@ Supplément X : Extension du domaine Domino

Ce supplément est conçu pour être utilisé conjointement avec l'ouvrage publié aux éditions Eyrolles :
Lotus Domino 7 Administration

Domino Console. Installer

- **Domino Console**
  - Sur station Windows ou Unix
  - Domino Administrator ou Domino installé
  - Se connecte à Domino Controller
  - Commandes Controller, Domino serveur et natives OS
- **Domino Controller**
  - Tourne sur l'OS – Unix, Windows – du serveur Domino
  - Démarrage et arrêt du serveur Domino à distance
- **Sécurité**
  - Définie dans le document du serveur

La Domino Console est un programme autonome – distinct de Domino Administrator – qui permet de gérer plusieurs serveurs Domino à partir d'une plate-forme Windows ou Unix. Des commandes peuvent être envoyées à un ou plusieurs serveurs Domino et aussi à l'OS sur lequel tournent ces serveurs. Domino Console dialogue avec Domino Controller.

Ce paragraphe aborde les points suivants :

– Rôles de Domino Controller et Domino Console,
– Le fichier admindata.xml,
– Démarrage de Domino Controller,
– Démarrage de Domino Console.

Les fonctions de Domino Console sont vues séparément.

Rôles de Domino Controller et Domino Console

Domino Controller contrôle le démarrage et l'arrêt du serveur Domino local, ainsi que les connexions de Domino Console. Sur un nœud physique sur lequel tourne un serveur Domino, Domino Controller est normalement toujours actif.

Domino Console peut se connecter via le réseau à plusieurs Domino Controllers pour arrêter, démarrer des serveurs Domino à distance, et aussi pour passer des commandes Domino ou à l'OS qui héberge le serveur Domino.

La communication entre Domino Console et Domino Controller se fait sur le port 2050. Ces deux programmes sont écrits en Java et sont apparus en version 6.

Fichier admindata.xml

Domino Controller connaît la configuration du domaine grâce au fichier *\Lotus\Domino\Data\ admindata.xml*. Il contient notamment les identifiants et mots de passe pour se connecter depuis Domino Console.

Il est recommandé de ne pas modifier ce fichier manuellement : Domino se charge d'effectuer une mise à jour – noms d'administrateurs et mots de passe – lorsque c'est nécessaire.

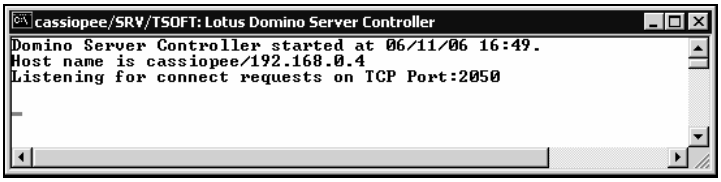
Démarrage de Domino Controller

Domino Controller se démarre en fournissant des paramètres à nserver.exe. Domino Controller peut démarrer immédiatement le serveur Domino et le programme Domino Console en local selon les paramètres fournis.

Paramètres NT	Résultat
nserver	Démarrage standard de Domino Server sans Domino Controller
nserver -jc	Démarrage de Domino Controller, de Domino Console en local, de Domino Server
nserver -jc -c	Démarrage de Domino Controller, de Domino Server
nserver -jc -s	Démarrage de Domino Controller, de Domino Console en local
nserver -jc -c -s	Démarrage de Domino Controller

Sous UNIX, la commande est du type : <*repertoire installation*>*/lotus/bin/server –jc.*

Une fois que Domino Controller est démarré, une fenêtre s'affiche.



L'exemple ci-dessus montre Domino Controller démarré avec la commande *nserver -jc -c –s*. Cette fenêtre devrait être iconisée.

Remarques

Il ne faut pas fermer la fenêtre ou terminer le processus depuis le gestionnaire de tâches. Si la tâche a été arrêtée brutalement, il faut supprimer le fichier .jsc_lock situé dans \Lotus\Domino\Data\.

Lorsque l'OS s'arrête normalement – Démarrer/Arrêter de Windows, par exemple –, la tâche s'arrête proprement. Une commande de Domino Console arrête proprement Domino Controller.

Domino Controller se démarre aussi comme service Windows ↳ Aide de Domino Console.

Démarrage de Domino Console

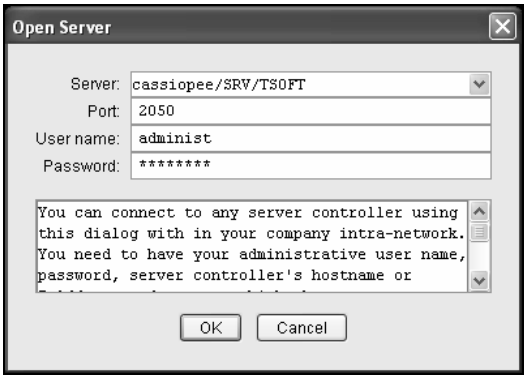
Le programme JConsole.exe – situé dans le répertoire du logiciel \Lotus\Domino\ ou \Lotus\Notes\ – correspond à Domino Console. Le logiciel Lotus Domino – ou Lotus Notes – doit être installé sur la station à partir de laquelle doit être lancé Domino Console. Il n'est pas nécessaire que le serveur Domino ou que le client Notes soient configurés et démarrés.

- Lancer *Lotus\Notes\Jconsole.exe*

La fenêtre de l'application s'affiche. Le programme ne communique avec aucun contrôleur.

Connexion à un Domino Controller

- Commande *File/Open Server*

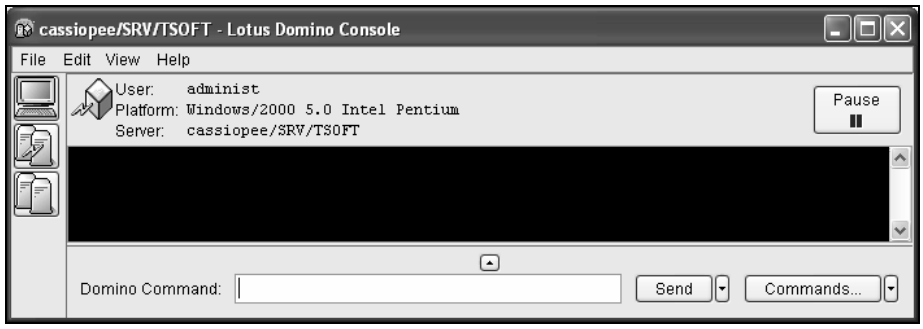


- <User name> : taper le nom abrégé Internet de l'administrateur du serveur Domino visé, ou son nom complet
- <Password> : taper le mot de passe Internet de l'administrateur
- <Server> : taper l'adresse réseau du serveur Domino à atteindre, par exemple : *cassiopee* ou *cassiopee.jfrmlv.fr* ou *192.168.0.4*
- <Port> : conserver 2050

Remarque

Le dialogue *Login Dialog* mémorise tous les noms de serveurs accédés précédemment. La liste déroulante <Server> affiche cette liste des serveurs en retirant tous ceux avec lesquels une connexion est actuellement active.

La connexion s'établit avec Domino Controller et le nom du serveur Domino géré par ce contrôleur s'affiche en haut de la fenêtre Domino Console.

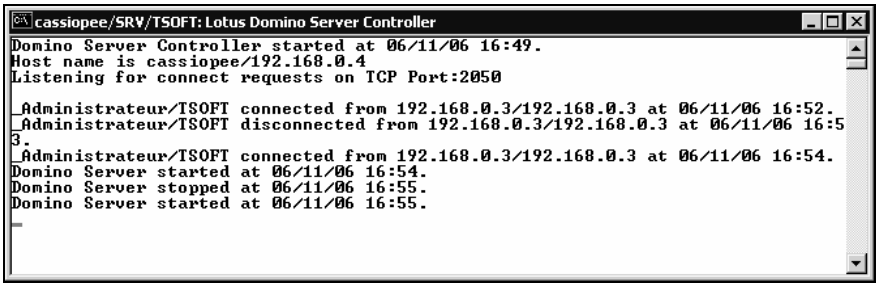


Une fois que la connexion est établie avec Domino Controller, le serveur Domino pourra être arrêté ou démarré ou encore exécuter des commandes.

Démarrage et arrêt de Domino

- Commande *File/Start Server* pour démarrer le serveur Domino sur le nœud
- Commande *File/Stop Server* pour arrêter Domino sur le nœud

La console de Domino Controller affiche l'authentification de l'administrateur depuis Domino Console, ainsi que les arrêts et démarrages du serveur Domino.



La console mode caractères de Domino n'est plus affichée. Il faut passer par Domino Console pour y accéder depuis un poste distant ou en local. Dans la pratique, Domino Console est utilisé sur le serveur local pour remplacer la console par défaut.

Remarque

Il est possible d'envoyer des commandes natives de l'OS dès que la connexion avec Domino Controller est établie et avant de démarrer Domino serveur. L'administrateur vérifie la connectivité réseau par des commandes *ping*, *ipconfig*… par exemple directement depuis Domino Console.

Déconnexion d'un Domino Controller

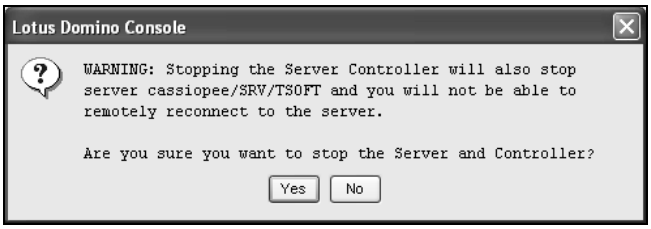
- Commande *File/Disconnect*..., puis cliquer (OK)

Si le serveur Domino tourne sur le nœud, il n'est pas arrêté et continue à fonctionner.

Il faut se reconnecter à Domino Controller avec identifiant et mot de passe pour obtenir à nouveau la console Domino.

Arrêt d'un Domino Controller

- Commande *File/Quit Controller*...



- Cliquer (Yes) pour arrêter le serveur Domino puis Domino Controller. Il ne sera plus possible ensuite d'établir une connexion avec ce nœud
- Cliquer (No), puis commande *File/Disconnect*... s'il s'agit de se déconnecter sans arrêter le serveur Domino
- Utiliser la commande *Quit* sur la console Domino s'il s'agit simplement d'arrêter le serveur Domino sans arrêter le Domino Controller

Domino Console. Commandes

- **Commandes pour le Controller**
  - Connexion et déconnexion du Controller
  - Démarrage et arrêt du serveur Domino
  - Visualisation des processus, des utilisateurs connectés
- **Commandes pour serveur Domino**
  - Toutes les commandes de console Domino
- **Commandes pour l'OS Unix, Windows**
  - Préfixe shell
  - Commandes Windows ou Unix
  - Droit Administrateur système

Les commandes disponibles se répartissent en trois catégories :

– Commandes Domino Controller,
– Commandes natives Domino,
– Commandes natives de l'OS (NT, UNIX).

Les commandes de l'OS sont acceptées si l'utilisateur est administrateur système dans le document du serveur Domino accédé via Domino Controller.

Commandes Domino Controller

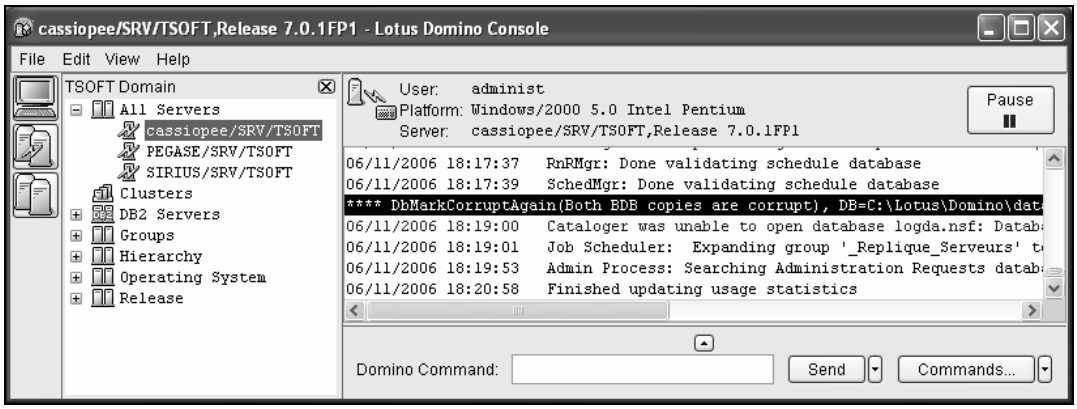
Les options du menu *File* de Domino Console génèrent des commandes envoyées à Domino Controller.

Menu	Résultat
File/Start Server	Démarrage du serveur Domino
File/Stop Server	Arrêt du serveur Domino
File/Kill Server	Arrêt brutal du serveur Domino si l'arrêt contrôlé ne fonctionne pas
File/Quit Controller…	Arrêt du serveur Domino et déconnexion de Domino Controller
File/Refresh Server List	Rafraîchissement de la liste des serveurs du domaine et de leur état – actif, inactif –
File/Local Logging	Journalisation locale dans un fichier texte
File/Show Users	Affichage de la liste des utilisateurs connectés
File /Show Processes	Affichage de la liste des tâches tournant sous contrôle du serveur Domino
File/Broadcast	Envoi d'un message aux utilisateurs

La commande est générée dans la zone de saisie <Domino Command> et peut être affichée en utilisant les flèches de défilement vertical du clavier. Les commandes de Domino Controller sont précédées de #, par exemple : #*start domino*.

#start domino	Démarre Domino serveur
quit	Arrête Domino serveur
#quit	Arrête Domino serveur et se déconnecte de Domino Controller
#enable user	Ferme la session avec Domino pour cet utilisateur jusqu'à ce que Domino Controller s'arrête
#disable user	Autorise l'ouverture de session avec Domino pour cet utilisateur, suite à une commande *disable*
# refresh servers	Rafraîchit la liste des serveurs disponibles
#refresh groups	Rafraîchit la liste des groupes disponibles
#refresh admins	Le serveur Domino met à jour périodiquement les données d'administration. Cette commande force Domino Controller à lire ces données

Commandes natives Domino



- Cliquer (Commands) pour obtenir de l'aide

- Sélectionner une commande puis cliquer (OK)

La commande s'affiche dans la zone de saisie <Domino Command>. Les paramètres obligatoires sont entre crochets ([ ]) et les paramètres optionnels entre les caractères inférieur et supérieur (< >).

- Remplacer le nom des paramètres par les valeurs appropriées
- Cliquer (Send)

Le serveur dont la console est affichée reçoit la commande.

Remarques

Les flèches verticales du clavier font défiler les commandes passées.

Un clic sur la flèche verticale à droite du bouton (Send) donne accès à des fonctions évoluées telles que l'envoi d'une même commande à un groupe de serveurs Domino.

Commandes natives de l'OS

Il est possible d'envoyer des commandes à l'OS sur lequel tourne le serveur Domino.

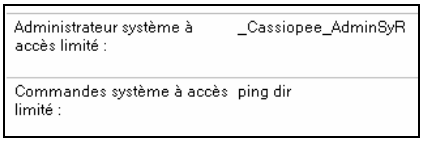
- <Domino Command> : taper
  – UNIX : la commande par exemple *ls *.log*
  – Windows : *shell* ou *she* suivi de la commande, par exemple *she ping sirius*

Droits d'utilisation

L'envoi de commandes à l'OS nécessite le droit Administrateur système ou Administrateur système à accès limité. Cet accès est compris dans Accès total. C'est le droit d'accès de l'identifiant qui a lancé Domino qui est considéré par l'OS.

	Console distante			
Niveau de droit	**Toute commande Domino**	**Commandes Domino consultation**	**Commandes OS**	**Commandes OS accès limité**
Accès total	**X**	**X**	**X**	
Administrateur	**X**	**X**		
Administrateur de bases				
Administrateur de console distante	**X**	**X**		
Administrateur en consultation uniquement		**X**		
Administrateur système			**X**	**X**
Administrateur système à accès limité				**X**

Le champ <Commandes système à accès limité> contient la liste des commandes autorisées pour les administrateurs système à accès limité.

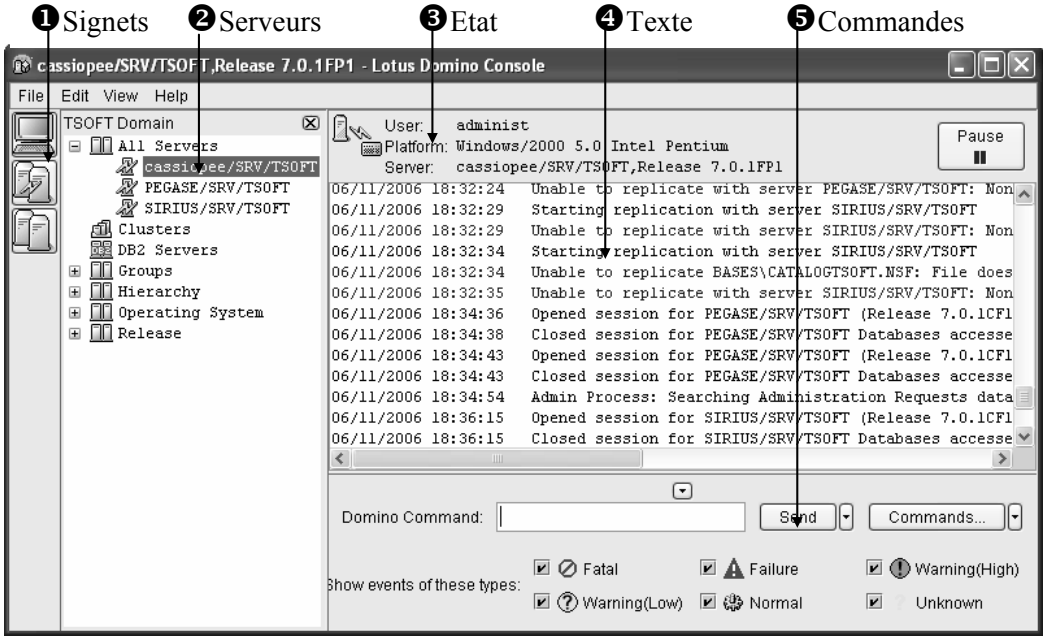


Domino Console. Espace de travail

- **Panneaux**
  - Signets
  - Serveurs
  - Etat
  - Commandes
  - Texte
- **Mise en évidence des messages critiques**
  - Configuration locale ou du serveur Domino
  - Filtres : ne voir que les messages critiques
  - Couleurs : mettre en évidence les messages critiques

L'espace de travail est organisé en panneaux facilitant la gestion de plusieurs serveurs. Les filtres d'événements et le choix des couleurs à l'affichage viennent par défaut de la configuration du serveur Domino ↳La console du serveur Domino. La configuration locale peut être modifiée.

Organisation de l'espace de travail



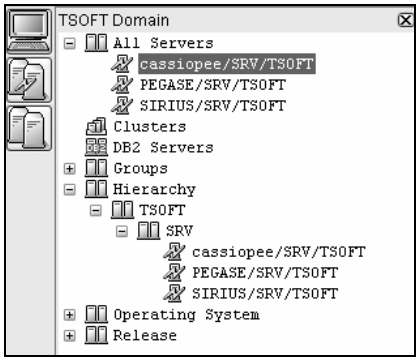
L'espace est organisé en quatre panneaux permanents (panneau de signets, d'état, de commande, de texte) et d'un panneau en option (panneau des serveurs disponibles ou connectés).

Panneau de signets (Bookmark panel)

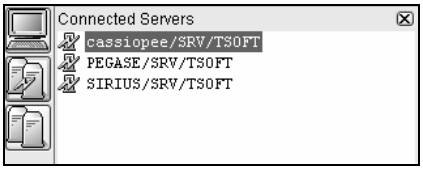
Il est composé de trois icônes :

	Accès au serveur local. Domino Controller tourne sur le même ordinateur.
	Affichage du panneau des serveurs connectés. Ce sont les serveurs pour lesquels une connexion à Domino Controller est en cours.
	Affichage du panneau des serveurs disponibles. Ce sont tous les serveurs du domaine pour lesquels une connexion a été faite.

Panneau des serveurs (Servers panel)



ou



Dans le panneau des serveurs, Domino Console affiche la liste des serveurs connectés ou des serveurs disponibles. L'icône à gauche du nom du serveur donne l'état du serveur.

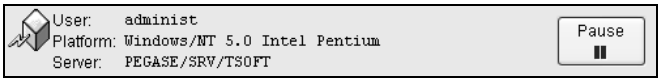
	Serveur distant, connecté, Domino actif
	Serveur local ou distant, Domino non actif

- Cliquer sur le nom du serveur pour afficher son état et la console dans le panneau Texte

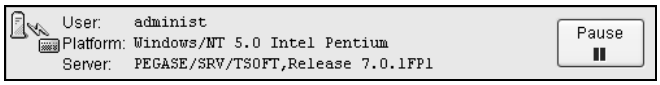
Le dialogue de connexion s'affiche si le Domino Controller n'est pas connecté.

- Clic droit sur le nom du serveur, puis commande
  – *connect* pour se connecter, équivalent de la commande *File/Connect Controller…*
  – *disconnect* pour se déconnecter, équivalent de la commande *File/Disconnect Controller…*
  – *server info* pour afficher un dialogue d'état du serveur

Panneau d'état (Status panel)



Le serveur Domino n'est pas démarré : le panneau Texte est vide.



Le serveur Domino est démarré : le panneau Texte affiche la console de ce serveur.

Panneau de commande (Command panel)

Les commandes à destination de Domino ou de l'OS sont saisies directement ou construites à partir du bouton (Commands…). Le bouton (Send) envoie la commande à un ou des serveurs.

Les commandes passées s'affichent en utilisant les flèches de défilement vertical du clavier.

Panneau Texte (Text panel)

Les messages de la console Domino s'affichent ici à partir de la connexion au Domino Controller correspondant.

Mise en évidence des alertes

La mise en évidence des alertes se fait :

- Par filtre en n'affichant dans le panneau Texte que les messages d'un degré de gravité déterminé,
- En donnant des couleurs différentes aux messages selon le degré de gravité.

Filtre de messages

- Commande *View/Show Ev*ents pour afficher ou masquer les filtres

Ou

- Cliquer sur la flèche verticale du bord supérieur du panneau de commande

Le panneau de filtres s'affiche en dessous du panneau de commandes.

- Sélectionner les messages affichés dans le panneau Texte d'après la gravité voulue

Remarque

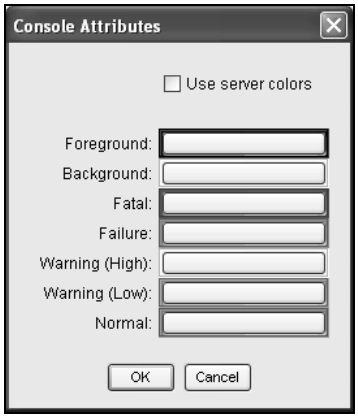
Le filtre des messages par type et niveau de gravité sont également paramétrables au niveau serveur ↳Module Installer le premier serveur – Configuration console distante. L'administrateur indique dans ces filtres ce qui ne doit pas être affiché sur la console de Domino Administrator et de Domino Console.

Le panneau de filtres présenté ici fonctionne comme celui de Domino Administrator et n'est opérationnel que sur le poste sur lequel tourne Domino Console.

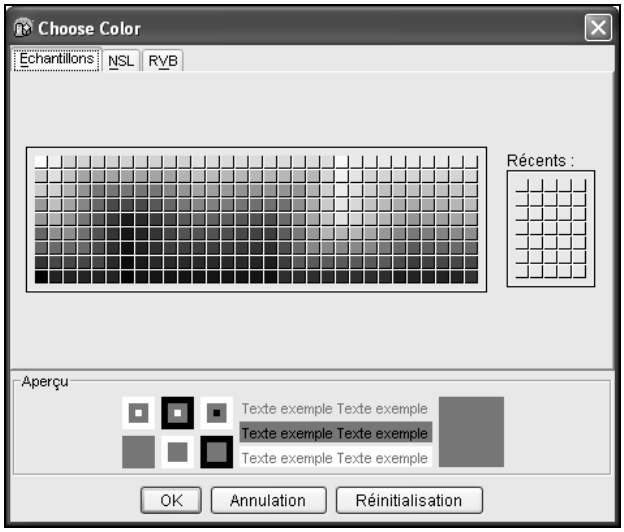
Ce filtre vient après celui défini au niveau serveur et il faut cocher ce qui doit être affiché.

