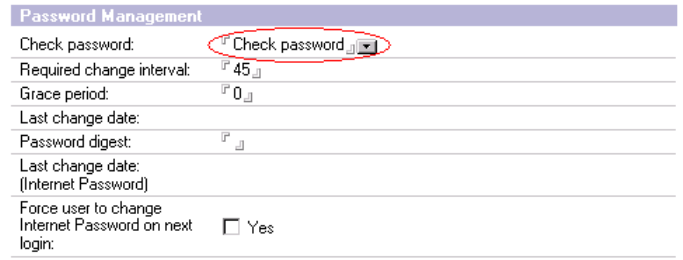


Fig.6

Vous pouvez aussi définir un interval de changement de mot de passe.

C'est également dans cet onglet que vous pouvez désactiver un utilisateur.

Remarque : Si vous faites de la délégation d'administration à plusieurs administrateurs secondaires, uniquement pour des enregistrements d'utilisateurs, nous vous conseillons de ne pas leur donner les mots de passe des ID certificateurs; mais plutôt de migrer vos certificateurs et d'utiliser le CA process. (Voir Nsmag N°3)

2.4 Sécurité de la messagerie

Sécurité d'échange de mail entre utilisateurs

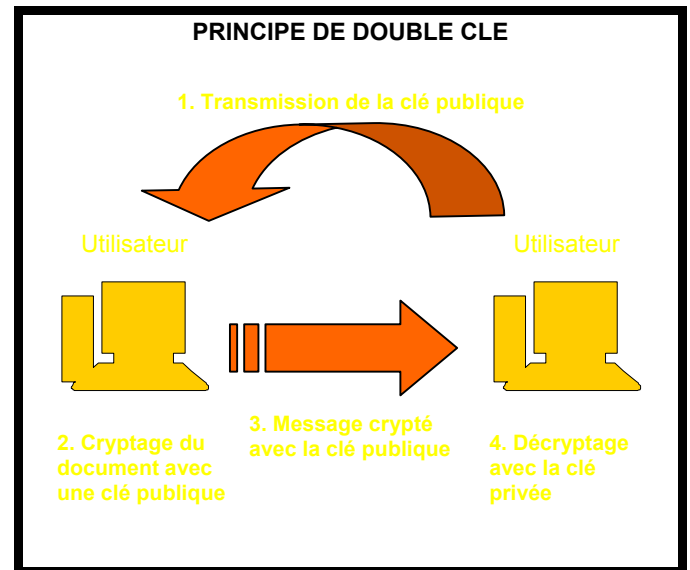


Fig.7

Il est possible d'utiliser le chiffrement du courrier Notes pour chiffrer le courrier envoyé à d'autres utilisateurs Notes, celui provenant d'autres utilisateurs Notes ou tous les documents enregistrés dans une base courrier. Notes utilise la clé publique du destinataire, enregistrée dans l'annuaire Domino ou dans le carnet d'adresses personnel de l'expéditeur, pour chiffrer le courrier en partance et enregistré.

On peut aussi crypter avec une clé simple (dite unique ou secrète) des documents à conserver dans les archives afin de contrôler les personnes qui auront accès à ces documents.

Du point de vue utilisation, le chiffrement d'un message est assez simple. Il suffit d'activer le codage du message dans les modalités d'envoi "menu Options de distribution" et d'employer une signature chiffrée pour se faire "authentifier" par le récepteur si nécessaire. Ces paramètres peuvent être prédefinis par l'utilisateur dans ces préférences de sécurité.

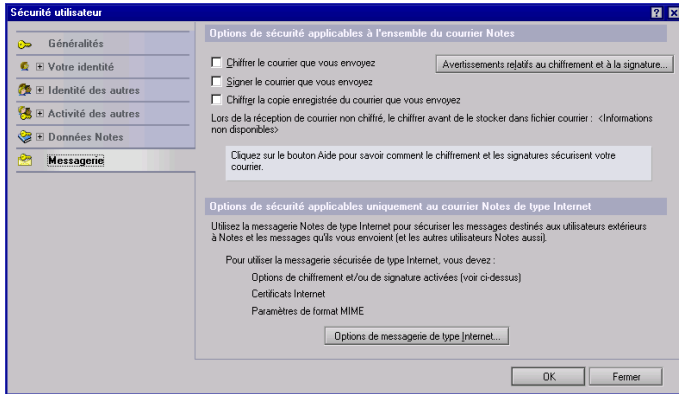


Fig.8

La création de clés personnelles de chiffrement s'effectue aussi à partir de la fenêtre de sécurité utilisateur du client Notes. On peut très facilement les faire parvenir à la personne avec qui l'on souhaite partager ce codage secret. Ces clés personnelles vont servir entre autre à coder les documents que l'on souhaite archiver. Pour cela, il suffit de choisir la clé de chiffrement souhaitée dans le menu " fichier | propriétés du document ".