Personnalisation des couleurs

- Commande *Edit*/*Console Attributes*



- Décocher ☐*Use server colors* qui correspond aux couleurs prédéfinies dans le document Console Attributes pour ce serveur
- Cliquer sur une couleur en face d'un texte et sélectionner une autre couleur



- Sélectionner une couleur dans la palette

Exemple de choix de couleurs :

– Warning High, Failure et Fatal : rouge foncé,
– Warning Low : noir,
– Normal : vert foncé.

Remarque

Penser à la lisibilité du texte : noir sur fond blanc est le plus lisible. Il vaut mieux éviter une trop grande variété de couleurs qui complique l'interprétation des messages affichés.

Domino Console. Fonctions avancées

- **Personnaliser des commandes avec des paramètres**
  - Domino Controller et natives OS
  - Domino serveur
- **Travailler avec des groupes de serveurs**
  - Envoi de commandes
  - Exécution planifiée de commandes
- **Journaliser les messages dans des fichiers texte en local**

Domino Console apporte des fonctions permettant de gérer des groupes de serveurs en basculant d'un serveur à l'autre ou en envoyant des groupes de commandes planifiées ou à la demande par exemple. Ces fonctions sont propres à Domino Console.

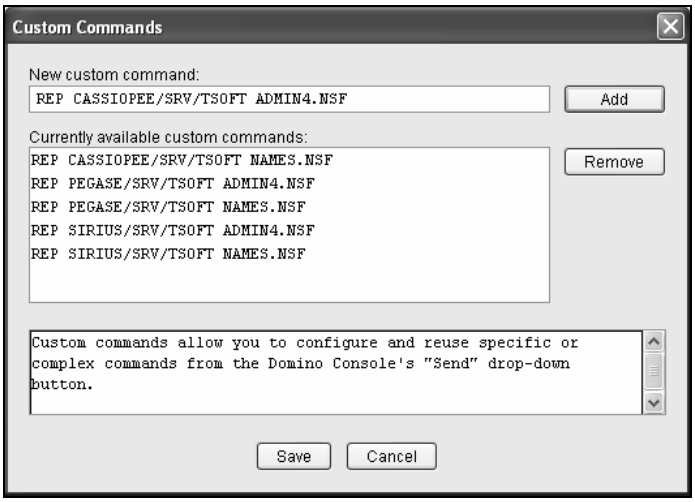
Ce paragraphe aborde les points suivants :

– Commandes personnalisées,
– Création de groupes de serveurs,
– Journalisation.

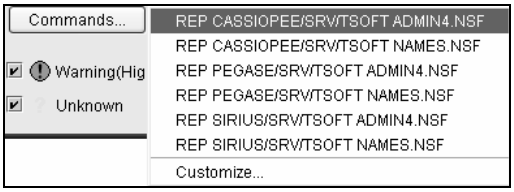
Commandes personnalisées

La commande personnalisée enregistre une commande avec ses paramètres.

	Cliquer sur la flèche, puis commande *Customize…* ou commande *Edit/Custom commands….*



- Taper le texte de la commande, puis cliquer (Add)
- Répéter l'opération pour chaque commande personnalisée
- Cliquer (Save)
- Cliquer sur la flèche à droite du bouton (Commands…)



- Sélectionner une commande

La commande est envoyée dans la zone de saisie de commande.

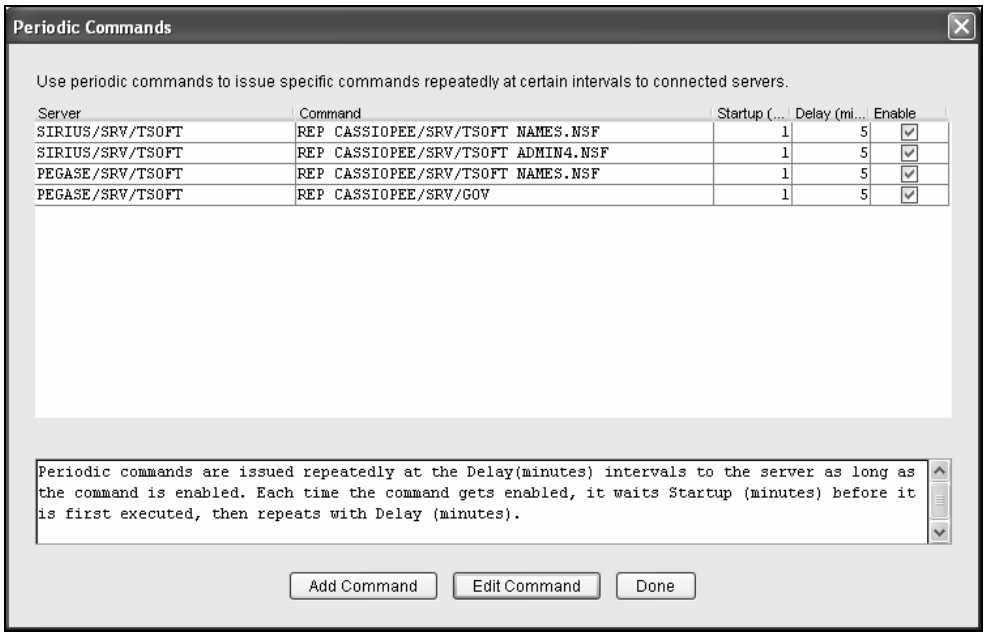
- Cliquer (Send)

Remarque
Les commandes peuvent être aussi des commandes *shell* de l'OS.

Commandes planifiées

Il est possible d'envoyer des commandes à intervalle régulier sur un ou des serveurs.

- Commande *Edit/Periodic Commands…*



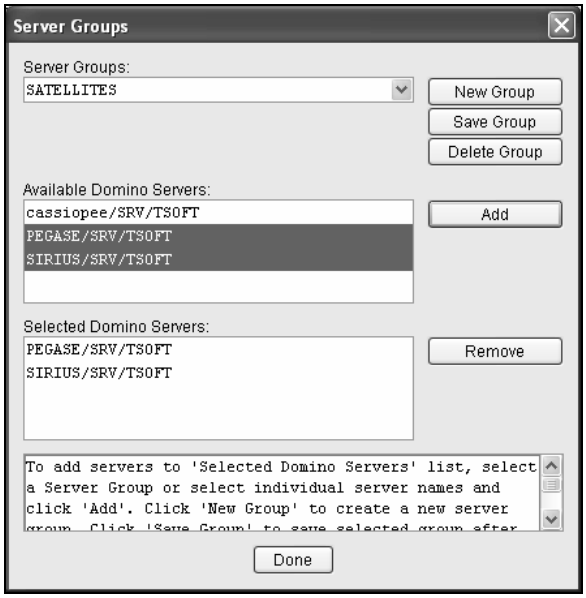
- Cliquer (Add Command)
- <Command> : double-cliquer puis taper la commande Domino ou de l'OS
- <Server> : sélectionner un nom de serveur
- <iDelay(m)> : double-cliquer puis taper le nombre de minutes entre deux exécutions
- <Delay(m)> : double-cliquer puis taper le nombre de minutes
- Cocher ☒*Enabled* pour activer la commande

- Cliquer (Save Command)
- Cliquer (Add Command) et répéter le processus pour une autre commande
- Double-cliquer sur une valeur existante pour la modifier, puis cliquer (Save Command)
- Cliquer (Done) pour terminer

Groupe de serveurs

Domino Console permet l'envoi de commandes à un groupe de serveurs. Ces groupes de serveurs sont créés dans Domino Console et ne correspondent en aucun cas aux groupes de l'annuaire Domino.

- Commande *Edit/Server Groups…*



Créer un groupe

- Cliquer (New Group)

- Taper un nom de groupe, puis cliquer (OK)
- <Server Groups> : sélectionner le groupe qui vient d'être créé
- <Available Domino Servers> : sélectionner un (ou des) serveur(s) en utilisant la touche Ctrl pour sélectionner plusieurs noms
- Cliquer (Add), puis (Save Group)

Modifier un groupe

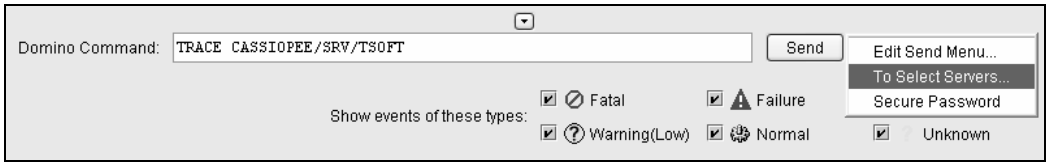
- <Server Groups> : sélectionner le groupe
- Porter les modifications dans le groupe avec les boutons (Add) et (Remove)
- Cliquer (Save Group)

Supprimer un groupe

- <Server Groups> : sélectionner le groupe, puis cliquer (Delete Group)

Envoyer une commande à un groupe

- Taper une commande ou cliquer (Command) et sélectionner une commande personnalisée
- Cliquer sur la flèche à droite de (Send)

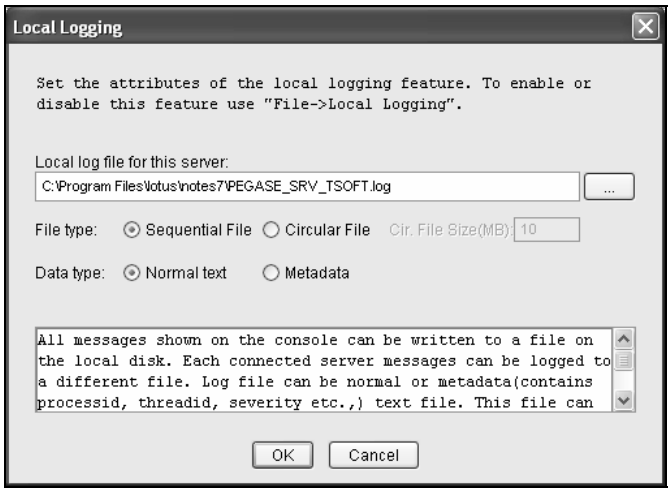


- Cliquer (To Select Servers)
- <Select a Group) : sélectionner un groupe dans la liste déroulante ou en tapant la première lettre de son nom
- Modifier éventuellement le groupe, puis cliquer (Send)

Journalisation

La journalisation se fait localement dans un fichier séquentiel qui peut être revu ultérieurement.

- Commande *Edit/Local Logging*

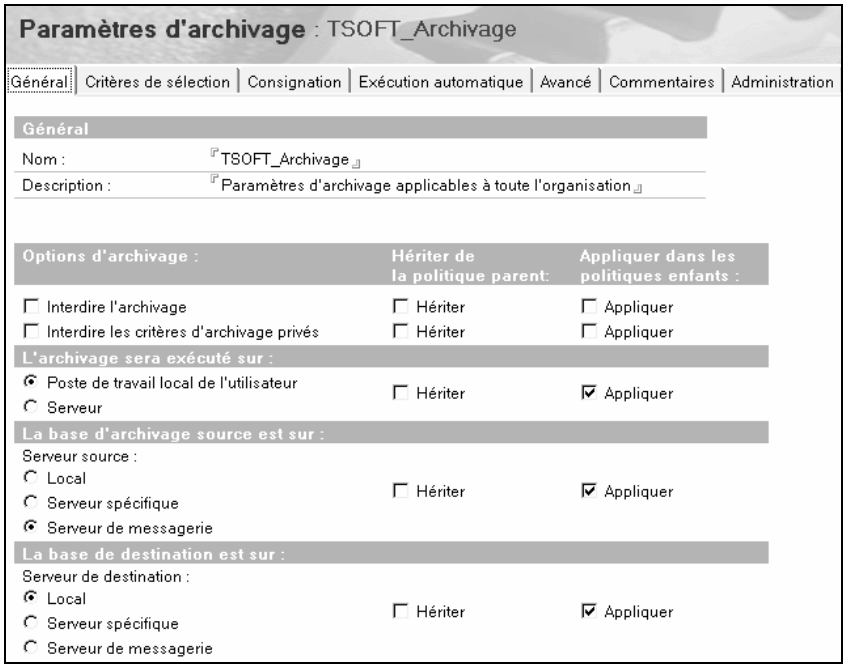


Archivage du courrier sur station

Le scénario proposé consiste à définir une règle applicable à l'ensemble de l'organisation : un archivage minimum de la base Courrier sur serveur vers la base d'archive sur le poste client de documents non modifiés depuis un an. Une politique explicite destinée à des utilisateurs ayant besoin de traçabilité des échanges peut être créée en suivant le même cheminement et des paramètres différents.

Paramètres d'archivage

- Cliquer sur l'onglet (Personnes et groupes), puis cliquer *Paramètres*
- Cliquer (Ajouter paramètres), puis commande *Archivage*

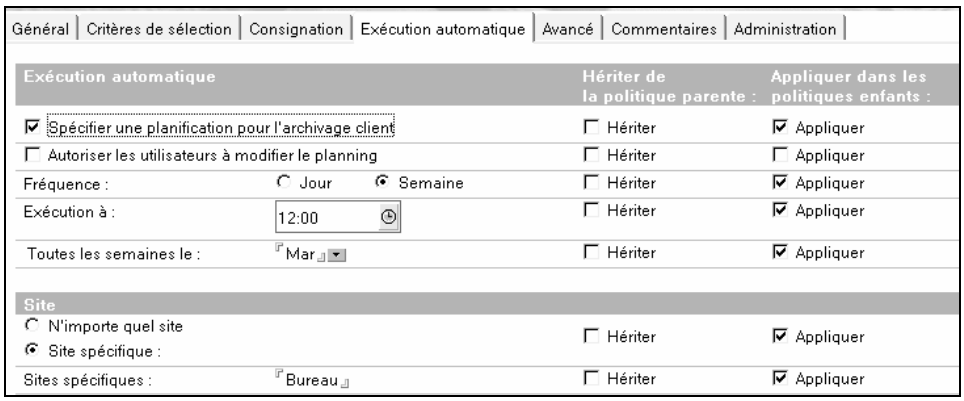


Les paramètres proposés ici vont s'appliquer dynamiquement aux postes installés.

- <L'archivage sera exécuté sur > : sélectionner ❍*Poste de travail local de l'utilisateur*
- <La base d'archivage source est sur> : sélectionner ❍*Serveur de messagerie*
- <La base de destination est sur> : sélectionner ❍*Poste de travail local de l'utilisateur*
- Cocher ☒*Appliquer* pour chacune des options : la règle est valable pour tous
- Cliquer (Consignation)

L'activité d'archivage peut être journalisée dans un journal d'archivage. Cette option n'est pas utilisée dans le scénario.

- Cliquer (Exécution automatique)
- Cocher ☒*Activer l'archivage planifié sur le client*
- <Fréquence> : sélectionner ❍*Jour* ou ❍*Semaine* et sélectionner un jour de la semaine dans <Toutes les semaines le>
- <Exécution à> : sélectionner une heure à laquelle le client Notes est démarré (pas seulement Windows), par exemple *12:00*

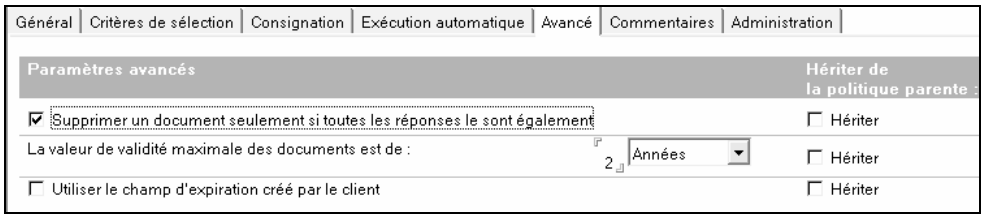


- <Site> : sélectionner ❍*Site spécifique* puis taper *Bureau* pour limiter l'exécution de l'archivage à un poste connecté en LAN sur le serveur de messagerie
- Cocher ☒*Appliquer* pour toutes les options
- Cliquer (Avancé)

Remarque

Les échanges de courrier – un mémo, la réponse au mémo, la réponse à la réponse du mémo… – forment une chaîne de discussion.

Cette représentation est visible dans la vue *Forums* de la base de messagerie.



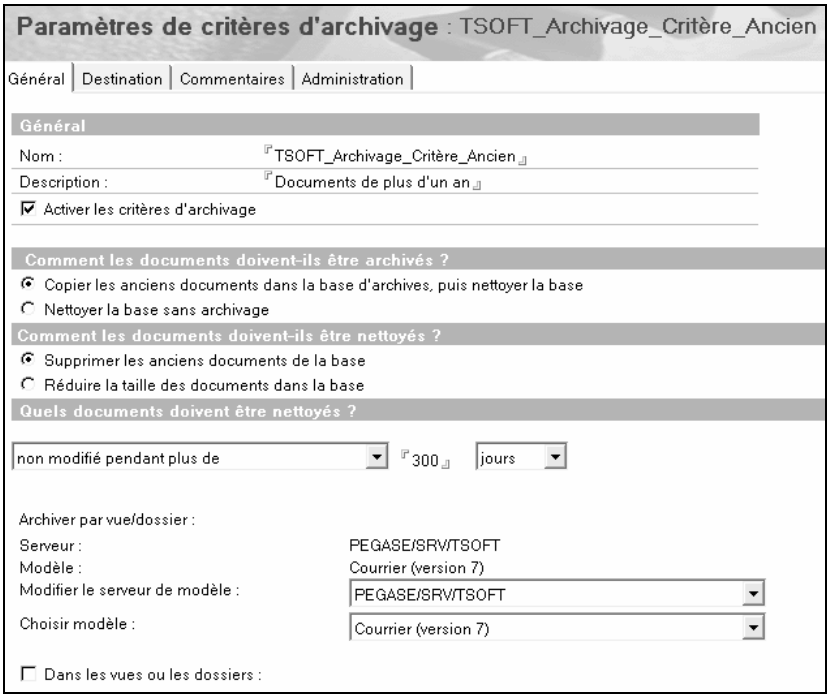
L'option n'est pas cochée par défaut ce qui altère l'intégrité de la chaîne.

- Cocher ☒*Supprimer un document seulement si toutes les réponses le sont également*
- <La valeur de validité maximale des documents est de> : taper *2 Années* pour limiter la conservation complète d'une chaîne de discussion
- Cocher ☒*Appliquer*
- Cliquer (Critères de sélection)

Les critères de sélection sont enregistrés dans un ou plusieurs documents séparés et partagés par des documents de paramètres d'archivage. Ils peuvent être créés puis ajoutés depuis cet onglet ou ajoutés s'ils existent déjà.

- Cliquer (Nouveaux critères)

Paramètres de critères d'archivage



- Cocher ☒*Activer les critères d'archivage* pour qu'ils soient applicables immédiatement. Cette option permet de préparer des critères séparément puis de les activer en bloc après vérification et tests le moment voulu
- <Comment les documents doivent-ils être archivés> : sélectionner ❍*Copier les anciens documents dans la base d'archives puis nettoyer la base* qui correspond au cas le plus fréquent
- <Comment les documents doivent-ils être nettoyés> : sélectionner ❍*Supprimer les anciens documents de la base* qui correspond au cas le plus fréquent

Le nettoyage de la base peut être une réduction de la taille des messages par suppression des fichiers rattachés dont un résumé est conservé ou une suppression des rattachements au-delà de 40 Ko.

Remarque

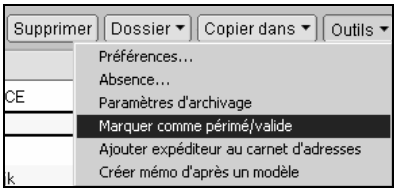
Les fichiers rattachés sont à l'origine du besoin d'archivage du fait qu'ils sont les principaux responsables de la place occupée sur disque. Une étude de la nature des fichiers rattachés en circulation montre que l'on a souvent affaire à deux situations :

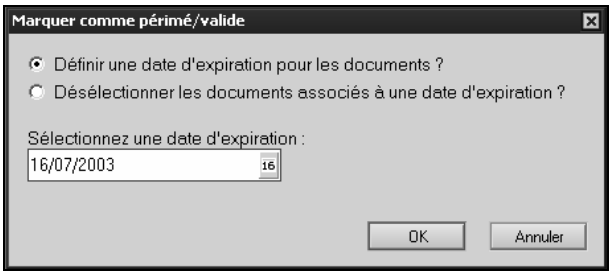
– Diffusion d'information : le fichier rattaché est distribué en multiples copies. Il vaudrait mieux qu'il soit dans une base groupware de type bibliothèque ou kiosque.
– Workflow : le fichier rattaché est révisé par les destinataires puis les révisions sont validées et le résultat diffusé. Il vaudrait mieux qu'un exemplaire unique circule au sein d'une base groupware de type workflow.

L'archivage est une réponse technique à l'occupation de la place disque. Il est largement préférable de penser à l'organisation avant. Ceci simplifie considérablement les critères d'archivage.

- <Quels documents doivent être nettoyés> : sélectionner
  – *auxquels un accès n'a jamais été établi*
  – *non modifiés*
  – *marqués périmés*
- Taper un délai en jours, par exemple *365*

Les documents sont marqués périmés par l'utilisateur qui clique sur (Outils) puis sur la commande *Marquer comme périmé/valide*.





Cette méthode désigne les documents archivables selon des critères personnels de l'utilisateur.

Il est possible de déterminer une règle qui archive les documents non modifiés depuis un an et une autre qui archive les documents marqués comme périmés. Une autre possibilité consiste à archiver les documents présents dans une vue ou un dossier de la base de courrier :

– L'utilisateur classe dans un dossier d'archives les documents voulus. C'est une alternative au marquage comme documents périmés.
– Une vue contient une formule de sélection indiquant quels documents sont archivables. Cette technique est à envisager notamment pour éviter l'archivage des entrées d'agendas : l'utilisateur qui planifie à l'avance des événements et veut conserver un historique de son emploi du temps n'est pas satisfait par un critère d'archivage des documents non modifiés depuis un an.

- Cliquer (Enregistrer et fermer)

Dans le document de paramètres d'archivage :

- Cliquer (Nouveaux critères) pour créer un autre critère d'archivage
- Cliquer (Ajouter critères), puis sélectionner le ou les critères

Le document de paramètres d'archivage est rattaché à une politique subordonnée à l'organisation ou à une unité d'organisation, ou encore à une politique explicite si elle s'applique à un groupe d'utilisateurs.

Migration vers un annuaire de configuration

- **Modifier les paramètres de réplication names.nsf sur le serveur Annuaire de configuration**
- **Répliquer names.nsf avec un serveur Annuaire principal : documents Personnes, Groupes, Bases courrier en arrivée supprimés**
- **Redémarrer le serveur Annuaire de configuration**
- **Requête administrative de mise à jour du document serveur Annuaire de configuration**
- **Commande *SHOW XDIR* : affiche le serveur Annuaire principal**

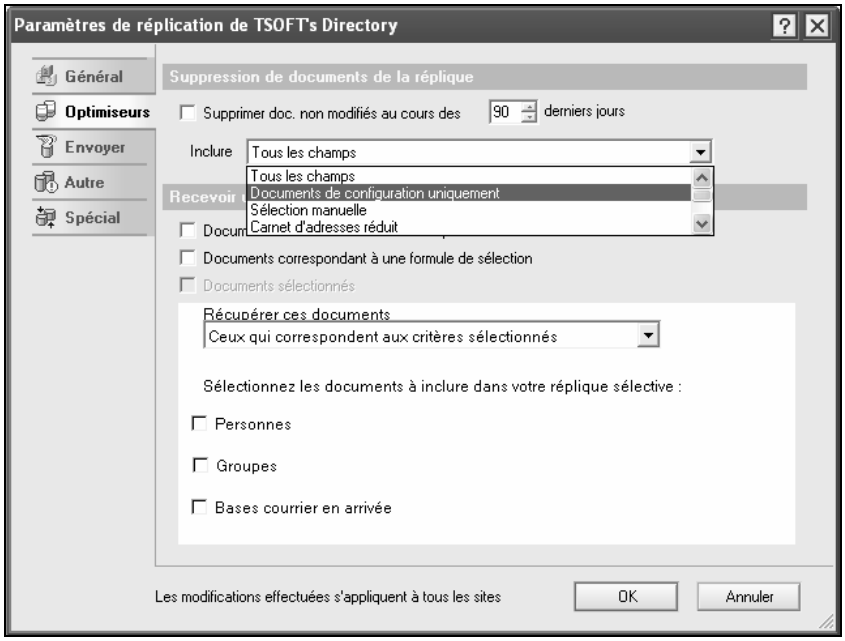
```
show xdir

  DomainName    DirectoryType        ClientProtocol Replica/LDAP Server
  ----------    -------------        ---------- -------------------------
1 TSOFT         Configuration-Notes  Notes      names.nsf
2 TSOFT         Remote Primary-Notes Notes & LDAP SIRIUS/SRV/TSOFT!!names.nsf
```

La migration d'un annuaire consiste à modifier un paramètre de réplication de l'annuaire puis à lancer une réplication de l'annuaire.

Paramètres de réplication

- Sélectionner le futur serveur de configuration depuis Domino Administrator
- Cliquer sur l'onglet (Fichiers)
- Clic droit sur *names.nsf*, puis commande *Propriétés*…
- Cliquer (Paramètres de réplication), puis cliquer (Optimiseurs)



- <Inclure> : sélectionner *Documents de configuration uniquement*

Remarque

Il ne faut pas confondre Documents de configuration uniquement avec Carnet d'adresses réduit qui ne concerne que des postes clients en version 4.x le plus souvent.

- Cliquer (OK), puis fermer le dialogue des propriétés de la base

Réplication de l'annuaire

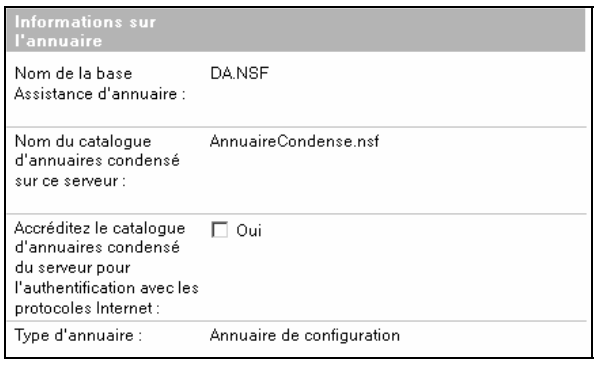
- Cliquer sur l'onglet (Serveur), puis (Etat), puis *Tâches serveur*
- Cliquer (Outils), puis (Serveur), puis commande *Répliquer*...

- <Répliquer avec le serveur> : sélectionner le serveur Annuaire principal, ici *CASSIOPEE/SRV/TSOFT*
- <Style de réplication> : sélectionner *Envoyer Répliquer* ou *Répliquer*
- <Répliquer> : sélectionner ❍*Base sélectionnée*
- Cliquer (Base de documents…)
- Sélectionner l'annuaire du domaine, ici *TSOFT'Directory names.nsf*
- Cliquer (OK), puis (Répliquer), puis (Quitter)

La commande est envoyée sur le serveur de configuration.

- Cliquer (Outils), puis (Serveur) puis commande *Redémarrer*...

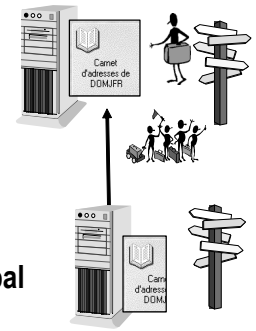
Le serveur est passé à l'état serveur de configuration. Une requête administrative se charge de mettre à jour – sur le serveur d'administration de l'annuaire – le document du serveur pour refléter cette situation.

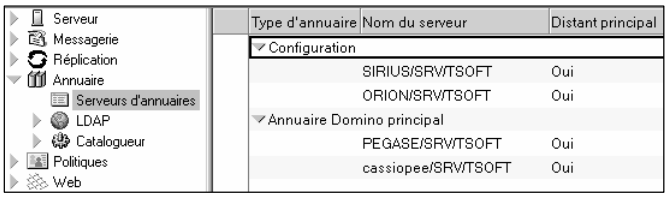


La commande `show xdir` sur la console du serveur Domino de configuration affiche le serveur d'annuaire principal recherché par celui-ci.

Accès à l'annuaire Domino principal

- **Accès aux documents de personnes et de groupes**
  - Authentification des utilisateurs, LCA
  - Routage de courrier
- **Identification de l'annuaire Domino principal**
  - Automatique
  - Dirigée via l'assistance d'annuaire





Le serveur hébergeant un annuaire de configuration doit accéder à des documents de personnes, de groupes, de bases Courrier en arrivée et de ressources pour :

- Authentifier un utilisateur qui se connecte,
- Interpréter les droits d'un utilisateur d'après les groupes inscrits dans la LCA,
- Envoyer du courrier à une personne, un groupe, une base de workflow,
- Accéder aux disponibilités.

L'identification d'un serveur hébergeant un annuaire principal est :

- Automatique : par défaut,
- Imposée avec l'assistance d'annuaire qui contient les liens vers les annuaires à utiliser,
- Inutilisée : un catalogue d'annuaires local contient les personnes, groupes, bases Courrier en arrivée.

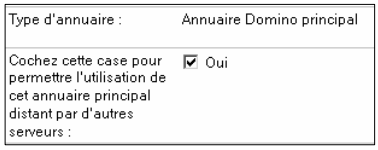
Recherche automatique d'un annuaire central

Les vues *Serveurs d'annuaires* et *($Directories)* listent les serveurs du domaine hébergeant un annuaire central. Le serveur d'annuaire de configuration identifie un annuaire central comme suit :

- Recherche dans l'historique de réplication de l'annuaire du serveur à partir duquel l'annuaire a répliqué, de la réplication la plus récente à la plus ancienne,
- Si la liste construite contient moins de cinq serveurs, recherche dans l'annuaire local les serveurs hébergeant un annuaire central et appartenant au même réseau nommé Domino,
- Si la liste contient moins de cinq serveurs, recherche dans la vue *($Directories)* classée par ordre alphabétique des noms de serveurs.
- La liste étant construite, le serveur cherche à accéder au premier serveur de la liste, puis au suivant jusqu'à ce qu'une connexion soit établie.

Accès dirigé par assistance d'annuaire

- **Créer Assistance d'annuaire sur le serveur Annuaire de configuration (da50.ntf)**
- **Créer un document pour le domaine Domino**
- **Modifier le document serveur**
- **Modifier les documents serveurs d'annuaire principal : décocher *Permettre l'utilisation de cet annuaire principal distant par d'autres serveurs***
- **Arrêter et démarrer le serveur**
- **Commande *SHOW XDIR***

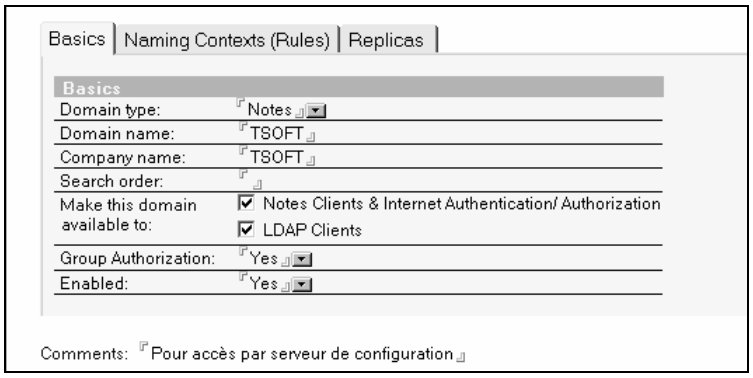


L'assistance d'annuaire est utilisée habituellement pour référencer des annuaires secondaires Domino ou LDAP. Elle est utilisée ici pour forcer un serveur de configuration à accéder à l'annuaire principal sur des serveurs déterminés. La base étant déjà créée sur le serveur de configuration – ↳ Assistance d'annuaire –, il faut procéder en deux temps :

– Créer un document pour l'annuaire Domino du domaine,
– Interdire l'accès automatique aux serveurs d'annuaire principal (option).

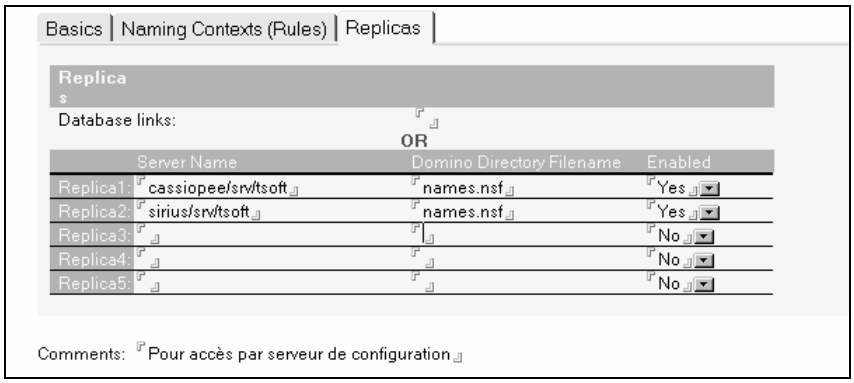
Document Directory Assistance pour names.nsf

- Cliquer sur l'onglet (Configuration), puis *Annuaire*, puis *Assistance d'annuaire*
- Cliquer (Add Directory Assistance)



- <Domain type> : laisser *Notes*
- <Domain name> : taper le nom du domaine Domino, par exemple *TSOFT*
- <Company name> : taper un texte, ce champ étant obligatoire

- <Group Authorization> : sélectionner *Yes* si ☒*LDAP Clients* est coché et que l'expansion des groupes pour un accès LDAP est requise
- Cliquer sur l'onglet (Replicas)



- <Server Name> : taper le nom du serveur principal d'annuaire accédé en priorité, ici *cassiopee/srv/tsoft*
- <Domino Directory Filename> : taper *names.nsf*
- <Enabled> : sélectionner *Yes*
- Taper le nom du serveur principal d'annuaire accédé si le premier ne répond pas sur la deuxième ligne, ici *sirius/srv/tsoft*
- Taper *names.nsf* et sélectionner *Yes* sur la deuxième ligne
- Continuer s'il y a d'autres serveurs de secours
- Cliquer (Save & Close), puis redémarrer le serveur

Vérification

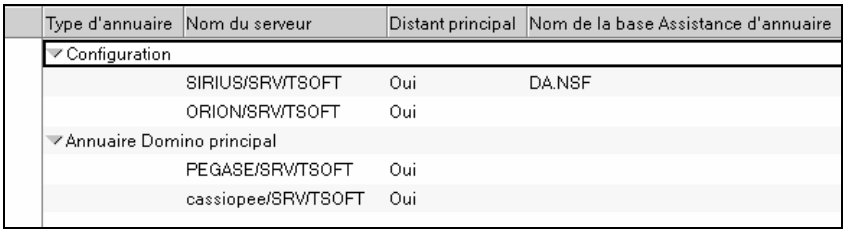
- Ouvrir la console du serveur de configuration, puis taper la commande *show xdir*

```
show xdir
DomainName DirectoryType ClientProtocol Replica/LDAP Server

1 TSOFT Configuration-Notes   Notes          names.nsf
2 TSOFT Remote Primary-Notes  Notes & LDAP
cassiopee/SRV/TSOFT!!names.nsf
Directory Assistance Database 'DA.NSF' in use
```

L'affichage indique le serveur d'annuaire principal qui est accédé.

- Cliquer sur l'onglet (Configuration), puis *Annuaire*, puis *Serveurs d'annuaires*

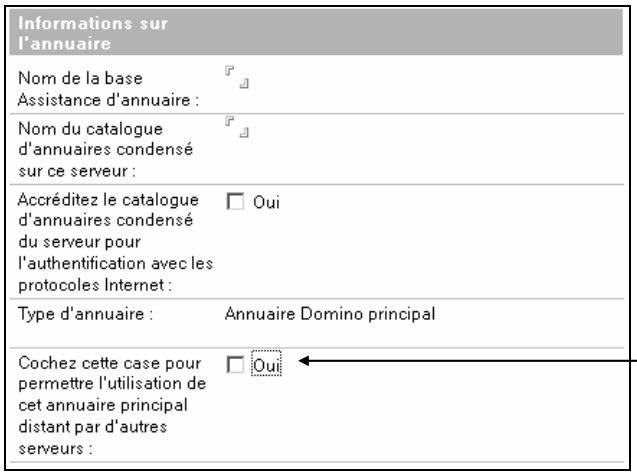


La vue reflète la nouvelle situation. Le serveur accédé – ici *cassiopee/srv/tsoft* – peut aussi être accédé par un serveur de configuration sans assistance d'annuaire.

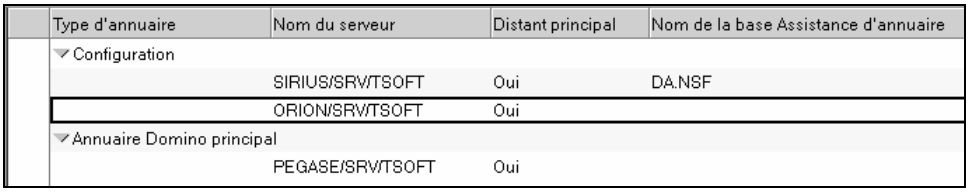
Interdire l'accès automatique

Tous les serveurs de configuration accèdent à un serveur principal d'annuaire déterminé par l'assistance d'annuaire. L'accès automatique n'est normalement pas mis en jeu. Pour l'interdire :

- Modifier le document serveur du serveur principal d'annuaire qu'il s'agit de restreindre, ici *cassiopee/srv/tsoft*
- Cliquer sur l'onglet (Général)



- <Utilisation de cet annuaire principal distant par d'autres serveurs> : décocher ☐*Oui*
- Redémarrer le serveur
- Cliquer sur l'onglet (Configuration), puis *Annuaire*, puis *Serveurs d'annuaires*



Type d'annuaire	Nom du serveur	Distant principal	Nom de la base Assistance d'annuaire
Configuration			
	SIRIUS/SRV/TSOFT	Oui	DA.NSF
	ORION/SRV/TSOFT	Oui	
Annuaire Domino principal			
	PEGASE/SRV/TSOFT	Oui	

– Le serveur *cassiopee/srv/tsoft* n'apparaît plus dans la vue dans la catégorie Annuaire Domino principal.
– Le serveur de configuration *sirius/srv/tsoft* accède à *cassiopee/srv/tsoft* du fait que ce dernier est documenté dans la base d'assistance d'annuaire DA.nsf.
– Le serveur de configuration *orion/srv/tsoft* accède au serveur d'annuaire principal *pegase/srv/tsoft* parce qu'il n'a pas d'assistance d'annuaire qui lui impose un serveur et qu'il n'y a qu'un seul serveur d'annuaire principal en accès automatique.

Catalogue d'annuaires condensé sur serveur de configuration

- **Le catalogue d'annuaires est accédé pour**
  - Les noms de personnes et les noms de groupes (messagerie, LCA…)
- **Créer un catalogue d'annuaires sur un serveur d'annuaire principal**
- **Activer la tâche Directory Cataloger**
- **Répliquer sur le serveur d'annuaire de configuration**
- **Mettre à jour les documents serveurs correspondants**
- **Activer la réplication périodique**
- **Arrêter et démarrer les serveurs d'annuaire de configuration**

Le catalogue d'annuaires est une forme condensée de l'annuaire (ou de plusieurs annuaires) contenant les personnes et les groupes. Cette technique ramène les personnes et les groupes sur le serveur de configuration: c'est un compromis entre l'accès réseau à un serveur d'annuaire principal et la place disque.

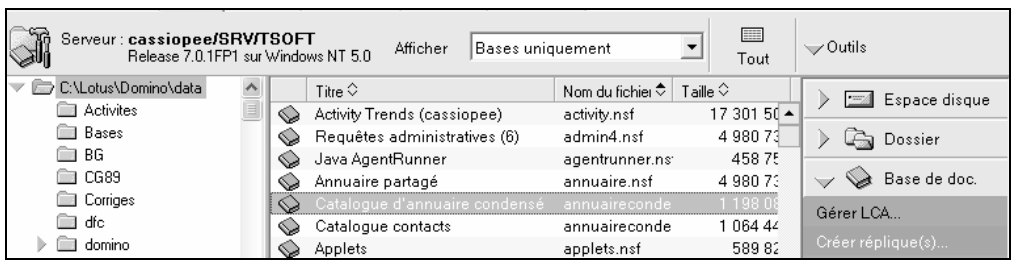
Le catalogue d'annuaires condensé est déjà mis en place sur le serveur d'administration de l'annuaire Domino – ↳Catalogue d'annuaires condensé –. Il faut procéder en trois étapes :

– Créer une réplique du catalogue d'annuaires condensé sur le serveur de configuration,
– Activer la réplication périodique du catalogue d'annuaires condensé,
– Porter le nom du catalogue d'annuaires condensé dans le document du serveur de configuration et vérifier le résultat.

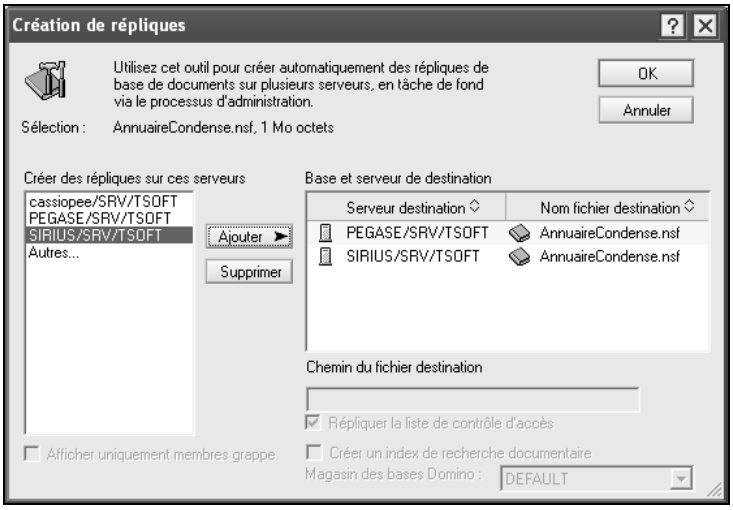
Créer une réplique du catalogue

La création de répliques est détaillée dans ↳Module Gérer les bases d'applications.

- Se connecter sur le serveur d'administration de l'annuaire Domino *CASSIOPE/SRV/TSOFT,* qui entretient le catalogue d'annuaires condensé
- Cliquer sur l'onglet (Fichiers)



- Sélectionner la base Catalogue d'annuaires condensés, ici *AnnuaireCondense.nsf*
- Cliquer (Outils), puis (Base de doc.), puis commande *Créer réplique(s)…*



- Sélectionner le serveur de configuration dans le panneau de gauche, puis cliquer (Ajouter), puis cliquer (OK)

Une requête est soumise dans Requêtes Administratives (6). Le suivi de cette requête aboutissant à la création de la réplique est détaillé dans ↳Module Gérer les bases d'applications. Créer une réplique de la base sur le serveur de configuration

Activer la réplication planifiée

Une solution consiste à répliquer le catalogue d'annuaires condensé en même temps que l'annuaire Domino. S'il n'y a pas eu de modification dans la base Catalogue, le temps de réplication n'est pas allongé de façon significative.

- Cliquer sur l'onglet (Configuration), puis *Serveur*, puis *Connexions*
- Modifier le document de réplication de l'annuaire entre serveur de configuration et serveur d'annuaire principal

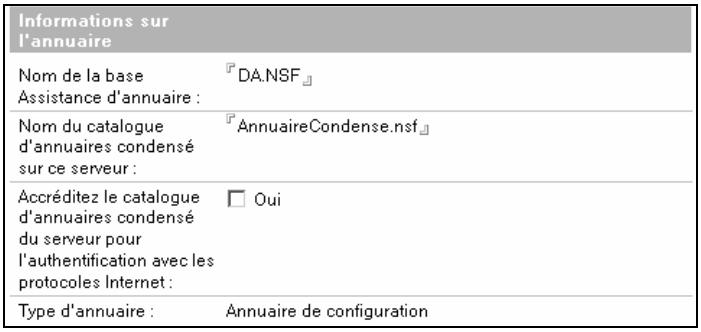
Si l'architecture pivot-satellite n'est pas en place – ce qui est normalement le cas actuellement – la réplication est initialisée depuis chaque serveur additionnel (source) vers le serveur d'administration de l'annuaire Domino (cible). Le serveur qui initialise la réplication n'a pas vraiment d'importance par rapport à notre propos actuel : l'important est que le catalogue d'annuaires condensé réplique. Les indications données sont uniquement destinées à vous aider à vous y retrouver.

- Modifier le document, puis cliquer sur l'onglet (Réplication routage)

- <Chemins des fichiers/répertoires à répliquer> : ajouter *AnnuaireCondense.nsf* après *names.nsf;admin4.nsf ;events4.nsf* en utilisant le séparateur point-virgule (;)
- Cliquer (Enregistrer et fermer)

Modifier le document serveur

- Modifier le document du serveur de configuration



- <Nom du catalogue d'annuaires condensé sur ce serveur> : taper le nom de la réplique qui a été créée sur le serveur, ici *AnnuaireCondense.nsf*
- Redémarrer le serveur Domino de configuration

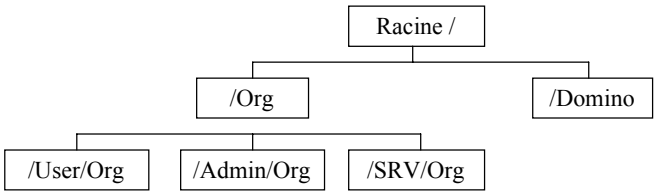
Vérification

- Ouvrir la console du serveur de configuration, puis taper la commande

```
> show xdir
DomainName DirectoryType ClientProtocol Replica/LDAP Server
1 TSOFT Configuration-Notes   Notes     names.nsf
2 TSOFT Remote Primary-Notes  Notes & LDAP
cassiopee/SRV/TSOFT!!names.nsf
Directory Catalog 'AnnuaireCondense.nsf' in use
Directory Assistance Database 'DA.NSF' in use
```

Le catalogue d'annuaires condensé sera utilisé pour les recherches de personnes et de groupes. Le serveur d'annuaire principal reste disponible si une entrée n'est pas trouvée.

LCA étendue. Exemples



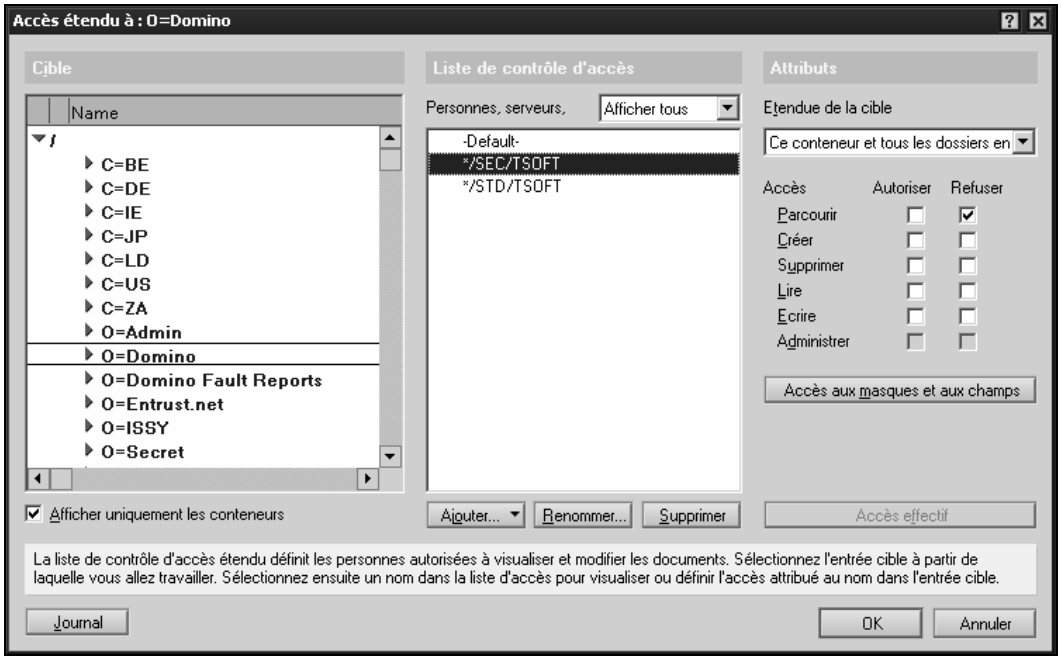
- **Cible : /Domino**
  - Sujet : /User/Org. Pas de visibilité
- **Cible : /SRV/Org**
  - Sujet : /Org. Pas de modification
  - Sujet /Admin/Org. Modification autorisée
- **Cible : /User/Org. Masque Person. Champ HTTPPassword**
  - Sujet : /Usr/Org. Pas de modification

Deux scénarios sont déroulés :

– Les utilisateurs de /User/Org ne voient pas les documents appartenant à l'espace de nom /Domino,
– Les utilisateurs de /User ne peuvent pas modifier le champ HTTPPassword du masque Person, même s'ils sont auteurs sur leur document (défaut dans l'annuaire).