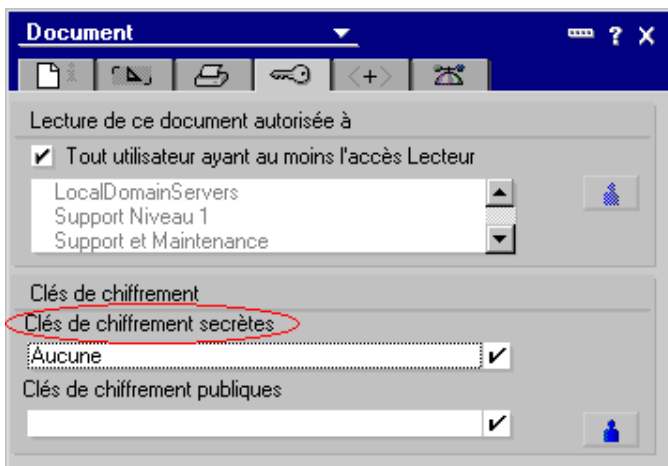


Fig.9

Les différentes clés de chiffrement créées par une personne ou mises à sa disposition sont liées à son fichier ID, d'où la nécessité de le protéger par un mot de passe le plus inviolable possible.

L'accès aux documents chiffrés ne nécessite aucune action particulière dans la mesure où les clés de décodage sont enregistrées dans l'ID de l'utilisateur. Dès que celui-ci ouvre Notes, il doit donner son mot de passe personnel qui fait référence à son ID, et tous les documents cryptés dont il possède la clé pourront être lus.

Les quelques dangers liés au chiffrement :

- Risque de perte des clés (les données seront perdues),
- Risque de perte du fichier ID et du mot de passe (courrier inaccessible),
- Difficultés pour gérer les clés : il faut les distribuer à tous ceux qui en ont besoin.

Sécurité de routage de courriers côté serveur

Pour assurer la sécurité des messages lors des transferts entre clients et serveurs, le serveur de messagerie Domino prend en charge l'authentification par nom et mot de passe, le protocole SSL (Secure Sockets Layer) pour le routage du courrier SMTP, IMAP et les accès POP3, et le chiffrement Notes pour le routage du courrier Notes. Nous venons de parler de ce dernier cas.

Si votre serveur est configuré pour faire du routage SMTP et être à l'écoute vis à vis de l'Internet vous devez absolument le sécuriser. Nous n'allons pas parler ici de l'utilisation de FireWall, proxy.... Mais une grande partie de votre sécurité peut déjà se faire sous Domino. Vous pourrez sécuriser les ports ouverts du serveur Domino, empêcher que votre serveur soit utilisé pour faire du relais par des personnes ou domaines malfaisants, éviter que vos utilisateurs et votre organisation se fassent spamés. Spamming et mailbombing sont aujourd'hui devenus des pratiques du monde internet.

Pour cela nous allons étudier le document de configuration du serveur. Ce document est créé par défaut pour le premier serveur Domino du domaine, mais on peut en créer pour un serveur additionnel.

Nous allons pour cela étudier en partie l'onglet Router/SMTP - Restrictions and controls de ce document.

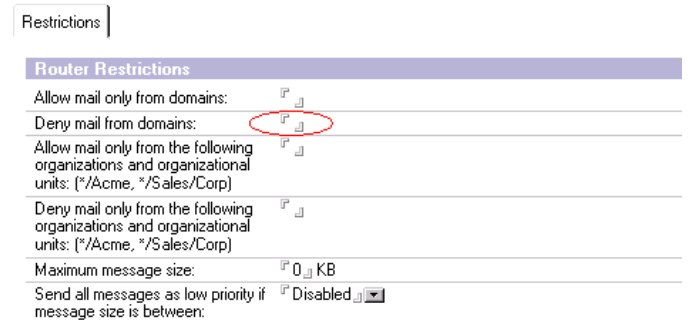


Fig.10

Ici vous pouvez interdire à des domaines spécifiques d'envoyer des mails au votre. Vous pouvez ainsi gérer vous même votre BlackList.

SMTP Inbound Controls

Inbound Relay Controls

Allow messages to be sent only to the following external internet domains:

Deny messages to be sent to the following external internet domains: (* means all) *

Allow messages only from the following internet hosts to be sent to external internet domains:

Deny messages from the following internet hosts to be sent to external internet domains: (* means all)

Inbound Relay Enforcement

Perform Anti-Relay enforcement for these connecting hosts: External hosts

Exclude these connecting hosts from anti-relay checks:

Exceptions for authenticated users: Allow all authenticated users to relay

DNS Blacklist Filters

DNS Blacklist filters: Enabled

DNS Blacklist sites:

Desired action when a connecting host is found in a DNS Blacklist: Log and reject message

Custom SMTP error response for rejected messages:

Inbound Connection Controls

Verify connecting hostname in DNS: Enabled

Fig.11

Le * dans le champ **Deny messages to be sent to following external internet domains** interdit tout relais par votre serveur, même si la traduction pète à confusion.

La zone **DNS Blacklist** permet de contrôler les courriels dont la messagerie internet fait l'objet en ce moment. Par contre l'activation de cette propriété risque de dégrader les performances de votre serveur; car pour chaque connexion SMTP il vérifiera la crédibilité du client ou serveur distant sur un site de liste noire auquel vous vous serez préalablement abonnés.

Dans la section suivante il vous est possible d'interdire à votre organistaion l'envoi de message vers d'autres domaines spécifiques. Et aussi d'interdire à des utilisateurs spécifiques d'envoyer des messages vers Internet.

SMTP Outbound Controls

Outbound Sender Controls

Allow messages only from the following Internet addresses to be sent to the Internet:

Deny messages from the following Internet addresses to be sent to the Internet:

Allow messages only from the following Notes addresses to be sent to the Internet:

Deny messages from the following Notes addresses to be sent to the Internet:

Outbound Recipient Controls

Allow messages only to recipients in the following Internet domains or hostnames:

Deny messages to recipients in the following Internet domains or hostnames:

Fig.12

A ces différents niveaux de sécurité s'ajoute aussi le filtrage et la journalisation des mails en fonction de

critères qui peuvent être basés sur l'expéditeur, le destinataire, le contenu

2.5. Sécurité dans les accès client Internet

Domino peut demander, l'authentification par nom/mot de passe pour inviter les clients Intranet/Internet à entrer leur nom et mot de passe, puis vérifie l'exactitude de ces informations en les comparant à un hachage sécurisé du mot de passe enregistré dans les documents Personne de l'annuaire Domino. Lorsque l'authentification est active, Domino ne demande un nom et un mot de passe qu'au moment où le client Internet/intranet tente d'accéder à une ressource protégée sur le serveur. L'accès Internet/intranet diffère de l'accès des clients Notes et des serveurs Domino par le fait qu'un serveur Domino demande un nom et un mot de passe aux clients Notes ou aux serveurs Domino lors de leur première tentative d'accès au serveur.

L'attribution d'un accès à un client Internet/intranet dans la LCA d'une base de documents va de paire avec la création d'un document Personne pour ce client dans l'annuaire Domino ou, facultativement, dans un annuaire Domino ou LDAP accrédité. Les clients qui ne disposent pas de documents Personne sont considérés comme anonymes et peuvent accéder aux seuls serveurs et bases de documents qui autorisent les accès anonymes.

Vous devez explicitement interdire l'accès anonyme à une ressource en créant dans la LCA une entrée **Anonymous** de type non spécifié.

Une authentification par nom/mot de passe avec TCP/IP ou SSL est possible sur tout serveur qui exécute un protocole Internet (LDAP, POP3, HTTP, SMTP, IIOIP ou IMAP). Pour chaque protocole Internet activé sur le serveur, vous pouvez spécifier la méthode de sécurité. Par exemple, vous pouvez activer l'authentification par certificat client pour les connexions HTTP et l'authentification par nom/mot de passe pour les connexions LDAP qui utilisent TCP/IP. Vous pouvez également choisir d'associer une sécurité par nom/mot de passe à une authentification anonyme et de client SSL, pour permettre aux utilisateurs possédant des certificats de client SSL de s'identifier via une authentification de client SSL, par exemple, tout en autorisant les autres utilisateurs à entrer un nom et un mot de passe s'ils ne disposent pas de certificat de client SSL.