- Afficher la LCA de l'annuaire
- Cliquer sur (Accès étendu)

Si le bouton (Accès étendu) est grisé, c'est que l'étape d'activation de l'accès étendu n'est pas allée à terme.



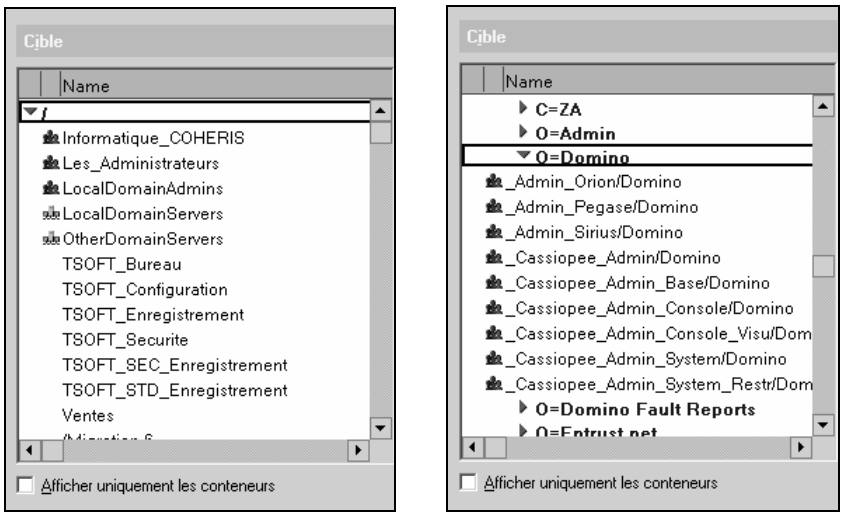
Cible

- <Cible> : sélectionner la catégorie de documents à protéger

Les documents Personnes, Serveurs, Connexions… sont catégorisés dans les vues parce que les noms sont hiérarchiques et contiennent le caractère /. Il y a des règles précises qui sont observées selon les documents. Par exemple c'est le contenu du champ *Nom complet* qui est pris en compte pour une personne, le contenu du champ *Nom serveur* pour celui d'un serveur.

Lorsqu'un document porte un nom hiérarchique – qui comprend des /, par exemple, le groupe *Administrateurs_Serveur/Domino* –, il est rattaché à une catégorie elle-même rattachée à la racine / – par exemple, /Domino –. Un document non catégorisé (nom à plat sans structure hiérarchique) apparaît directement dans la racine.

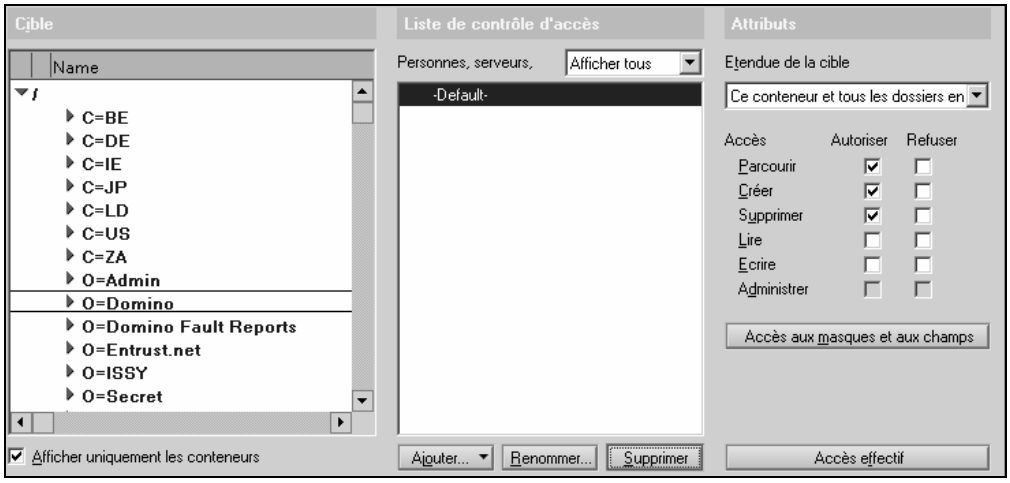
Pour voir les documents rattachés à une catégorie :



- Décocher ☐*Afficher uniquement les conteneurs*

Sujet

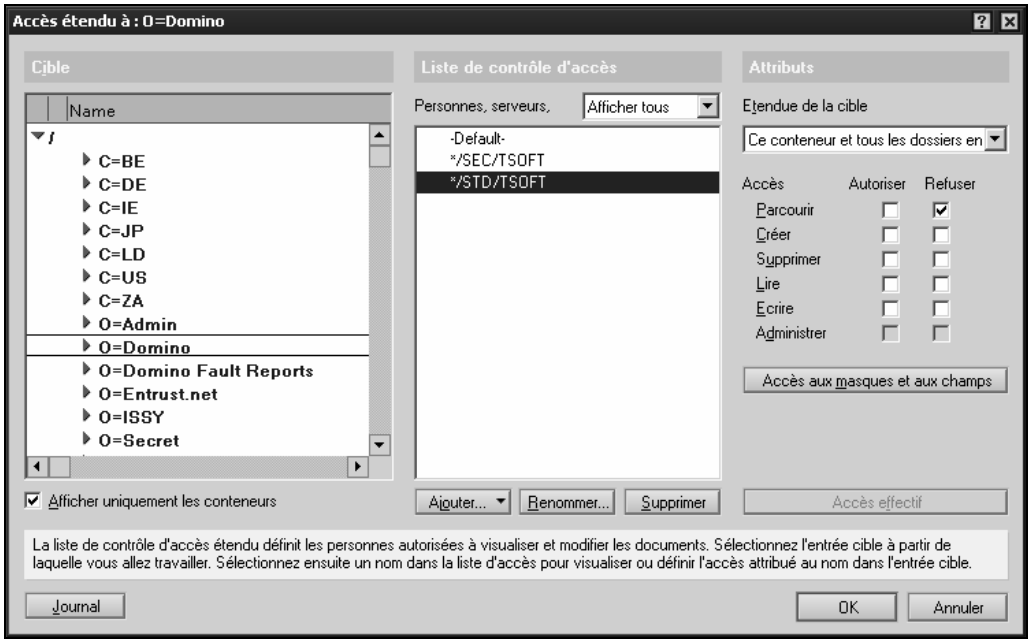
La cible étant identifiée, le sujet – celui ou ceux auxquels s'appliquent les restrictions – est sélectionné.



- <Liste de contrôle d'accès> : cliquer (Ajouter)
- Sélectionner *-Default-*
- <Attributs><Etendue de la cible> : sélectionner *Ce conteneur et tous les dossiers enfants* pour que la règle s'applique à des catégories dépendant de la cible choisie, par exemple /Pers/Domino

La règle à mettre en place est que *par défaut*, les droits de la LCA ne sont pas restreints. Il faut alors cocher toutes les cases *Autoriser*. Le fait de cocher ☒*Créer* ne donnera pas à un utilisateur qui est Lecteur sur l'annuaire le droit de créer des documents. Si un utilisateur est Auteur avec le privilège ☒*Créer des documents*, son droit est conservé.

Les accès *Lire* et *Ecrire* s'appliquent aux entrées d'annuaires LDAP.



- <Liste de contrôle d'accès> : cliquer (Ajouter)
- Sélectionner Nom…, puis taper **/SEC/TSOFT*
- <Parcourir> : cocher <☒*Refuser* pour que les utilisateurs ne puissent pas voir les documents dans une vue
- Répéter l'opération avec **/STD/TSOFT*

Remarque

Les restrictions s'appliquent à un couple Sujet-Cible, la cible étant un ensemble de documents appartenant à une catégorie. La cible ne peut pas être un document.

Lorsque la cible est un niveau donné sans les enfants – par exemple /TSOFT dont les enfants sont /SEC/TSOFT, /STD/TSOFT, /SRV/TSOFT – alors :

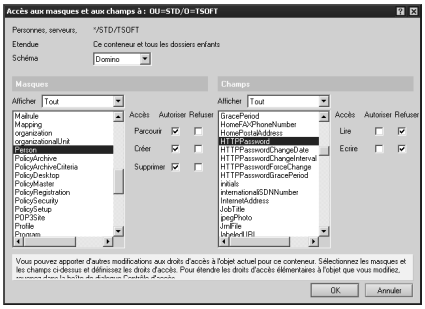
- <Etendue de la cible> : sélectionner *Ce conteneur uniquement*

Administration Requests et LCA étendue

La granularité de l'accès en modification à l'annuaire Domino du domaine peut être étendue aux serveurs : au lieu de concentrer les modifications de l'annuaire par *Administration Requests* sur un seul serveur, plusieurs serveurs vont se partager la tâche, chacun ne traitant qu'une portion – un espace nom déterminé – de l'annuaire. Cette option prend tout son sens lorsque des milliers de documents de Administration Requests répliquent entre quelques centaines de serveurs dans le monde : la remontée vers un seul serveur pour traitement crée des goulets d'étranglement.

LCA étendue. Accès

- **Parcourir : lire le nom hiérarchique du document ou de l'entrée LDAP dans une vue**
- **Créer, écrire, supprimer, lire : un document, une entrée LDAP**
- **Administrer : si le sujet est**
  - Utilisateur Web ou Notes, Editeur ou Concepteur : il peut modifier des accès dans la LCA étendue
  - Un serveur d'administration – adminp – pour les documents cibles



Les restrictions ont été appliquées au niveau des documents. Il est possible d'autoriser la lecture globalement sur un document et de la refuser sur un champ en particulier.

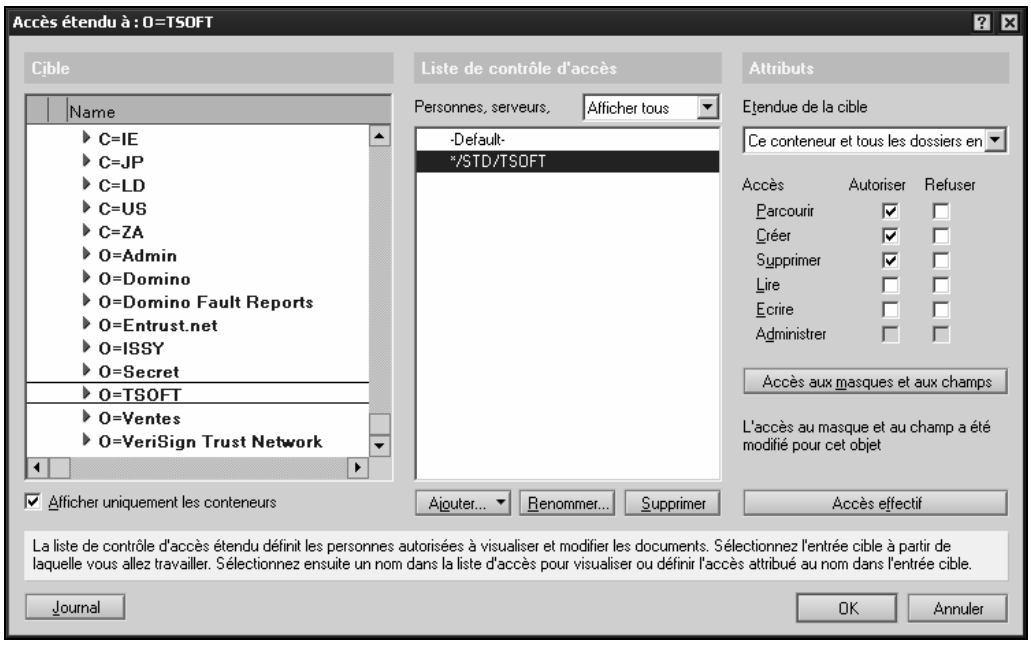
Signification des attributs

Parcourir	Voir les documents dans une vue.
Créer	Créer un document.
Supprimer	Supprimer un document.
Lire	(LDAP) Voir le contenu des champs d'un document.
Ecrire	(LDAP) Modifier le contenu des champs d'un document.
Administrer	Permet à celui qui a un accès Concepteur ou Editeur de modifier les accès pour une cible de la LCA étendue. Un serveur Domino 6 autre que le serveur d'administration de l'annuaire peut exécuter les requêtes administratives se trouvant dans la cible indiquée.

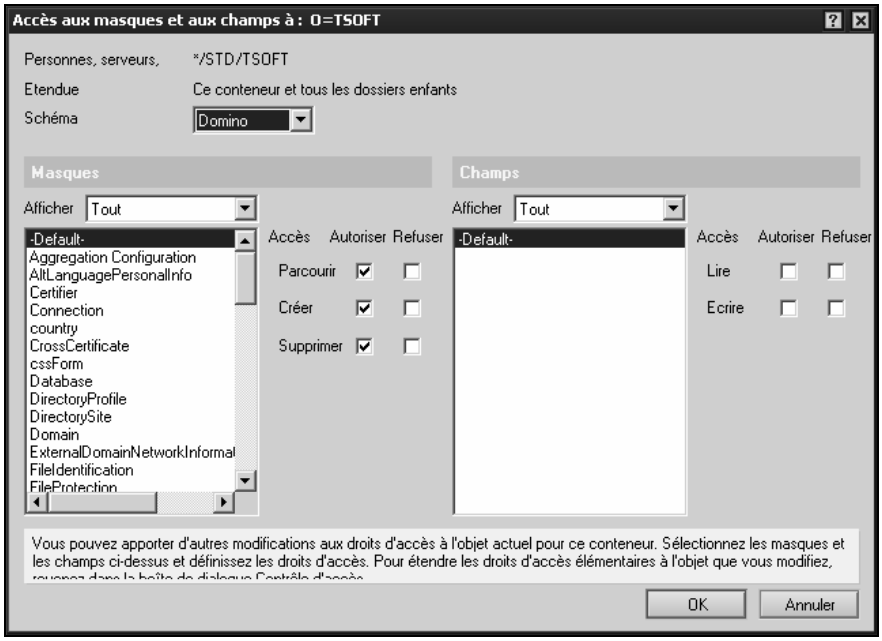
Restrictions sur un champ

Les utilisateurs /SEC/TSOFT et /STD/TSOFT ne doivent pas voir le champ HTTPPassword avec le masque Person.

- <Cible> : sélectionner /TSOFT
- <Etendue de la cible> : sélectionner *Ce conteneur et tous les dossiers enfants*
- <Liste de contrôle d'accès> : cliquer (Ajouter)
- Sélectionner Nom…, puis taper ***/SEC/TSOFT***



- <Accès> : cocher ☒*Autoriser* pour les lignes indiquées afin de ne pas restreindre les utilisateurs au niveau document. Lire et Ecrire concernent les annuaires LDAP et ne sont pas applicables ici
- Répéter l'opération avec **/STD/TSOFT*
- Sélectionner une entrée, **/STD/TSOFT* par exemple
- Cliquer (Accès aux masques et aux champs)



Les options affichées sont héritées du dialogue précédent : on retrouve ☒*Parcourir*, ☒*Créer* et ☒*Supprimer* sélectionnés.

- <Masques> : sélectionner Person
- <Champs> : sélectionner -Default-. ☒*Lire* et ☒*Ecrire* sont *Autoriser* par défaut
- <Champs> : sélectionner HTTPPassword puis cocher ☒*Ecrire :Refuser*

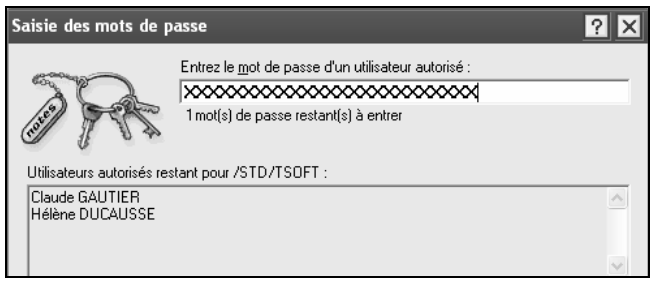
Migration d'un certificateur d'OU Domino

Le scénario proposé consiste à migrer le certificat d'unité d'organisation dont dépendent les utilisateurs n'ayant pas besoin d'un haut niveau de sécurité. Le certificat bénéficiera de la sécurité minimum.

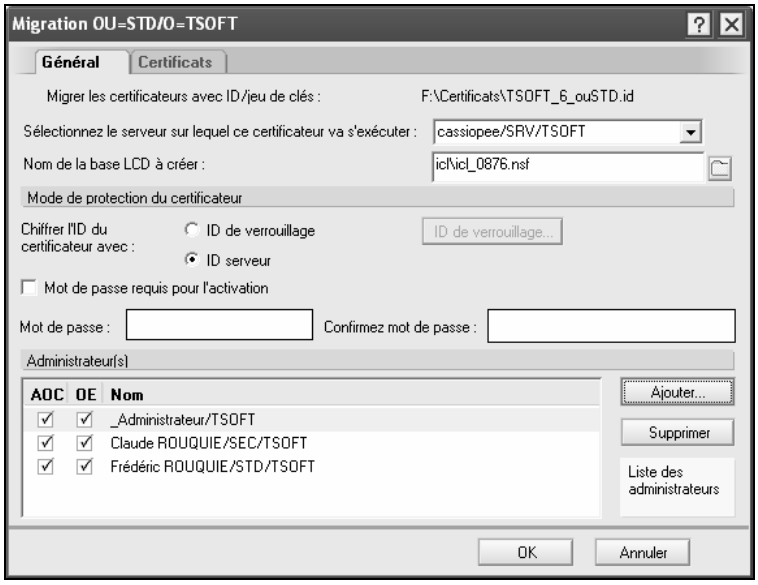
Le fichier ID est accessible depuis le poste d'administration utilisé.

- Aller dans *Domino Administrator*
- Cliquer sur l'onglet (Configuration)
- Cliquer (Outils), puis (Certification), puis *Faire migrer certificateur…*

- Cliquer (Sélectionner…) puis naviguer jusqu'au dossier contenant le fichier ID correspondant à l'unité d'organisation, puis cliquer (OK)



- <Mot de passe> : taper le mot de passe du certificat, puis cliquer (OK)



- <Sélectionner le serveur sur lequel ce certificateur va s'exécuter> : sélectionner un serveur, par exemple le serveur d'administration de l'annuaire du domaine

- <Nom de la base LCD à créer> : laisser le défaut (conseillé). Le nom de l'unité d'organisation sera automatiquement ajouté dans le titre de cette base
- <Mode de protection du certificateur> : choisir une option

Option	Mot de passe	Activation
ID de verrouillage	Celui du fichier ID	Déverrouillage manuel
ID serveurD	Aucun	Automatique
Mot de passe	Celui qui est entré	Activation manuelle

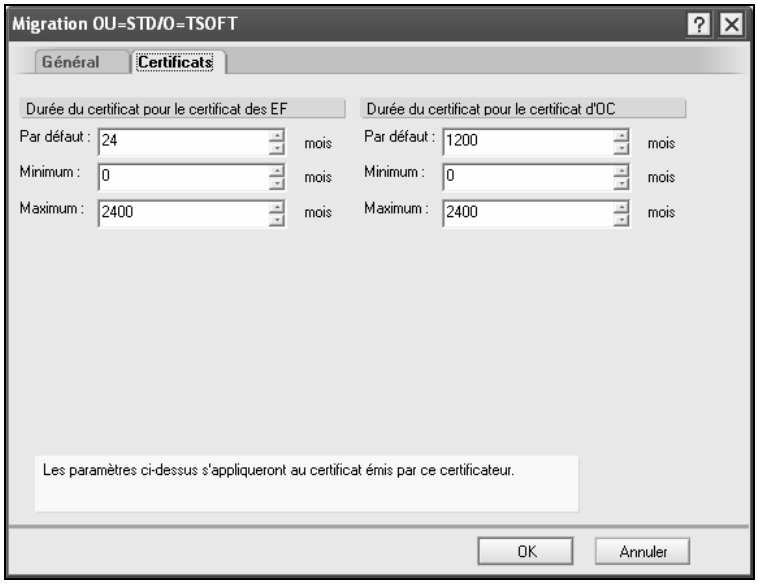
– Cliquer ❍ *ID serveur* pour que le certificat soit activé automatiquement au démarrage du serveur. Le certificat actuel ayant besoin du niveau de sécurité minimum, cette option est retenue
– Cocher ☒*Mot de passe requis pour l'activation* pour un certificat qui doit être activé par saisie d'un mot de passe. L'utilisation du certificat a un niveau de sécurité moyen
– Cliquer ❍ *ID de verrouillage* pour que le certificat soit activé manuellement après démarrage du serveur par saisie du mot de passe du fichier ID. L'utilisation du certificat a un niveau de sécurité maximum

- Cliquer (Ajouter…) et choisir un administrateur supplémentaire devant avoir le rôle OC ou OR

Remarque

Il est conseillé d'utiliser l'identifiant de « super administrateur » dans un but de simplification comme autorité de certification – rôle OC – et d'ajouter les identifiants personnels des administrateurs devant enregistrer des utilisateurs Notes – rôle OR –.

- Cliquer sur l'onglet (Certificats)



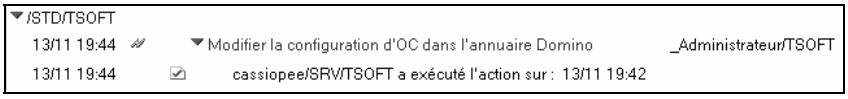
Cette page permet de déterminer les fourchettes de durées de validité des certificats. A l'issue de la période de validité, un certificat émis – de personne, de serveur ou d'unité d'organisation – doit être recertifié.

Champ	Valeurs
Durée du certificat pour le certificat des EF	Durée en mois par défaut, minimum et maximum pour un certificat client Notes. Ce certificat est dit EF (Entité Finale).

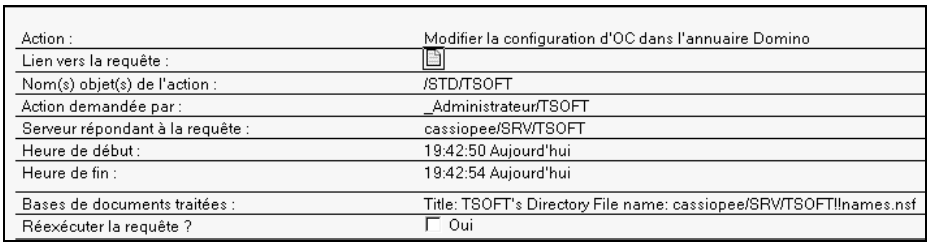
Durée du certificat pour le certificat d'OC	Durée en mois par défaut, minimum et maximum pour un certificat d'unité d'organisation Domino. Ce certificat est dit OC (Organisme de certification).

La durée de vie par défaut d'un certificat Notes peut être portée à 48 mois.

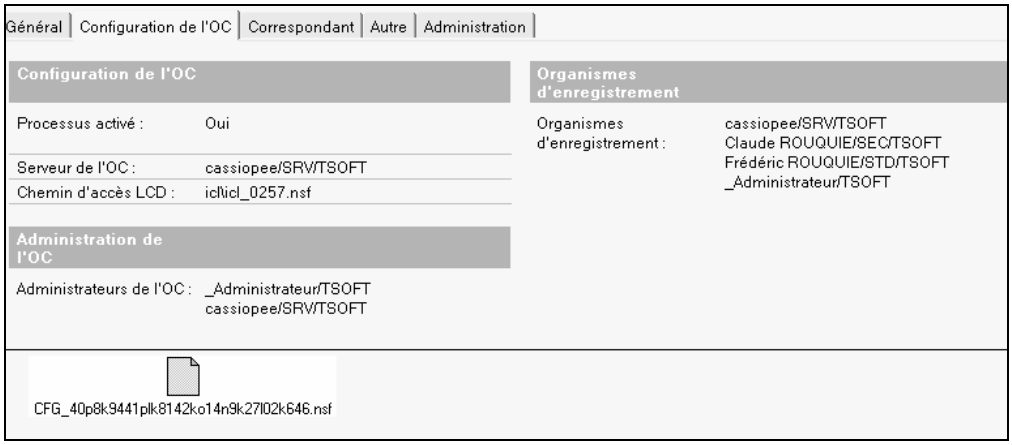
- Cliquer (OK)



Une requête administrative est soumise : elle met à jour l'annuaire.



- Cliquer sur l'onglet (Personnes et groupes), puis sur la vue *Certificats*
- Ouvrir le document correspondant au certificat migré, ici /STD/TSOFT
- Cliquer sur l'onglet (Configuration de l'OC)



L'onglet (Configuration de l'OC) est présent pour un certificat migré uniquement. Le fichier en pièce attachée – une base Notes – ne sert à rien à l'heure actuelle et est réservé à des améliorations à venir. Les informations ne sont pas modifiables directement ↳Modification d'un certificat migré.

Vérification de la migration

- Ouvrir la console du serveur, puis taper successivement les commandes en **gras**

```
> load ca
> tell ca status
10/11/2006 17:29:36   CA Process Status:
```

```
10/11/2006 17:29:36     1. OU=STD/O=JFRI
10/11/2006 17:29:36          Certifier Type: Notes
10/11/2006 17:29:36          Active: Yes
10/11/2006 17:29:36          ICL DB Path: icl\icl_9312.nsf
```

Le certificat migré apparaît comme étant *actif* : il est chiffré avec l'ID du serveur sans mot de passe. Le nom de la base ICL qui lui correspond est affiché.

OC. Désactiver, modifier certificateur

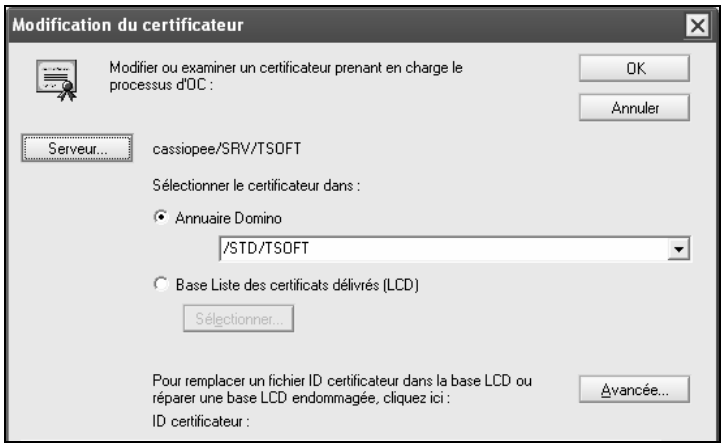
Désactivation d'un certificateur migré

Cette opération désactive la migration. Il faudra migrer à nouveau le certificateur ultérieurement si nécessaire.

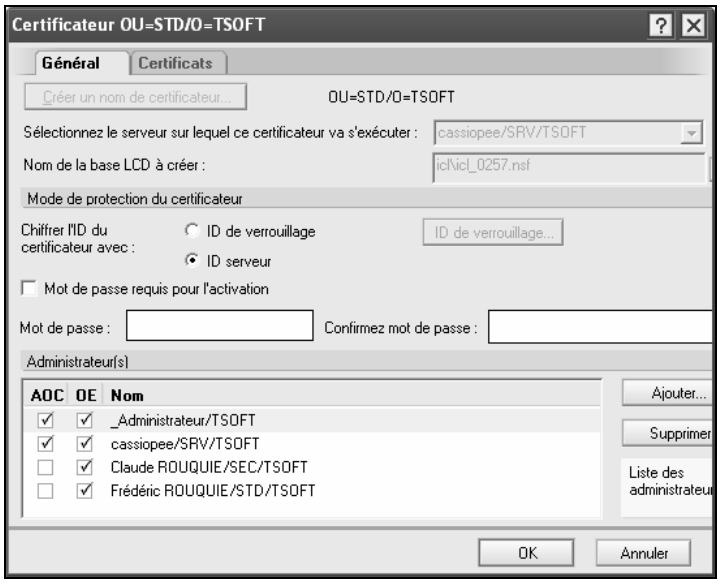
- Ouvrir en modification le document du certificateur dans l'annuaire
- Cliquer sur l'onglet (Configuration d'OC)
- <Processus activé> : sélectionner *Non*

Modification d'un certificateur migré

- Cliquer sur l'onglet (Configuration)
- Cliquer (Outils), puis (Certification), puis *Modifier certificateur*…



- Cliquer ❍*Annuaire Domino*, puis sélectionner le certificateur



- Porter les modifications voulues, puis cliquer (OK)
- Taper la commande `tell ca refresh` sur la console du serveur Domino

OC. Sécurité renforcée de certificateur

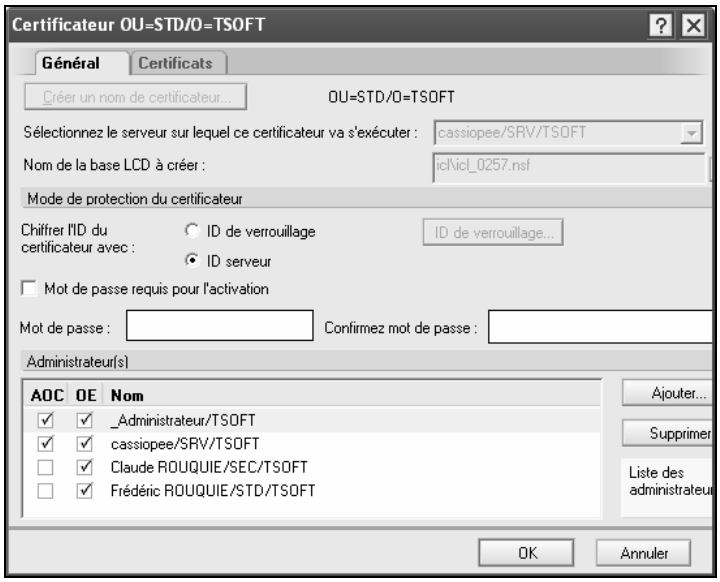
Le scénario proposé consiste à migrer le certificateur d'unité d'organisation dont dépendent les utilisateurs ayant besoin d'un haut niveau de sécurité. Le certificateur bénéficiera de la sécurité maximum : il devra être déverrouillé manuellement et les certificats Notes émis seront activés manuellement. Ces deux mesures doivent permettre en principe d'éviter une utilisation frauduleuse.

Remarque

Lorsqu'un certificateur d'unité d'organisation a un usage restreint, il n'est pas nécessaire de le migrer. Son utilisation reposant sur l'accès physique au fichier ID correspondant et à la connaissance d'un ou plusieurs mots de passe, il est protégé par les standards de sécurité Domino/Notes.

Le fichier ID est accessible depuis le poste d'administration utilisé.

- Aller dans *Domino Administrator*
- Cliquer sur l'onglet (Configuration)
- Cliquer (Outils), puis (Certification), puis *Faire migrer certificateur…*
- Cliquer (Sélectionner…) puis naviguer jusqu'au dossier contenant le fichier ID correspondant à l'unité d'organisation
- Cliquer (OK)
- <Mot de passe> : taper le mot de passe du certificateur, puis cliquer (OK)



- <Mode de protection du certificateur> : cliquer ❍ *ID de verrouillage* pour que le certificateur soit activé manuellement après démarrage du serveur
- Cliquer (ID de verrouillage) et sélectionner le nom de l'administrateur dont l'ID servira au chiffrement du certificat et à son déverrouillage, de préférence un identifiant générique de « super administrateur »
- ☒*Mot de passe requis pour l'activation* : cocher cette option puis taper le mot de passe d'activation
- Cliquer (Ajouter…) et choisir un administrateur supplémentaire devant avoir le rôle OC et/ou OR
- Cliquer sur l'onglet (Certificats) puis ajuster les durées de vie des certificats émis en fonction des contraintes de sécurité de l'entreprise

- Cliquer (OK), puis de nouveau (OK)

Une requête administrative met à jour le document du certificat dans l'annuaire.

- Ouvrir le document du certificat et vérifier que l'onglet (Processus d'OC) a été ajouté et que les informations sont correctes
- Taper la commande `tell ca refresh` à la console du serveur, puis la commande `tell ca stat`

```
> tell ca refresh
10/11/2006 17:56:14    Certifier [OU=SEC/O=JFRI] is
deactivated.  It will require password to activate it.
10/11/2006 17:56:14   CA Process: 'tell ca refresh' finished.
Use 'tell ca status' to check result.
> tell ca status
10/11/2006 17:56:25   CA Process Status:
10/11/2006 17:56:25     1. OU=STD/O=JFRI
10/11/2006 17:56:25         Certifier Type: Notes
10/11/2006 17:56:25         Active: Yes
10/11/2006 17:56:25         ICL DB Path: icl\icl_9312.nsf
10/11/2006 17:56:25     2. OU=SEC/O=JFRI
10/11/2006 17:56:25         Certifier Type: Notes
10/11/2006 17:56:25         Active: No
10/11/2006 17:56:25         Password Required: Yes
10/11/2006 17:56:25         ICL DB Path: icl\icl_4818.nsf
```

Le certificat /SEC/TSOFT n'est pas actif car il a besoin d'un mot de passe.

```
> tell ca activate 2 azertyui
10/11/2006 18:12:23   CA Process: 'tell ca activate' finished.
Use 'tell ca status' to check result.
> tell ca status
10/11/2006 18:12:26   CA Process Status:
10/11/2006 18:12:26     1. OU=STD/O=JFRI
10/11/2006 18:12:26         Certifier Type: Notes
10/11/2006 18:12:26         Active: Yes
10/11/2006 18:12:26         ICL DB Path: icl\icl_9312.nsf
10/11/2006 18:12:26     2. OU=SEC/O=JFRI
10/11/2006 18:12:26         Certifier Type: Notes
10/11/2006 18:12:26         Active: Yes
10/11/2006 18:12:26         Password Required: Yes
10/11/2006 18:12:26         ICL DB Path: icl\icl_4818.nsf
```

- Taper la commande
  - `tell ca activate <#certificat> <motDePasseActivation>` si le certificateur a un mot de passe d'activation
  - `tell ca unlock <cheminFichierID> <motDePasseActivation>` si le certificateur est verrouillé avec un fichier ID d'administration

L'activation du certificateur se fait en principe après l'enregistrement des utilisateurs. Le mot de passe d'activation apparaît en clair sur la console du serveur. Il n'est pas enregistré dans le journal du serveur.

OC. Enregistrer des utilisateurs Notes depuis Administrator

- **Droits requis pour créer les utilisateurs Notes**
  - Annuaire du domaine : accès Auteur et rôle [UserCreator]
  - Base Certification Log certlog.nsf : accès Auteur
  - Certificateur : être listé comme OR
- **Enregistrement depuis le client Domino Administrator**
- **Activation de la signature des certificats Notes émis**
  - Automatique
  - Par mot de passe d'activation ou de déverrouillage
- **Mise à jour des documents Personnes : requête administrative**
  - Le fichier ID est signé après rattachement dans Personne

Le but poursuivi par le processus d'OC est d'alléger l'administration Domino en confiant les tâches répétitives et lourdes – l'enregistrement d'utilisateurs – entre les mains d'administrateurs ayant des droits limités. La gestion des droits d'administration est centralisée ce qui renforce la sécurité du domaine Domino.

Le paragraphe examine :

– La liste des droits nécessaires et suffisants pour l'administrateur qui devra enregistrer les utilisateurs Notes,
– L'utilisation de certificats migrés dans le processus d'OC dans Administrator,
– L'intervention d'un administrateur central sur la console du serveur Domino pour activer la signature des certificats Notes créés,
– La mise à jour des documents Personnes créés par les requêtes administratives.

Droits nécessaires

Droit	Objet
Annuaire du domaine : – accès *Auteur*, – Privilège ☒*Créer des documents* – Rôle [*UserCreator*]	Créer des documents Personnes dans l'annuaire.
Journal de certification : certlog.nsf – Accès *Auteur* – Privilège ☒*Créer des documents*	L'enregistrement d'un utilisateur génère un document dans le journal de certification.
Certificat migré – Rôle *Administrateur OR*	Pour pouvoir signer des certificats utilisateurs avec le certificateur.
Serveur de messagerie – Création de bases autorisée	Pour pouvoir créer la base Courrier d'un utilisateur.

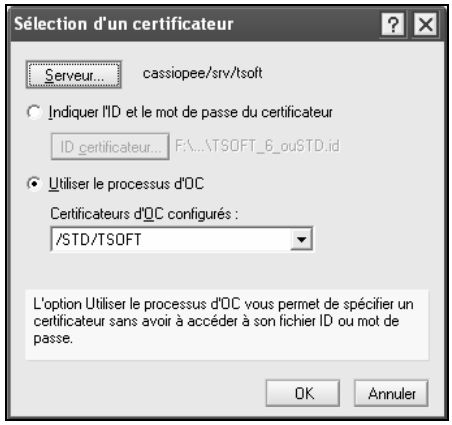
Le tableau liste les droits nécessaires pour enregistrer des utilisateurs Notes depuis Domino Administrator en passant par le processus d'OC et sans accéder à un certificat d'organisation ou d'unité d'organisation.

Enregistrement depuis Domino Administrator

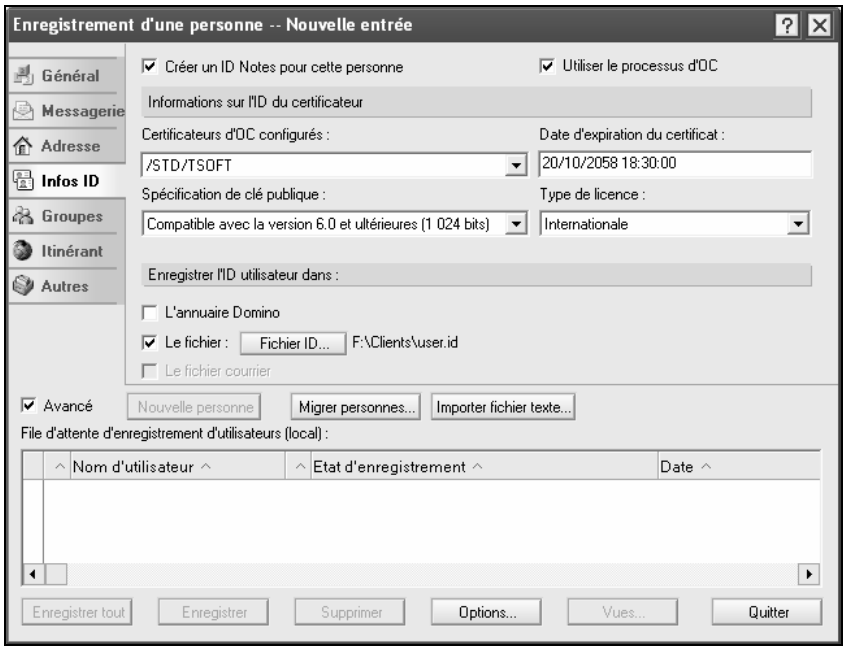
La tâche CA tourne sur le serveur Domino.

L'administrateur avec rôle OR se signe avec Domino Administrator.

- Cliquer sur l'onglet (Personnes et groupes)
- Cliquer (Outils), puis (Personnes), puis *Enregistrer*…
- Cliquer (Annuler) si le mot de passe du certificat précédemment utilisé est demandé



- Sélectionner ❍*Utiliser le processus d'OC*
- <Certificateurs d'OC configurés> : sélectionner un certificat
- Cliquer (OK)
- Cocher ☒*Avancé*, puis cliquer (Informations ID)



Il est possible de modifier le choix du certificat actuel :

- Cocher ☒*Utiliser le processus d'OC*

- <Certificateurs d'OC configurés> : sélectionner le certificateur d'unité d'organisation
- Compléter les autres champs puis enregistrer les personnes

Activation des certificats

Activation automatique

Lorsque l'activation des certificats clients ne demande pas de mot de passe – ici */STD/TSOFT* –, un message d'information est envoyé à la console du serveur.

```
10/11/2006 15:43:23   Database mail\ldavis.nsf created by
Claude GAUTIER/SEC/TSOFT
10/11/2006 15:43:25   The ACL in database mail\ldavis.nsf has
been changed by Claude GAUTIER/SEC/TSOFT.
10/11/2006 15:43:33   Certifying Lou DAVIS/STD/TSOFT
10/11/2006 15:43:34   CA Process (OU=STD/O=TSOFT): Certificate
Request processed.
```

Activation manuelle par mot de passe

Une intervention à la console du serveur est nécessaire pour activer manuellement les certificats émis lorsque le certificat migré demande un mot de passe d'activation. Le certificat */SEC/TSOFT* correspond à ce cas de figure dans l'exemple démontré ici.

Le mot de passe qui doit être entré correspond à celui qui a été spécifié lors de la migration du certificat, l'option ☒*Mot de passe requis pour l'activation* étant cochée.

- Taper `load ca` pour démarrer la tâche CA. Un message d'avertissement apparaît indiquant qu'un mot de passe est requis

```
> load ca
10/11/2006 14:15:30   CA Process: Certifier OU=STD/O=TSOFT
initialized.
10/11/2006 14:15:30   CA Process: Password is needed to
activate the certifier (OU=SEC/O=TSOFT).
```

- Taper `tell ca show status` pour connaître le numéro du certificat

```
> tell ca status
10/11/2006 14:15:39   CA Process Status:
10/11/2006 14:15:39     1. OU=STD/O=TSOFT
10/11/2006 14:15:39          Certifier Type: Notes
10/11/2006 14:15:39          Active: Yes
10/11/2006 14:15:39          ICL DB Path: icl\icl_9312.nsf
10/11/2006 14:15:39     2. OU=SEC/O=TSOFT
10/11/2006 14:15:39          Certifier Type: Notes
10/11/2006 14:15:39          Active: No
10/11/2006 14:15:39          Password Required: Yes
10/11/2006 14:15:39          ICL DB Path: icl\icl_4818.nsf
```

- Taper `tell ca show queue *` pour connaître les demandes en attente

```
> tell ca show queue *
10/11/2006 14:17:05   CA request queues for OU=STD/O=TSOFT:
10/11/2006 14:17:05 Certificate Requests:No Entries in Queue
…
10/11/2006 14:17:05 CA request queues for OU=SEC/O=TSOFT:
10/11/2006 14:17:05 Certificate Requests:
10/11/2006 14:17:05 1. Subject: CN=John BULL/OU=SEC/O=TSOFT
10/11/2006 14:17:05 RA: CN=Hélène ROUQUIE/OU=SEC/O=TSOFT
10/11/2006 14:17:05 Submitted On: 10/11/2006 21:20:27
```

- Taper `tell ca activate 2 azertyui` pour activer le deuxième certificat avec le mot de passe *azertyui*

```
> tell ca activate 2 azertyui
10/11/2006 14:17:33   CA Process: 'tell ca activate' finished.
Use 'tell ca status' to check result.
10/11/2006 14:17:36   Certifying John BULL/SEC/TSOFT
10/11/2006 14:17:37   CA Process (OU=SEC/O=TSOFT): Certificate
Request processed.
```

Un message indique quelles sont les requêtes traitées.

Activation manuelle par ID de verrouillage

Une intervention à la console du serveur est nécessaire pour activer manuellement les certificats émis lorsque le certificat migré demande un mot de passe de déverrouillage. Le certificat /SEC/TSOFT – modifié par rapport à ce qui précède – correspond à ce cas de figure dans l'exemple démontré ici.

Le mot de passe qui doit être entré correspond à celui du fichier ID qui a été spécifié lors de la migration du certificat, l'option ❍*Chiffrement avec ID de verrouillage* étant sélectionnée.

- Taper `tell ca show queue *` pour connaître les demandes en attente

```
10/11/2006 14:42:56   Database mail\pdugommi.nsf created by
Hélène ROUQUIE/SEC/TSOFT
> tell ca show queue *
10/11/2006 14:43:56 CA request queues for OU=SEC/O=TSOFT:
10/11/2006 14:43:56 Certificate Requests:
10/11/2006 14:43:56 1. Subject: CN=Paul
DUGOMMIER/OU=SEC/O=TSOFT
10/11/2006 14:43:56 RA: CN=Hélène ROUQUIE/OU=SEC/O=TSOFT
10/11/2006 14:43:56 Submitted On: 10/11/2006 14:42:56
```

La requête de signature du certificat Notes apparaît en attente.

- Taper `tell ca show status` pour connaître le numéro du certificat et l'ID de verrouillage

```
> tell ca status
10/11/2006 14:46:16   CA Process Status:
10/11/2006 14:46:16     1. OU=STD/O=TSOFT
10/11/2006 14:46:16          Certifier Type: Notes
10/11/2006 14:46:16          Active: Yes
10/11/2006 14:46:16          ICL DB Path: icl\icl_9312.nsf
10/11/2006 14:46:16     2. OU=SEC/O=TSOFT
10/11/2006 14:46:16          Certifier Type: Notes
10/11/2006 14:46:16          Lock ID Name:
CN=_Administrateur/O=TSOFT
10/11/2006 14:46:16          Active: No
10/11/2006 14:46:16          ICL DB Path: icl\icl_4818.nsf
```

- Taper `tell ca unlock d:\ID_PR6\Clients\admin.id azertyui` pour déverrouiller tous les certificats qui correspondent à cet ID de verrouillage – indiqué par son chemin d'accès sur le serveur d:\ID_PR6\Clients\admin.id – suivi du mot de passe d'accès à cet ID, ici *azertyui*

```
> tell ca unlock d:\ID_R6\Clients\admin.id azertyui
10/11/2006 14:47:03   CA Process: 'tell ca unlock' finished.
Use 'tell ca status' to check result.
10/11/2006 14:47:06   Certifying Paul DUGOMMIER/SEC/TSOFT
10/11/2006 14:47:06   CA Process (OU=SEC/O=TSOFT): Certificate
Request processed.
```

- Taper `tell ca status` pour afficher l'état des certificateurs

```
> tell ca status
10/11/2006 14:47:13   CA Process Status:
10/11/2006 14:47:13     1. OU=STD/O=TSOFT
10/11/2006 14:47:13          Certifier Type: Notes
10/11/2006 14:47:13          Active: Yes
10/11/2006 14:47:13          ICL DB Path: icl\icl_9312.nsf
10/11/2006 14:47:13     2. OU=SEC/O=TSOFT
10/11/2006 14:47:13          Certifier Type: Notes
10/11/2006 14:47:13          Lock ID Name:
CN=_Administrateur/O=TSOFT
10/11/2006 14:47:13          Active: Yes
10/11/2006 14:47:13          ICL DB Path: icl\icl_4818.nsf
```

Mise à jour des documents de personnes

La requête de signature du certificat est écrite dans la base des requêtes administratives – admin4.nsf – à l'issue de l'enregistrement.

C'est cette requête qui est traitée automatiquement par la tâche CA ou après activation ou déverrouillage manuel du certificat d'unité d'organisation. Elle est visible dans la vue *Requêtes de certificats*.

Ceci fait, une nouvelle requête est initialisée dont l'objectif est de mettre à jour le document Personne de l'utilisateur enregistré. Elle est visible dans la vue *Toutes les requêtes par nom* où elle apparaît catégorisée avec le nom de l'utilisateur concerné.

La clé publique recertifiée de l'utilisateur est écrite dans le document Personne correspondant.

OC. Commandes console

Les commandes console utilisées dans les exemples sont listées ici.