Il suffit pour cela de créer un document de site Internet pour le protocole concerné dans l'onglet configuration de Domino administrator, puis Web et site Internet.

SSL permet :

- Le chiffrement des données transférées entre le serveur Domino et les clients Web,
- La confirmation de la provenance et de la non - falsification des données,
- La signature électronique

Domino peut également faire de l'authentification liée à la session. Ce qui permet de faire du single Sign On (SSO) notamment avec des applications comme Websphere. Elle permet également à un client de quitter sa session sans fermer le navigateur et sans que celle-ci puisse être détournée.

Attention il faut inclure tous vos serveurs participant au Single Sign On dans le document Web SSO configuration que vous créez à cet effet. Il vous faut également définir au niveau du document serveur la prise en compte de l'authentification par session.

2.6 Sécurité du poste client Notes

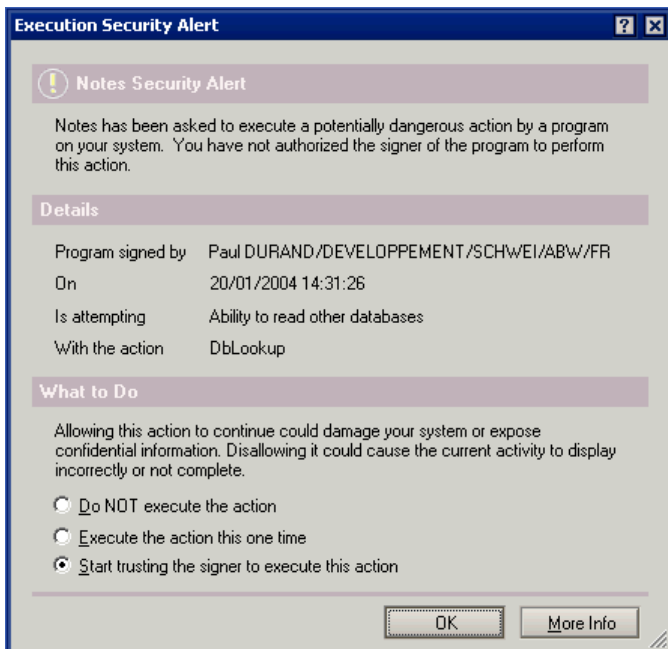
Au niveau de chaque poste de travail, il existe une sécurité supplémentaire : la LCE ou Liste de Contrôle d'Exécution. Chaque utilisateur est responsable pour son poste. Cette liste permet aux utilisateurs de protéger leurs données contre les risques de bombes, virus, etc. La LCE possède un mécanisme pour contrôler l'exécution de fichiers exécutables et leur niveau d'accès. En cas de signataire non accrédité par cette LCE, une notification d'alerte avertit l'utilisateur.

Cette LCE peut être gérée par l'administrateur. On parle de LCE d'administration définie au niveau de l'annuaire et diffusée ensuite aux clients. Les fréquences de mise à jour peuvent être également planifiées. On peut aussi en interdire la modification aux utilisateurs. Nous vous conseillons de gérer la LCE plutôt au niveau du domaine en vous basant sur votre politique de sécurité.

Conclusion

La sécurité doit être tous les jours au cœur du fonctionnement de votre système d'information.

Sa maintenance se fait par le biais des demandes de certification et de la gestion des ID. L'administrateur doit être tenu au courant du départ des personnes afin de détruire ou de bloquer leur ID ou de leur interdire l'accès au serveur. Il peut par ailleurs rappeler aux utilisateurs qu'ils doivent changer régulièrement leur mot de passe afin d'assurer l'étanchéité du système vis à vis de l'extérieur. Il doit penser à étudier les journaux du serveur afin de prévenir des dysfonctionnements (aussi bien les log sur l'activité du serveur que sur les authentifications de clients Internet). Il ne doit pas oublier d'attribuer des serveurs d'administration à ses bases pour une bonne gestion du TurnOver.



Pour cela il vous suffit de créer une policy hiérarchique prenant en compte cette sécurité.