TELL CA STATUS	Affiche les informations récapitulatives de tous les certificats gérés par le processus d'OC. Le numéro du certificat est utilisé pour le désigner dans la plupart des commandes TELL CA. CA Process Status: 1. OU=STD/O=TSOFT Certifier Type: Notes Active: Yes ICL DB Path: icl\icl_9312.nsf 2. OU=SEC/O=TSOFT Certifier Type: Notes Lock ID Name: CN=_Administrateur/O=TSOFT Active: No ICL DB Path: icl\icl_4818.nsf
TELL CA SHOW QUEUE	Affiche toutes les requêtes en attente – certificats, révocation, modification, restauration – pour un certificat ou tous les certificats (*). TELL CA SHOW QUEUE <#Certificat> TELL CA SHOW QUEUE *
TELL CA ACTIVATE	TELL CA ACTIVATE <#Certificat> [mot de passe] TELL CA ACTIVATE * Active un certificat qui a été créé avec un mot de passe d'activation ou qui a été désactivé. Active tous les certificats désactivés précédemment avec la commande TELL CA DEACTIVATE.
TELL CA DEACTIVATE	TELL CA DEACTIVATE <#Certificat> TELL CA DEACTIVATE * Désactive un certificat ou tous les certificats (*).
TELL CA LOCK	TELL CA LOCK <chemin fichier ID> Verrouille tous les certificats qui ont été créés avec cet ID de verrouillage. Le fichier ID est accessible depuis le serveur.
TELL CA UNLOCK	TELL CA UNLOCK <chemin fichier ID> <mot de passe> Déverrouille tous les certificats qui ont été créés avec cet ID de verrouillage. Le fichier ID est accessible depuis le serveur.
TELL CA REFRESH	Force le processus d'OC à rafraîchir la liste des certificats et de leurs paramètres. C'est l'équivalent d'un arrêt puis d'un redémarrage de la tâche. Il y a lieu d'activer et de déverrouiller à nouveau les certificats voulus.
TELL CA QUIT	Arrête la tâche CA.
TELL CA HELP TELL CA -?	Affiche l'aide pour les commandes CA.

OC. Création du certificateur Internet

- Aller dans Domino Administrator
- Cliquer sur l'onglet (Configuration)
- Cliquer (Outils), puis (Enregistrement), puis *Certificateur Internet…*

- Sélectionner ❍*Je souhaite enregistrer un nouveau certificateur Internet qui utilise le processus d'OC*

Remarque

L'option *J'ai un fichier jeu de clés que je souhaite enregistrer* correspond au cas où un certificat a été signé par un organisme de certification extérieur, Verisign ou un autre.

Le dialogue Enregistrer un nouveau certificat Internet s'affiche.

- Cliquer (Créer un nom de certificateur)

- Taper les informations qui identifient ce certificat

Le nom du certificateur a une structure hiérarchique plus détaillée que celui d'un certificateur Domino.

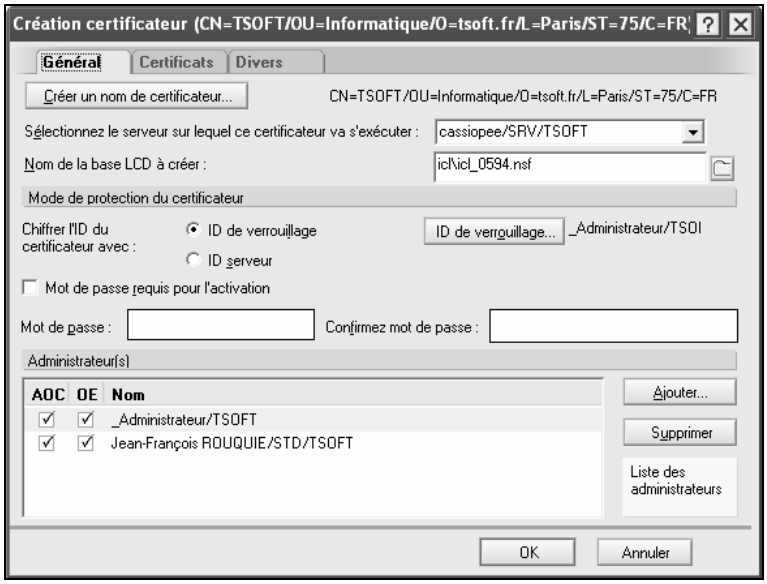
- <Nom commun> : taper le nom du certificateur, ici *TSOFT*
- <Subordonné> : taper le nom d'une unité d'organisation, ici *Informatique*. Ce paramètre optionnel est utilisable lorsque plusieurs certificateurs sont créés au sein d'une organisation tout comme les unités d'organisation Domino
- <Organisation> : le nom de l'organisation qui émet le certificat, ici *tsoft.fr*
- <Ville ou localité> : taper le nom du lieu d'émission (option), ici *Paris*
- <Département ou région> : taper l'état – EU, Canada – ou la province où est établie l'organisation, ici *75*

- <Pays> : taper le nom du pays – selon la norme internationale à deux caractères – où est établie l'organisation, ici *FR*
- Taper (OK)
- <Sélectionner le serveur sur lequel ce certificat sera exécuté> : sélectionner un serveur, par exemple le serveur d'administration de l'annuaire du domaine
- <Nom de la base LCD à créer> : laisser le défaut (conseillé). Le nom de l'unité d'organisation sera automatiquement ajouté dans le titre de cette base
- <Mode de protection du certificateur> : choisir une option

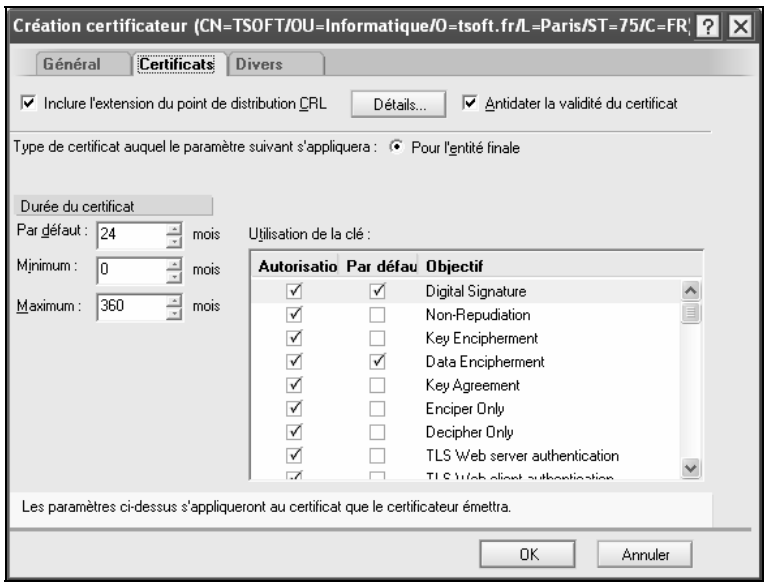
Option	Mot de passe	Activation
ID de verrouillage	Celui du fichier ID	Déverrouillage manuel
ID serveur	Aucun	Automatique
Mot de passe	Celui qui est entré	Activation manuelle

– Cliquer ❍ *ID serveur* pour que le certificateur soit activé automatiquement au démarrage du serveur. L'utilisation du certificateur actuel a le niveau de sécurité minimum
– Cocher ☒*Mot de passe requis pour l'activation* pour un certificateur qui doit être activé par saisie d'un mot de passe. L'utilisation du certificateur a un niveau de sécurité moyen
– Cliquer ❍ *ID de verrouillage* pour que le certificateur soit activé manuellement après démarrage du serveur par saisie du mot de passe du fichier ID. L'utilisation du certificateur a un niveau de sécurité maximum. C'est l'option qui a été retenue ici

- Cliquer (Ajouter…) et choisir un administrateur supplémentaire devant avoir le rôle OR et/ou OC



- Cliquer sur l'onglet (Certificats)

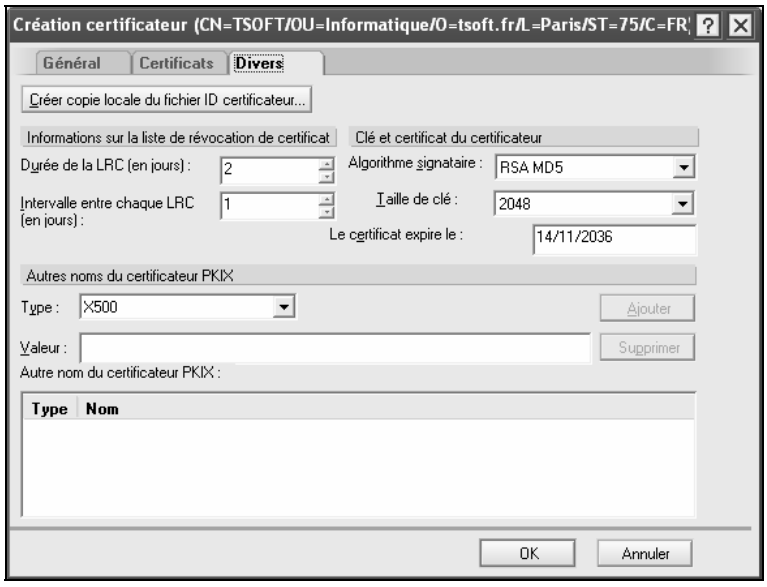


Les options s'appliquent aux certificats émis à partir du présent certificateur.

- <Type de certificat auquel le paramètre suivant s'appliquera> : sélectionner
  – ❍*Pour l'entité finale* c'est-à-dire des serveurs et/ou des clients
- <Durée du certificat> : taper les valeurs minimum, maximum et par défaut en mois
- <Utilisation de la clé> : cocher les options correspondant à l'utilisation qui sera faite des certificats émis. Par défaut, sauf cochées :
  – ☒*Digital signature* pour la signature de messages
  – ☒*Data enciphement* pour le chiffrement des données autres que les clés de chiffrement

Il est conseillé de conserver les valeurs par défaut.

- Cocher ☒*Antidater la validité du certificat* (défaut) pour que la date de validité du certificat puisse être différente de celle de sa création
- Cocher ☒*Inclure l'extension du point de distribution CRL* (défaut) qui identifie un serveur à partir duquel seront distribuées les listes de révocation de certificat. La révocation de certificat est vue avec la gestion des certificats clients
- Cliquer sur l'onglet (Divers)



Les informations concernant la liste de révocation (CRL) seront vues avec la gestion des certificats émis. Les algorithmes de chiffrement ne sont pas abordés ici.

- Cliquer (Créer copie locale du fichier d'ID certificateur…)

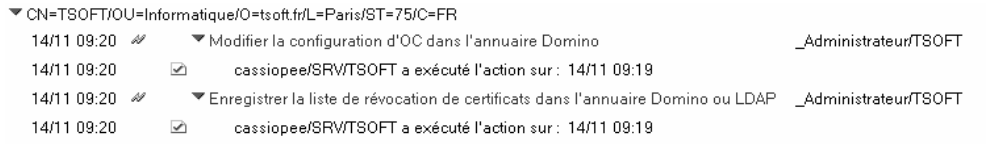
- Cliquer (Définir fichier d'ID…)
- Sélectionner le serveur de fichiers sur lequel se trouvent enregistrés les fichiers ID
- Sélectionner le chemin voulu
- Taper le mot de passe d'accès à ce fichier ID, puis cliquer (OK)

Remarque

Il est recommandé de prendre une copie de sécurité du certificat sous forme de fichier. Ceci permettra de l'importer dans le processus d'OC suite à une perte d'informations sur le serveur Domino.

- Cliquer (OK)

Deux requêtes sont soumises dans la base des requêtes administratives pour la mise à jour de l'annuaire Domino.



- `load ca` : taper cette commande sur la console du serveur Domino si la tâche *CA* ne tourne pas

Ou

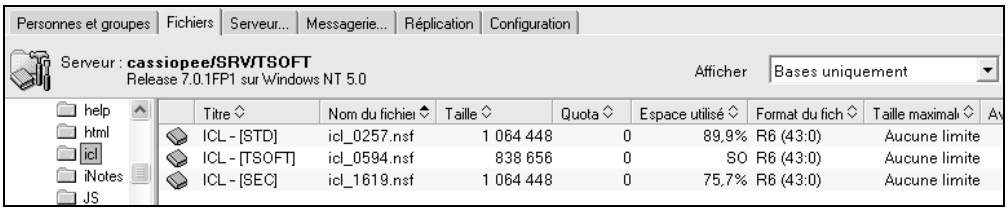
- `tell ca refresh` : taper cette commande si la tâche *CA* est déjà chargée

```
> load ca
14/11/2006 09:23:45   CA Process: Certifier OU=STD/O=TSOFT
initialized.
14/11/2006 09:23:45   CA Process: Certifier
CN=JFRI/OU=Informatique/O=JFRI Com/L=Lognes/ST=IDF/C=FRANCE
initialized.
14/11/2006 09:23:45   CA Process: Certifier
CN=TSOFT/OU=Informatique/O=tsoft.fr/L=Paris/ST=75/C=FR
initialized.
14/11/2006 09:23:45   CA Process: Password is needed to
```

```
activate the certifier (OU=SEC/O=TSOFT).
14/11/2006 09:23:54   Remote console command issued by
_Administrateur/TSOFT: tell
> tell ca refresh
14/11/2006 09:24:23    Certifier
[CN=JFRI/OU=Informatique/O=JFRI Com/L=Lognes/ST=IDF/C=FRANCE]
is locked.  It will need to be unlocked.
14/11/2006 09:24:23    Certifier
[CN=TSOFT/OU=Informatique/O=tsoft.fr/L=Paris/ST=75/C=FR] is
locked.  It will need to be unlocked.
14/11/2006 09:24:23    Certifier [OU=SEC/O=TSOFT] is
deactivated.  It will require password to activate it.
14/11/2006 09:24:23   CA Process: 'tell ca refresh' finished.
Use 'tell ca status' to check result.
```

Vérifications

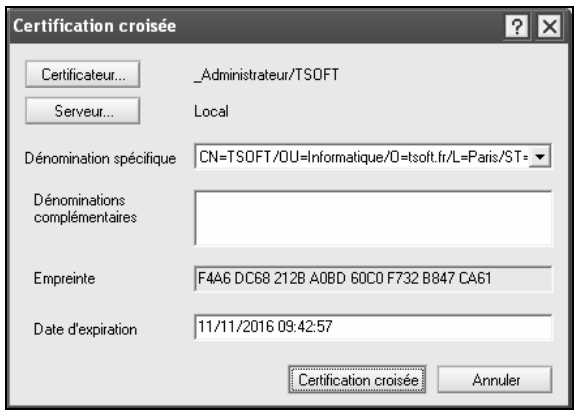
Base LCD : liste des certificats délivrés



Cette base s'appelle *ICL* en anglais : Issued Certificates List. Elle a été créée sur le serveur dans le dossier ICL\ si le défaut proposé à l'enregistrement a été conservé.
La LCA de la base a été automatiquement créée avec tous les administrateurs OC avec l'accès Gestionnaire et tous les administrateurs OR avec l'accès Lecteur.
La base contient des documents propres aux certificats Internet (qui sont absents pour les certificats Notes) :

Issued Certificates\By Subject Name	Le certificat de l'autorité de certification et les certificats EE émis par la suite.
Configuration\Revocation profile	Les règles de révocation applicables à un certificat Internet émis par une autorité de certification.

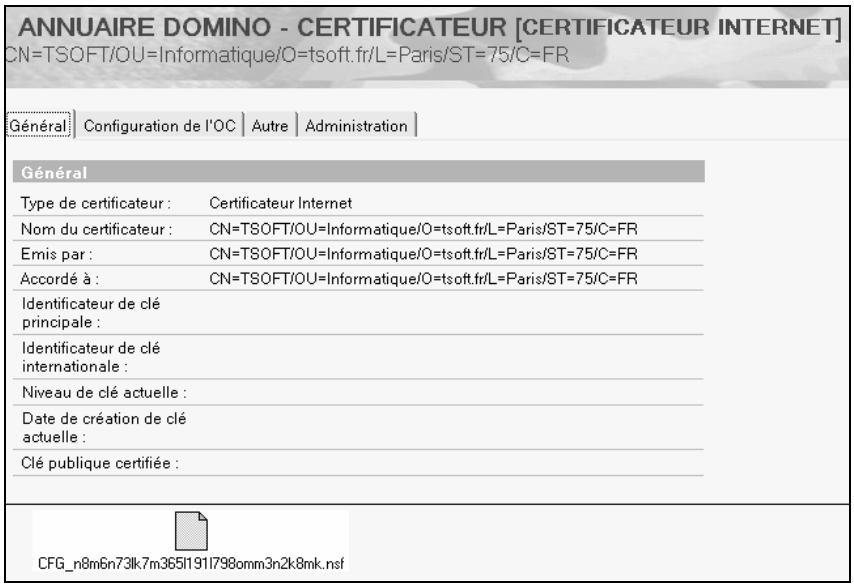
Ces documents ne peuvent pas être modifiés directement. Il faut utiliser l'option de modification du certificateur. L'ouverture de l'un de ces documents provoque l'affichage d'un message de contre-certification : le certificat d'autorité de certification a son propre jeu de clés publiques et privées et il n'est pas rattaché à l'organisation Domino.



- Cliquer (Certification croisée) pour faire confiance au certificat

Annuaire Domino

- Cliquer sur l'onglet (Personnes & Groupes)
- Ouvrir la vue *Certificats*, puis cliquer sur la catégorie *Certificats Internet* : le certificat est catégorisé par code pays



OC. Modifier, réparer, désactiver certificateur

Modifier le certificateur

- Cliquer sur l'onglet (Configuration)
- Cliquer (Outils), puis (Certificats), puis *Modifier un certificateur*…

- <Sélectionner certificateur dans> : choisir indifféremment
  – ❍*Annuaire Domino* puis sélectionner le certificat dans la liste déroulante
  – ❍*Base Liste des certificats délivrés (LCD)* puis cliquer (Sélectionner) et ouvrir la base LCD voulue depuis le serveur
- Cliquer (OK), puis porter les modifications voulues, et de nouveau cliquer (OK)

La modification est répercutée dans l'annuaire par une requête administrative.

Réparer le certificateur

Si la base ICL est endommagée ou si le certificateur doit être remplacé pour revenir à une situation antérieure, il faut charger la copie locale qui en a été faite au moment de sa création ou après une modification antérieure.

- Sélectionner le certificateur à modifier
- Cliquer (Avancé…), puis sélectionner le fichier certificateur sur disque

Désactiver le certificateur

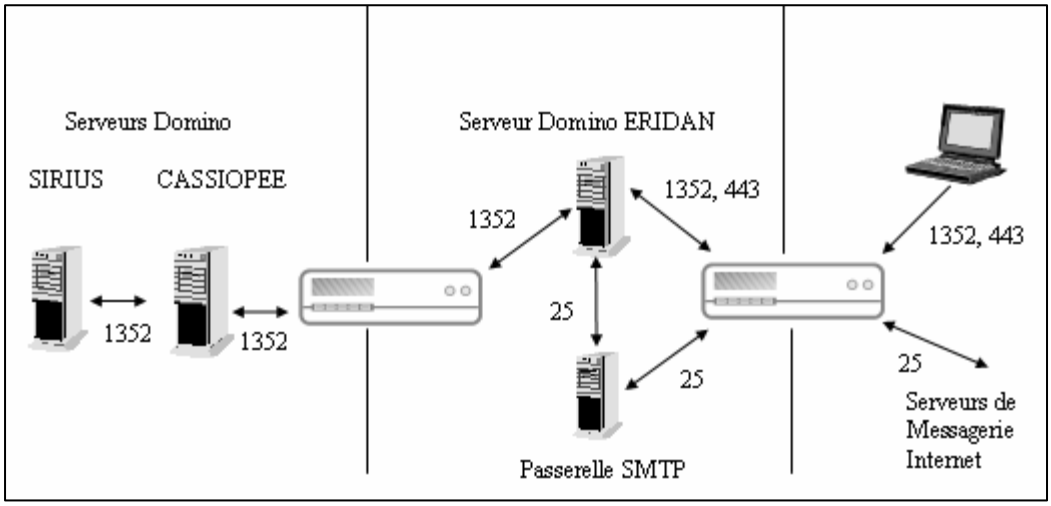
Le certificateur doit être désactivé temporairement ou de façon permanente.

- Ouvrir le document du certificateur dans l'annuaire Domino
- Cliquer sur l'onglet (Configuration de l'OC)
- <Processus activé> : cliquer *Désactivé*, puis enregistrer et fermer le document
- `tell ca refresh` : taper cette commande sur la console serveur

Installation domaine DMZ

Cette annexe déroule une procédure d'installation d'un serveur domino en domaine DMZ dans une situation réelle. Le domaine est complètement opérationnel à la fin de la procédure. Les choix proposés doivent être adaptés selon les situations.

Contexte



L'intranet comprend deux serveurs de messagerie en grappe. Les spécifications du serveur Domino en DMZ sont les suivantes :

- Le router dispose de deux adresses publiques pour les MX du domaine Internet de l'entreprise, soit mail1.domaine.com et mail2.domaine.com,
- Il y a deux passerelles SMTP : mail1.domaine.com et mail2.domaine.com,
- Le réseau TCP de la DMZ est distinct de celui de l'intranet,
- L'échange de courrier de DMZ avec l'intranet se fait uniquement sur le port 1352 : les adresses IP des deux serveurs de messagerie, celle de la station d'administration et celle du serveur en DMZ sont les seules à pouvoir communiquer sur ce port,
- Les ports 25 et 80 sont fermés entre DMZ et intranet. La liste des ports ouverts est très réduite,
- Les bases courrier des utilisateurs distants sont répliqués en DMZ et accédés par Lotus Notes ou navigateur sur port 443,
- L'annuaire du domaine intranet est répliqué en DMZ,
- Le serveur Domino en DMZ communique avec deux passerelles SMTP sur le port 25,
- Le serveur Domino donne un accès LDAP sécurisé – à la réplique de l'annuaire – à chaque passerelle SMTP,
- L'anti-virus et l'anti-spam s'exécutent sur les deux passerelles SMTP,
- Le serveur en DMZ est administré par les administrateurs du domaine d'intranet,
- L'administrateur Lotus Domino doit pouvoir accéder aux serveurs d'intranet depuis son portable et Lotus Domino Administrator en utilisant le serveur Domino en DMZ comme relais Lotus Domino.

Check-list d'installation

La check liste proposée ici est déroulée dans la suite de l'annexe.

Étape	Description	OK
1	Déterminer la configuration réseau intranet, DMZ et communication	

	avec l'extérieur	
2	Installation du logiciel Lotus Domino DMZ	
3	Configuration de Domino DMZ et lancement	
4	Configuration de la sécurité du serveur Domino DMZ	
5	Activation du relais Lotus Domino sur les serveurs d'intranet et de DMZ	
6	Configuration de la station d'administration pour accès local à Domino en DMZ	
7	Configuration d'une station d'administration distante pour accès à Domino en DMZ et en intranet (par relais Domino)	
8	Installation d'une réplique de l'annuaire de l'entreprise en DMZ	
9	Configuration de l'accès LDAP pour la passerelle SMTP	
10	Ouvrir le port 25 sur le serveur DMZ	
11	Modification de la topologie de routage de courrier Internet	
12	Configuration de l'accès HTTPS pour l'accès aux bases courrier	
13	Réplication des bases courrier en DMZ pour l'accès distant	

Configuration réseau

Dans l'ensemble de la configuration réseau, ce qui intéresse la messagerie se résume aux redirections suivantes :

– Adresse publique et port 25 sur l'une des deux passerelles,
– Adresse publique et port 1352 ou 443 sur le serveur Domino en DMZ.

Installation du serveur Domino

Le serveur Domino est dans la même organisation Lotus Domino – ici /TSOFT – que les serveurs d'intranet et dans un domaine Domino séparé, ici DMZ.

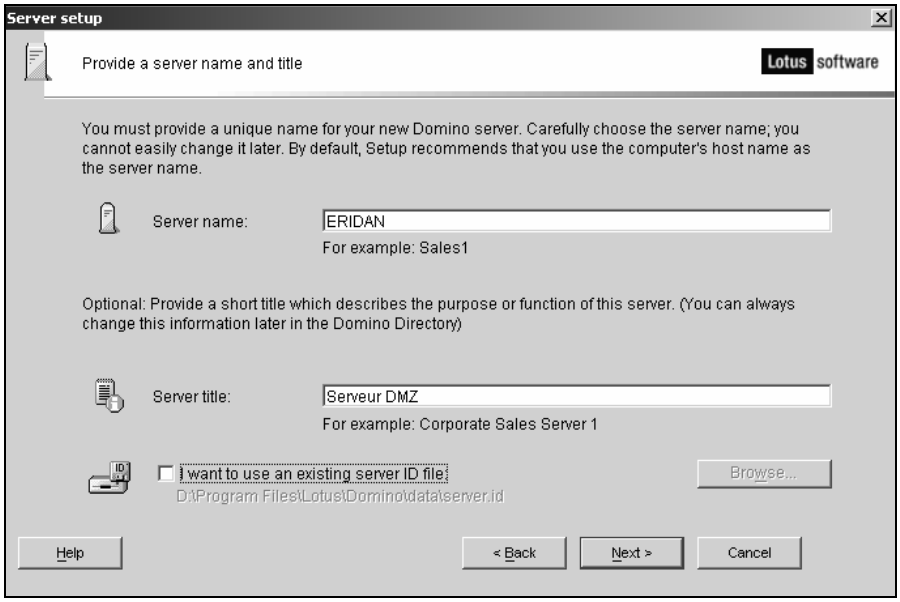
Chargement du logiciel

Le logiciel Domino Messaging Server en anglais est suffisant : pas de mise en grappe prévue. Le logiciel sera sur C:\ sur RAID 0 et les données sur D:\ en RAID 5.

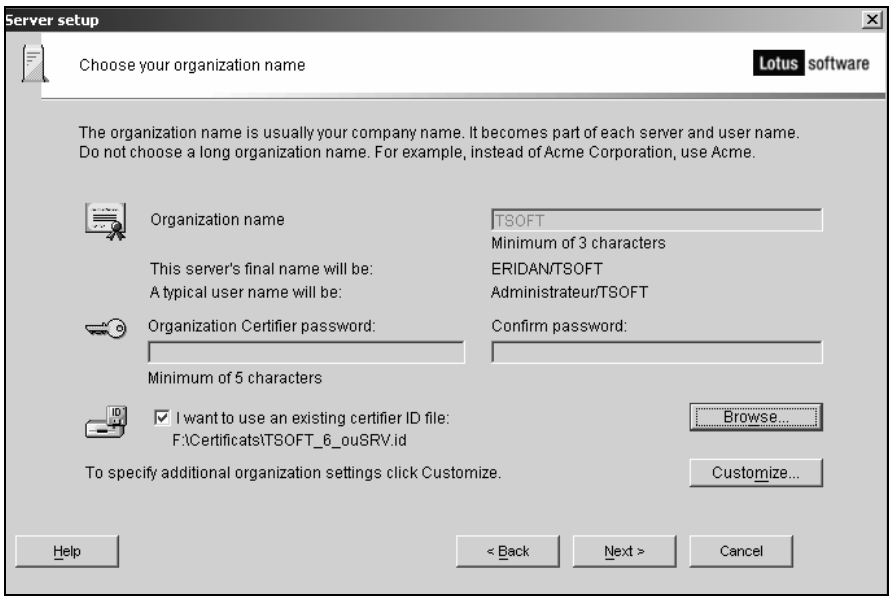
- Cliquer (Next >) depuis la première fenêtre *Lotus Domino Installer*
- Cliquer ❍*J'accepte les dispositions du contrat de licence*, puis (Next >)
- Sélectionner le répertoire du logiciel, puis (Next >)
- Sélectionner le répertoire des données, puis (Next >)
- Cliquer ❍*Messaging Server* puis (Next >)
- Vérifier les emplacements et la liste des fonctions
- Aller à la dernière ligne qui affiche l'espace total nécessaire
- Cliquer (Next), puis (Finish)

Configuration Domino

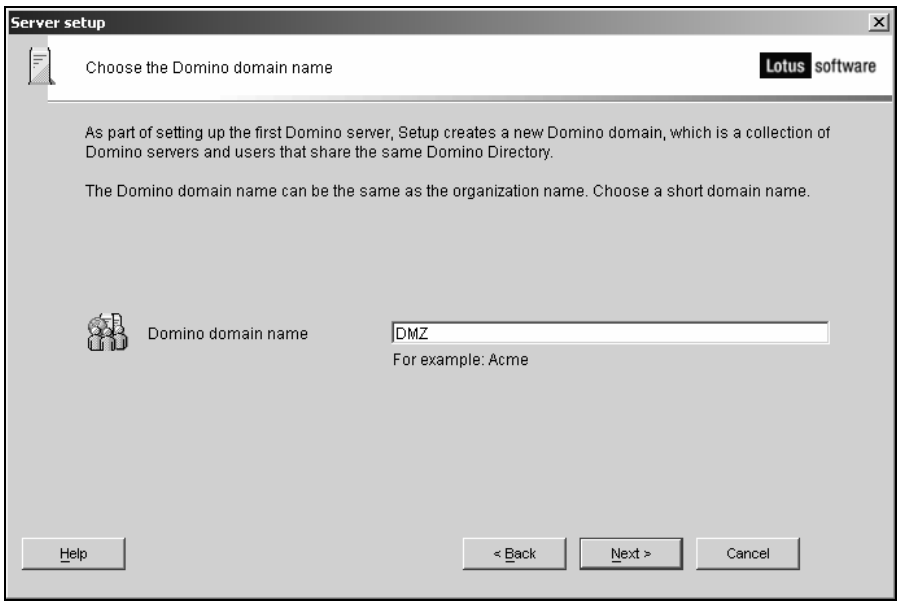
- Copier le fichier ID du super administrateur – ici _Administrateur/TSOFT – et le certificat réservé aux serveurs – ici /SRV/TSOFT – dans Lotus\Domino\Data ou le rendre disponible par un partage provisoire
- Lancer Domino server comme application, puis cliquer (Next)
- Cliquer ❍*Set up the first server or a stand-alone server*, puis cliquer (Next)



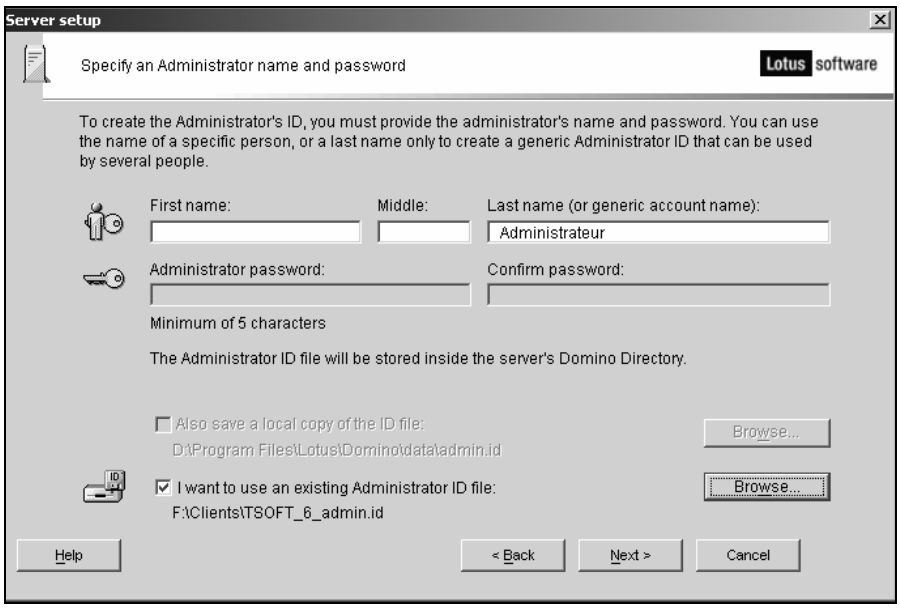
- <Server name> : taper le nom du serveur Domino, ici *eridan*
- <Server Title> : taper un texte indiquant le rôle du serveur, ici *Serveur DMZ*



- Cocher ☒*I want to use an existing certifier ID file* puis cliquer (Browse…) pour rechercher le fichier certificat d'organisation sur le disque, ici *F:\Certificats\TSOFT_6_ouSRV.id*
- Cliquer (Next), puis taper le mot de passe du certificat

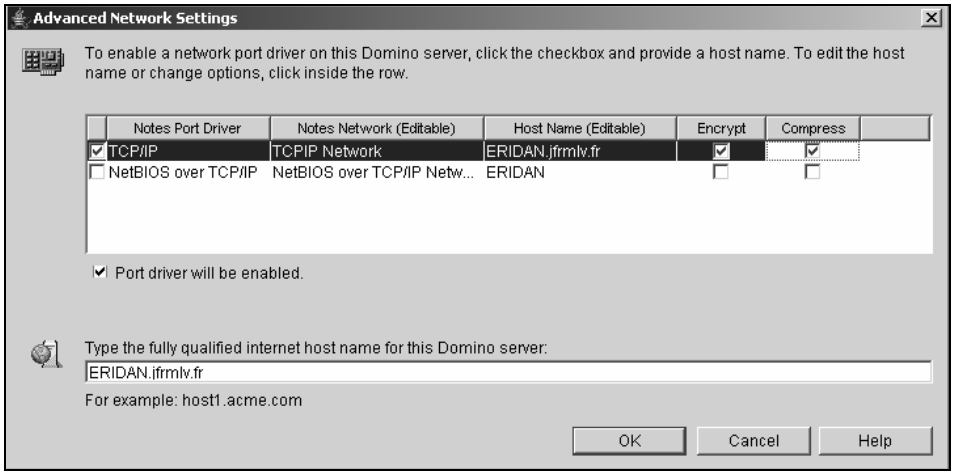


- <Domino domain name> : taper le nom du domaine Domino, ici *DMZ*
- Cliquer (Next)



- Cocher ☒*I want to use an existing Administrator ID file* puis cliquer (Browse…) pour rechercher le fichier ID de l'administrateur sur le disque, ici *F:\Certificats\TSOFT_6_admin.id*
- Cliquer (Next), puis taper le mot de passe de l'administrateur
- What Internet Services should this Domino server provide : cliquer (Customize…)
- Cocher les options suivantes pour le serveur Domino en DMZ
  – ☒**Mail Routeur,*
  – ☒**Agent Manager,*
  – ☒**Administration process,*
  – ☒*Statistics,*
  – ☒*Statistic collector,*
  – ☒*Ispy,*
  – ☒*LDAP,*
  – ☒*HTTP,*
  – ☒*SMTP Server*

- Cliquer (OK), puis (Next)
- Domino Network Settings : cliquer (Customize…)



- Cocher ☒*Compress* pour bénéficier de la compression réseau
- Cocher ☒*Encrypt* pour activer le chiffrement des données sur réseau
- Cliquer (OK), puis (Next)
- Secure your Domino Server : laisser les options par défaut et cliquer (Next)
- Vérifier les choix, puis Cliquer (< Back) pour modifier une ou des options ou cliquer (Setup)
- Lancer le serveur Domino comme application
- Taper la commande console TRACE pour vérifier l'accès aux serveur d'intranet, par exemple :

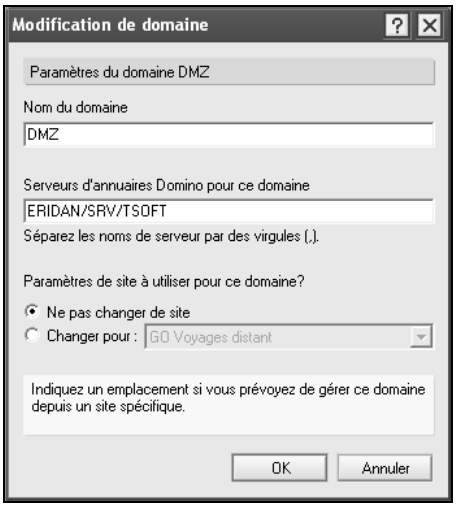
```
> trace cassiopee/srv/gov
10/11/2006 10:02:17   Remote console command issued by
_Administrateur/TSOFT: trace cassiopee/srv/gov
10/11/2006 10:02:17   Network: Determining path to server
CASSIOPEE/SRV/GOV
10/11/2006 10:02:17   Network: Available Ports:  TCPIP
10/11/2006 10:02:17   Network: Checking normal priority connection
documents only...
10/11/2006 10:02:17   Network: Allowing wild card connection
documents...
10/11/2006 10:02:17   Network: Enabling name service requests and
probes...
10/11/2006 10:02:17   Network: Checking for CASSIOPEE/SRV/GOV on
TCPIP using address 'CASSIOPEE'
10/11/2006 10:02:17   Network:   Requesting IP Address for
CASSIOPEE from DNS
10/11/2006 10:02:17   Network:   DNS returned address 192.168.0.4
for CASSIOPEE
10/11/2006 10:02:36   Network:   Connected to server
CASSIOPEE/SRV/TSOFT
```

Ajout du domaine DMZ dans Administrator

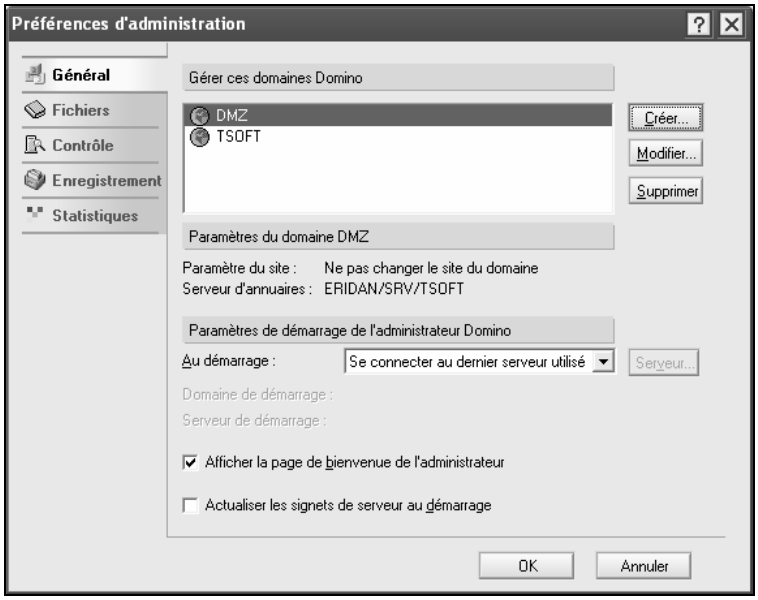
- Vérifier que le serveur Domino de DMZ est accessible depuis l'intranet depuis la station d'administration.

L'accès direct de la station d'administration au serveur Domino sera remplacé rapidement par l'utilisation des serveurs Domino d'intranet pour servir de relais vers le serveur en DMZ.

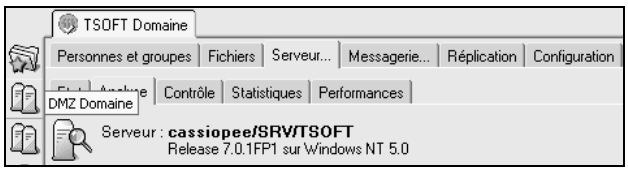
- Lancer Domino Administrator
- Commande Fichier/Préférences/Préférences d'administration…
- Cliquer (Créer)



- <Nom du domaine> : taper le nom du domaine qui vient d'être créé, ici *DMZ*
- <Serveurs d'annuaires Domino pour ce domaine> : taper le nom du serveur Domino qui vient d'être créé, ici *ERIDAN/SRV/TSOFT*
- Cliquer (OK)



Le nouveau domaine apparaît dans la liste.



Un deuxième groupe de serveurs – DMZ Domaine – apparaît dans la barre de signets de Domino Administrator. Il est ainsi possible en cliquant sur cette icône de se connecter sur le serveur en DMZ, puis de revenir sur le domaine d'intranet en cliquant sur l'icône appropriée.

Configuration sécurité Domino

La sécurité est plus restrictive que sur un serveur Domino d'intranet :

- Accès limité aux serveurs Domino et aux administrateurs,
- Exécution des agents restreinte aux signatures d'administrateur. La signature du serveur est exclue parce que l'ID de serveur n'a pas de mot de passe et sa signature n'est donc pas fiable dans l'environnement de DMZ.

Par ailleurs, l'utilisation de relais Lotus Domino est mise en place :

- Le serveur de DMZ, ici ERIDAN/SRV/TSOFT accepte de servir de relais à un client Notes connecté en DMZ pour atteindre les serveurs d'intranet : restriction aux administrateurs,
- Les serveurs d'intranet acceptent de servir de relais à un client Notes connecté en intranet pour atteindre les serveurs d'intranet : restriction aux administrateurs,
- Le serveur de DMZ accepte d'être atteint via un relais en intranet : restriction aux administrateurs et aux serveurs.

Groupes à modifier en Intranet

Le groupe OtherDomainServers est destiné à recevoir les noms de serveurs appartenant aux autres domaines Domino de l'organisation.

Groupe	Type	Membres
OtherDomainServers	LCA uniquement	ERIDAN/SRV/TSOFT

Groupes à créer en Intranet

Les serveurs d'intranet en communication avec le serveur Domino en DMZ doivent pouvoir servir de relais aux administrateurs et aux autres serveurs du domaine Domino d'intranet. Pour chacun des serveurs faisant relais, ici CASSIOPEE :

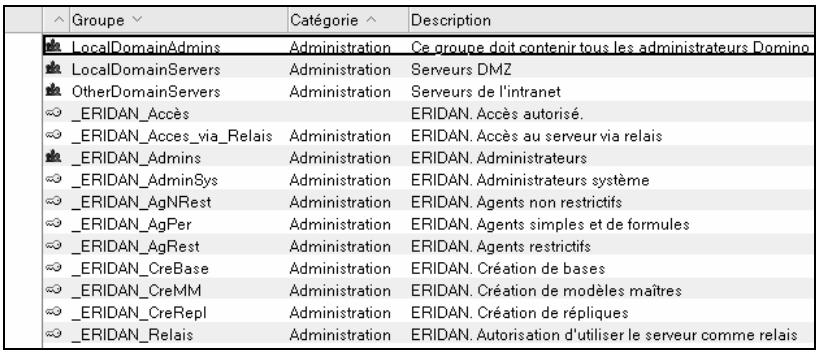
Groupe	Type	Membres
Accès au serveur via relais		
*_CASSIOPEE_*Acces*_via_Relais*	LCA uniquement	*_NomduServeur_*Admins_ OtherDomainServers
Autoriser l'utilisation du serveur comme relais		
_CASSIOPEE_Relais	LCA uniquement	*_NomduServeur_*Admins LocalDomainServers

Groupes à modifier en DMZ

Le groupe OtherDomainServers correspond aux serveurs de l'intranet devant communiquer avec le serveur ERIDAN en DMZ notamment pour les réplications.

Groupe	Type	Membres
OtherDomainServers	LCA uniquement	Serveurs d'intranet

Groupes à créer en DMZ



Groupe	Catégorie	Description
LocalDomainAdmins	Administration	Ce groupe doit contenir tous les administrateurs Domino
LocalDomainServers	Administration	Serveurs DMZ
OtherDomainServers	Administration	Serveurs de l'intranet
_ERIDAN_Accès		ERIDAN. Accès autorisé.
_ERIDAN_Acces_via_Relais	Administration	ERIDAN. Accès au serveur via relais
_ERIDAN_Admins	Administration	ERIDAN. Administrateurs
_ERIDAN_AdminSys	Administration	ERIDAN. Administrateurs système
_ERIDAN_AgNRest	Administration	ERIDAN. Agents non restrictifs
_ERIDAN_AgPer	Administration	ERIDAN. Agents simples et de formules
_ERIDAN_AgRest	Administration	ERIDAN. Agents restrictifs
_ERIDAN_CreBase	Administration	ERIDAN. Création de bases
_ERIDAN_CreMM	Administration	ERIDAN. Création de modèles maîtres
_ERIDAN_CreRepl	Administration	ERIDAN. Création de répliques
_ERIDAN_Relais	Administration	ERIDAN. Autorisation d'utiliser le serveur comme relais

Groupe	Type	Membres
_*ERIDAN*_Intrus	Liste des intrus uniquement	-vide-
_ *ERIDAN* _Acces	LCA uniquement	_ *ERIDAN* _*Admins* *OtherDomainServers*
Administrateurs du serveur		
_ *ERIDAN* _Admins	Multifonction	_*Administrateur/TSOFT* Autres administrateurs
Administrateur système pour l'utilisation de commandes de l'OS		
_ *ERIDAN* _AdminSys	LCA uniquement	_ *ERIDAN* _*Admins*
Créer bases et modèles (par défaut tout le monde)		
_ *ERIDAN* _CreBase	LCA uniquement	_ *ERIDAN* _*Admins* LocalDomainServers
Créer de nouvelles répliques de bases (par défaut personne)		
_ *ERIDAN* _CreRepl	LCA uniquement	_ *ERIDAN* _Admins_ LocalDomainServers
Créer des modèles maîtres		
_ *ERIDAN* _CreMM	LCA uniquement	_ *ERIDAN* _Admins_
Exécuter les agents simples et de formules		
_ *ERIDAN* _AgPer	LCA uniquement	_*Administrateur*/*TSOFT* *Lotus Notes Template Development/Lotus Notes*
Exécuter les agents LotusScript/Java restrictifs		
_ *ERIDAN* _AgRest	LCA uniquement	_*Administrateur*/*TSOFT* *Lotus Notes Template Development/Lotus Notes*
Exécuter des méthodes et des opérations non restrictives		
_ *ERIDAN* _AgNRest	LCA uniquement	_*Administrateur*/*TSOFTnom du serveur*
Accès au serveur via relais		
_ *ERIDAN* _Acces_*via*_*Relais*	LCA uniquement	_ *ERIDAN* _Admins_ OtherDomainServers
Autoriser l'utilisation du serveur comme relais		
_ *ERIDAN* _*Relais*	LCA uniquement	_ *ERIDAN* _Admins

Modification du document de serveur en DMZ

Administrateurs	
Administrateurs avec accès total :	_Administrateur/TSOFT
Administrateurs :	_ERIDAN_Admins
Administrateurs de base :	
Administrateurs de console à distance :	
Administrateurs en consultation uniquement :	
Administrateur système :	_ERIDAN_AdminSys
Administrateur système à accès limité :	
Commandes système à accès limité :	
Obsolète à compter de Domino 6 : Administrer le serveur à partir d'un navigateur :	

La sécurité est simplifiée pour le serveur DMZ : les droits sont donnés à quelques administrateurs et aux serveurs. Ce modèle est applicable comme solution minimum pour un serveur d'intranet.

Restrictions de programmabilité	Autorisation pour -
Exécuter des méthodes et des opérations non restrictives :	_ERIDAN_AgNRest
Signer des agents à exécuter pour le compte de quelqu'un d'autre :	_ERIDAN_AgNRest
Signer des agents à exécuter pour le compte de l'utilisateur appelant cet agent :	_ERIDAN_AgNRest
Exécuter les agents LotusScript/Java restrictifs :	_ERIDAN_AgRest
Exécuter les agents simples et de formule :	_ERIDAN_AgPer
Signer des bibliothèques de script à exécuter pour le compte de quelqu'un d'autre :	_ERIDAN_AgNRest
Les paramètres suivants sont obsolètes à partir de Domino 6. Ils sont utilisés uniquement à des fins de compatibilité avec les versions précédentes :	
Exécuter les agents Java/Javascript/COM restrictifs :	
Exécuter les agents Java/Javascript/COM non restrictifs :	

La section concernant la sécurité des agents est complétée comme pour un serveur d'intranet. C'est le contenu des groupes qui détermine des restrictions importantes en DMZ.

Accès à Internet	
Authentification Internet :	Moins de variantes de noms et plus de sécurité

L'authentification Internet est renforcée au maximum en permettant peu de variantes d'identification.

Utilisation de relais	Autorisation pour -
Accès au serveur :	_ERIDAN_Acces_via_Relais
Autoriser le routage à :	_ERIDAN_Relais
Autoriser l'appel à :	
Destinations autorisées :	

L'utilisation du serveur de DMZ comme relais est renseignée : des champs vides correspondent à une interdiction.

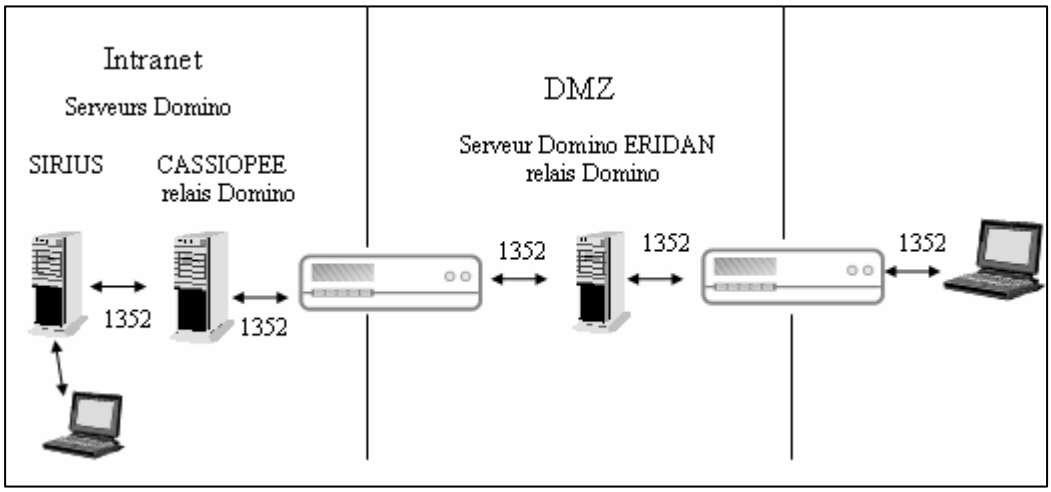
Paramètres de sécurité	
Comparer les clés publiques :	Appliquer la vérification de clés uniquement aux utilisateurs Notes et serveurs Domino répertoriés dans les annuaires sécurisés
Consigner les incompatibilités de clés publiques :	Consigner les incompatibilités de clés uniquement pour les utilisateurs Notes et serveurs Domino répertoriés dans les annuaires sécurisés
Autoriser les connexions Notes anonymes :	○ Oui ◉ Non
Vérifier le mot de passe d'authentification des ID Notes :	○ Activé ◉ Désactivé

Accès serveur	Autorisation pour -
Accès au serveur autorisé :	_ERIDAN_Accès
Accès au serveur interdit :	_ERIDAN_Intrus
Créer bases et modèles :	_ERIDAN_CreBase
Créer de nouvelles répliques :	_ERIDAN_CreRepl
Créer modèles maîtres :	_ERIDAN_CreMM
Autorisé(s) à utiliser les contrôles	
Non autorisé(s) à utiliser les contrôles :	
Serveurs accrédités :	

Les serveurs d'intranet et les utilisateurs peuvent s'authentifier auprès du serveur de DMZ parce qu'ils appartiennent tous à la même organisation, ici /TSOFT. Des contrôles supplémentaires peuvent être ajoutés en comparant la clé publique présentée à l'authentification avec celle enregistrée dans l'annuaire. Il est conseillé de ne pas mettre cette option en place tant que les annuaires ne sont pas opérationnels.

Activation du relais en intranet

La section Utilisation de relais est modifiée pour les serveurs ayant besoin de communiquer avec le serveur en DMZ soit directement, soit indirectement via un serveur assurant le relais. La station d'administration est également configurée pour faire du relais.



Serveur assurant le relais

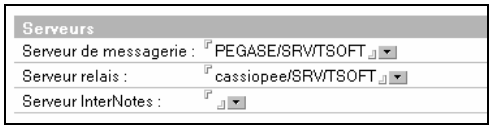
Utilisation de relais	Autorisation pour -
Accès au serveur :	_CASSIOPEE_Acces_via_Relais
Autoriser le routage à :	_CASSIOPEE_Relais
Autoriser l'appel à :	
Destinations autorisées :	

- Modifier le document serveur approprié, ici CASSIOPEE
- Redémarrer le serveur
- Taper la commande `TRACE ERIDAN/SRV/TSOFT` pour vérifier la connexion

```
> trace eridan/srv/tsoft
10/11/2006 14:23:42   Network: Determining path to server
ERIDAN/SRV/TSOFT
10/11/2006 14:23:42   Network: Available Ports:  TCPIP
10/11/2006 14:23:42   Network: Checking normal priority connection
documents only...
10/11/2006 14:23:42   Network: Local network connection document
found for ERIDAN/SRV/TSOFT
10/11/2006 14:23:42   Network:   Verifying address 'ERIDAN' for
ERIDAN/SRV/TSOFT on TCPIP
10/11/2006 14:23:42   Network:     Requesting IP Address for ERIDAN
from DNS
10/11/2006 14:23:42   Network:     DNS returned address 192.168.0.3
for ERIDAN
10/11/2006 14:23:42   Network:   Connected to server ERIDAN/SRV/TSOFT
```

Le serveur d'intranet dispose d'une connexion opérationnelle vers le serveur DMZ.

Serveurs communiquant avec DMZ via le relais

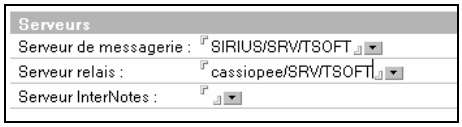


- Modifier le document du premier serveur concerné, ici PEGASE
- Cliquer l'onglet (Général), puis la section Informations de site du serveur
- <Serveur relais> : sélectionner *CASSIOPEE/SRV/TSOFT*
- Redémarrer le serveur
- Taper la commande `TRACE ERIDAN/SRV/TSOFT` pour vérifier la connexion

```
> trace eridan/srv/tsofr
10/11/2006 14:35:52   Network: Determining path to server
ERIDAN/SRV/TSOFR
10/11/2006 14:35:52   Network: Available Ports:  TCPIP
10/11/2006 14:35:52   Network: Checking normal priority connection
documents only...
10/11/2006 14:35:52   Network: Allowing wild card connection
documents...
10/11/2006 14:35:52   Network: Enabling name service requests and
probes...
10/11/2006 14:35:52   Network: Checking for ERIDAN/SRV/TSOFR on TCPIP
using address 'ERIDAN'
10/11/2006 14:35:52   Network:   Requesting IP Address for ERIDAN
from DNS
10/11/2006 14:35:54   Network:   DNS did not return an IP address for
ERIDAN
10/11/2006 14:35:54   Network:   Unable to connect to
ERIDAN/SRV/TSOFR on TCPIP (The remote server is not a known TCP/IP
host.)
10/11/2006 14:35:54   Network: Checking low and normal priority
connection documents...
10/11/2006 14:35:54   Network: The default passthru server is
cassiopee/SRV/TSOFT
10/11/2006 14:35:54   Network: Searching for path to
cassiopee/SRV/TSOFT
10/11/2006 14:35:54   Network:   Local network connection document
found for cassiopee/SRV/TSOFT
10/11/2006 14:35:54   Network:     Verifying address 'cassiopee' for
```

```
cassiopee/SRV/TSOFT on TCPIP
10/11/2006 14:35:54   Network:         Using address '192.168.0.4'
for cassiopee/SRV/TSOFT on TCPIP
10/11/2006 14:35:54   Network:     cassiopee/SRV/TSOFT is available
on TCPIP
10/11/2006 14:35:54   Network: Pass through cassiopee/SRV/TSOFT to
connect to ERIDAN/SRV/TSOFR
10/11/2006 14:35:54   Network: Connecting to cassiopee/SRV/TSOFT over
TCPIP
10/11/2006 14:35:54   Network:   Using address '192.168.0.4' for
cassiopee/SRV/TSOFT on TCPIP
10/11/2006 14:35:54   Network session      25B: Buffer size = 4000
10/11/2006 14:35:54   Network session      25B: Path length = 1,
including 0 slow links
10/11/2006 14:35:54   Network session      25B: Connected to
cassiopee/SRV/TSOFT
10/11/2006 14:35:54   Network session      25B: Authenticating with
cassiopee/SRV/TSOFT
10/11/2006 14:35:54   Network session      25B: Asking server for
connection to ERIDAN/SRV/TSOFR10/11/2006 14:23:42   Network:
Determining path to server ERIDAN/SRV/TSOFT
10/11/2006 14:23:42   Network: Available Ports:  TCPIP
10/11/2006 14:23:42   Network: Checking normal priority connection
documents only...
10/11/2006 14:23:42   Network: Local network connection document
found for ERIDAN/SRV/TSOFT
10/11/2006 14:23:42   Network:   Verifying address 'ERIDAN' for
ERIDAN/SRV/TSOFT on TCPIP
10/11/2006 14:23:42   Network:     Requesting IP Address for ERIDAN
from DNS
10/11/2006 14:23:42   Network:     DNS returned address 192.168.0.3
for ERIDAN
10/11/2006 14:23:42   Network:   Connected to server ERIDAN/SRV/TSOFT
```

La trace montre que le serveur d'intranet SIRIUS cherche d'abord à accéder au serveur de DMZ ERIDAN par accès à la DNS. Ceci s'avérant infructueux, le serveur s'adresse à son serveur relais CASSIOPEE qui effectue le relais.



- Modifier le document du serveur concerné suivant, ici SIRIUS
- Cliquer l'onglet (Général), puis la section Informations de site du serveur
- <Serveur relais> : sélectionner *CASSIOPEE/SRV/TSOFT*
- Redémarrer le serveur
- Taper la commande `TRACE ERIDAN/SRV/TSOFT` pour vérifier la connexion

Station d'administration en accès local

Cette configuration doit être effectuée uniquement si la station d'administration n'a pas un accès LAN au réseau TCP de DMZ.

- Modifier le site Bureau de chaque station d'administration

- <Serveur relais> : taper le nom du serveur d'intranet assurant le relais vers la DMZ, ici CASSIOPEE/SRV/TSOFT

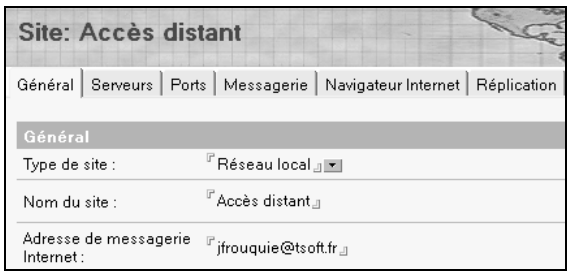
Pour tester la connexion :

- Placer la station d'administration dans un contexte de connexion au LAN interne d'intranet
- Lancer Lotus Notes
- Commande *Fichier/Préférences/Préférences utilisateur*...
- Cliquer (Ports), puis (Historique)
- <Serveur de destination> : taper le nom le nom du serveur de DMZ à atteindre, ici *ERIDAN/SRV/TSOFT*

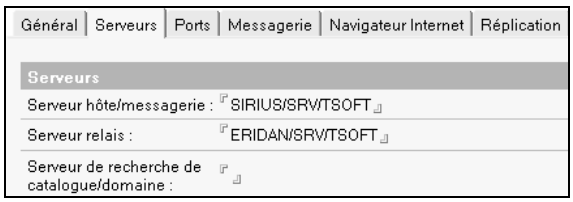
La trace doit montrer une connexion sur le serveur ERIDAN en passant par le serveur de messagerie puis le serveur CASSIOPEE.

Station d'administration en accès distant

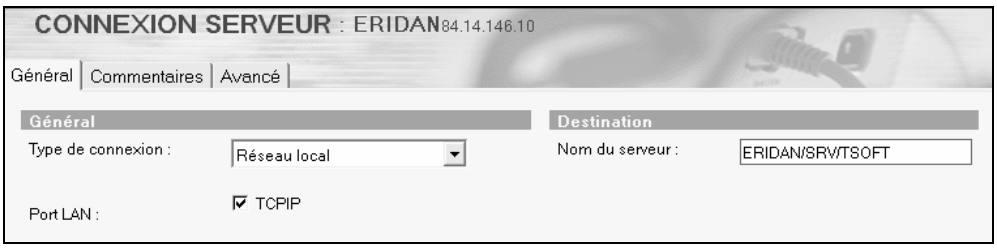
Par ailleurs, si l'administrateur doit accéder aux serveurs Domino depuis son portable via Internet, il faut configurer un site spécial « Accès distant » de type LAN et c'est le serveur de DMZ – accédé par son adresse publique – qui sert de relais vers les serveurs d'intranet. Le document site est associé à un document de connexion dans le carnet d'adresses local de la station names.nsf.



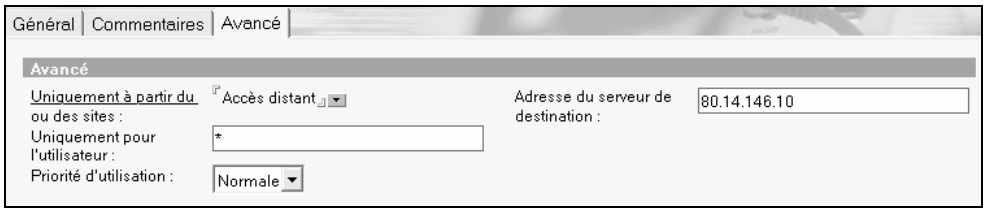
- Créer le document site *Accès distant* de type *Réseau local* sur la station d'administration



- <Serveur hôte/messagerie> : taper le nom du serveur de messagerie de l'administrateur, ici *SIRIUS/SRV/TSOFT*
- <Serveur relais> : taper le nom du serveur Domino en DMZ, ici *ERIDAN/SRV/TSOFT*



- Créer un document de connexion de type *Réseau local*
- <Nom du serveur> : taper le nom du serveur Domino en DMZ, ici *ERIDAN/SRV/TSOFT*



- <Uniquement à partir du ou des sites> : sélectionner Accès distant. La connexion n'est utilisable que depuis le réseau public
- <Adresse du serveur de destination> : taper l'adresse publique du serveur, ici l'adresse purement imaginaire *80.14.146.10.* Le firewall mappe les demandes sur le port 1352 à cette adresse sur l'adresse interne du serveur Domino en DMZ

Pour tester la connexion :

- Placer la station d'administration dans un contexte de connexion sur l'adresse publique
- Lancer Lotus Notes
- Commande *Fichier/Préférences/Préférences utilisateur…*
- Cliquer (Ports), puis (Historique)
- <Serveur de destination> : taper le nom le nom du serveur d'intranet à atteindre, ici *SIRIUS/SRV/TSOFT*

```
Recherche du chemin d'accès au serveur SIRIUS/SRV/TSOFT
Ports disponibles :  TCPIP
Vérification des documents de connexion de priorité normale
uniquement...
Document de connexion Relais  trouvé pour SIRIUS/SRV/TSOFT via
ERIDAN/SRV/TSOFT
Recherche du chemin vers ERIDAN/SRV/TSOFT
  document de connexion Réseau local  trouvé pour ERIDAN/SRV/TSOFT
    Vérification de l'adresse '80.14.146.10' de ERIDAN/SRV/TSOFT sur
TCPIP
    ERIDAN/SRV/TSOFT est disponible sur TCPIP
Utilisez le serveur ERIDAN/SRV/TSOFT comme relais pour vous connecter
au serveur SIRIUS/SRV/TSOFT
Connexion à ERIDAN/SRV/TSOFT via TCPIP en cours
  Utilisation de l'adresse '84.14.146.10' pour ERIDAN/SRV/TSOFT sur
TCPIP
Connecté à ERIDAN/SRV/TSOFT
Authentification de ERIDAN/SRV/TSOFT
Demande au serveur de connexion à SIRIUS/SRV/TSOFT
  Ajouter un serveur CASSIOPEE/SRV/TSOFT vers le chemin d'accès
```

```
Le port du serveur relais sera TCPIP
Sur le serveur relais, connecter au CASSIOPEE/SRV/TSOFT
Connecté à CASSIOPEE/SRV/TSOFT
Authentification de CASSIOPEE/SRV/TSOFT
Demande au serveur de connexion à SIRIUS/SRV/TSOFT
  Le port du serveur relais sera TCPIP
  Sur le serveur relais, connecter au SIRIUS/SRV/TSOFT
  Connecté à SIRIUS/SRV/TSOFT
  Connecté au serveur SIRIUS/SRV/TSOFT
```

Le chemin suivi est affiché :

- La connexion à SIRIUS est possible via ERIDAN
- ERIDAN est accédé par son adresse publique
- L'authentification avec ERIDAN s'effectue
- ERIDAN ne sait pas comment accéder à SIRIUS et passe la demande à CASSIOPEE
- L'authentification auprès de CASSIOPEE s'effectue
- CASSIOPEE fait le relais vers SIRIUS
- L'authentification avec SIRIUS s'effectue

Installation réplique de l'annuaire en DMZ

L'identité des destinataires du courrier SMTP entrant doit être vérifié dans l'annuaire de l'intranet. Une réplique locale est installée en DMZ.

Création de la réplique

- Modifier la LCA de l'annuaire en intranet
  – OtherDomainServers doit être lecteur
  – Anonymous est interdit d'accès
- Copier l'annuaire names.nsf depuis le serveur gestionnaire de l'annuaire vers le serveur Domino en DMZ en la renommant, ici *TSOFTnames.nsf*

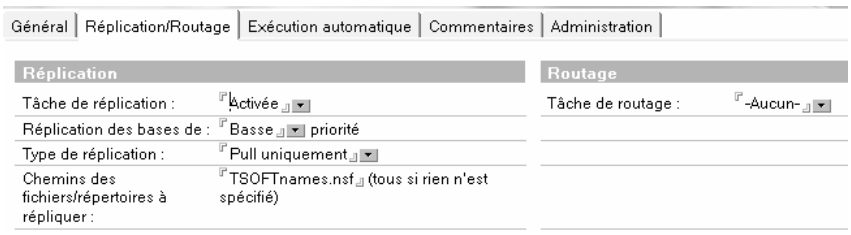
Ou

- Ouvrir la base depuis Lotus Notes et créer une réplique sur le serveur DMZ

Planifier la réplication

- Créer un document de réplication de l'annuaire d'intranet, ici TSOFTnames.nsf, dans l'annuaire du domaine DMZ sur le serveur DMZ

- <Serveur source> : c'est nécessairement le serveur DMZ puisque le document de connexion est dans l'annuaire names.nsf du domaine DMZ, ici *ERIDAN/SRV/TSOFT*
- <Serveur de destination> : de préférence, le serveur avec lequel il ny a une connexion directe, ici *CASSIOPEE/SRV/TSOFT*



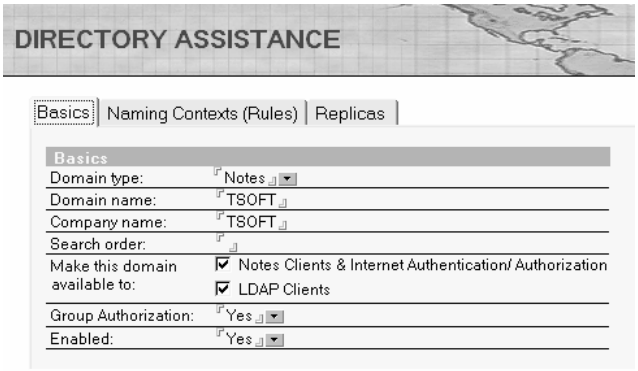
- <Type de réplication> : sélectionner *Pull uniquement*. La LCA n'autorise pas le retour de modifications de DMZ vers l'intranet et Push est donc inutile
- <Chemin des fichiers/répertoires à répliquer> : taper le nom de l'annuaire de l'intranet sur le serveur de DMZ, ici *TSOFTnames.nsf*

- Choisir une réplication toutes les six heures ce qui est en principe suffisant

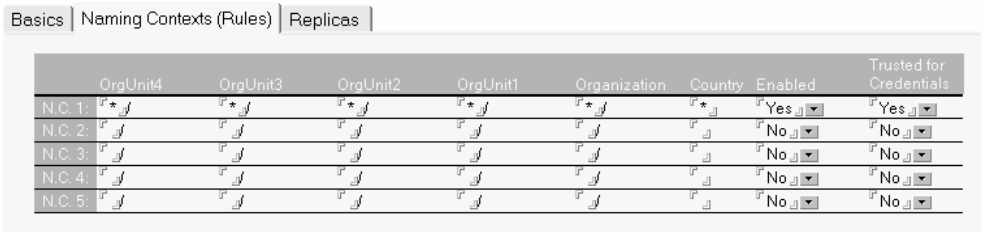
Configurer l'assistance d'annuaire

La base doit être définie dans l'assistance d'annuaire pour pouvoir être service par LDAP. La procédure détaillée de création de l'assistance d'annuaire est vue dans ↳Module Annuaires.

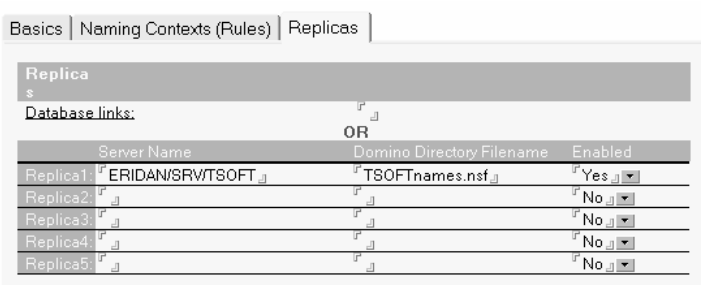
- Créer la base d'assistance d'annuaire DA.NSF sur le serveur DME
- Créer un document d'assistance d'annuaire



- Taper le nom du domaine d'intranet
- Autoriser cet annuaire pour les clients Notes, l'authentification Internet (pour les itinérants connectés par HTTPS) et pour les clients LDAP



- Compléter les règles de contexte de nom comme indiqué



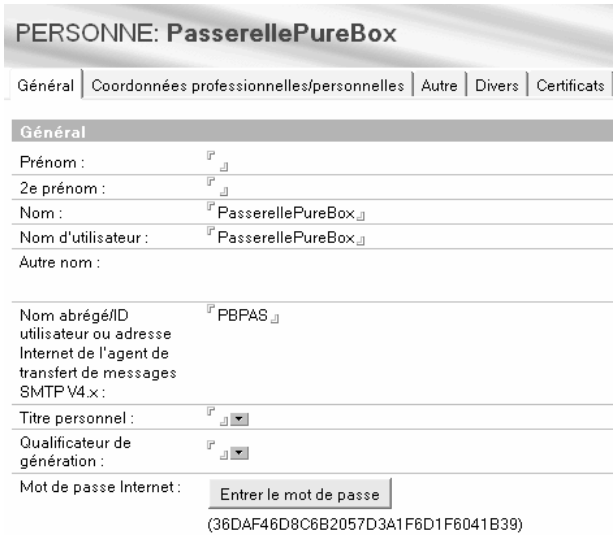
- Indiquer où se trouve la réplique : le nom du fichier sur le serveur de DMZ, ici *TSOFTnames.nsf* sur *ERIDAN/SRV/TSOFT*

- Taper le nom de la base d'assistance d'annuaire, ici DA.NSF, dans le document du serveur de DMZ, ici ERIDAN/SRV/TSOFT

Configuration LDAP pour passerelle SMTP

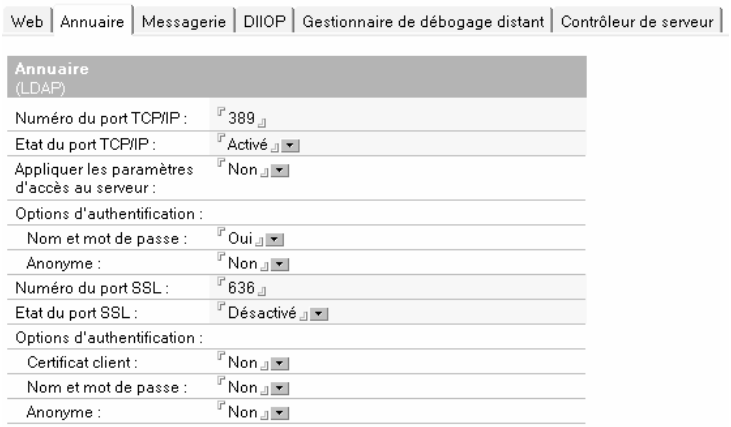
La passerelle SMTP doit faire un accès authentifié à l'annuaire par LDAP. Un utilisateur est enregistré dans l'annuaire Domino du domaine DMZ pour les besoins de l'authentification.

Authentification de la passerelle



- Ouvrir l'annuaire Domino du domaine DMZ
- Ouvrir la vue Personnes, puis cliquer (Ajouter une personne)
- <Prénom> : zone non obligatoire
- <Nom> : zone obligatoire, ici, ici *PasserellePureBox* car la passerelle SMTP de l'exemple est un boîtier PureBox proposé par Sophos et Dataswift
- <Nom d'utilisateur> : taper à nouveau le nom, ici *PasserellePureBox*
- Entrer un mot de passe associé
- <Système de messagerie> : sélectionner aucun

Configuration LDAP sur le serveur Domino



- Ouvrir le document du serveur DMZ
- Cliquer sur l'onglet (Ports), puis (Ports Internet), puis (Annuaire)
- Désactiver l'option d'authentification anonyme
- Vérifier que le NOTES.INI du serveur contient bien la tâche LDAP dans la ligne `ServerTasks=`

Configuration LDAP sur la passerelle

Cette configuration dépend bien sur du logiciel serveur SMTP utilisé. Pour PostFix, la configuration se fait dans le fichier main.cf.

```
ldapaliases1_server_host = eridan
ldapaliases1_search_base = /
ldapaliases1_query_filter = (&(ObjectClass=dominoPerson)
(|(cn=%s) (mail=%s)) )
ldapaliases1_result_attribute = mail
ldapaliases1_bind = yes
ldapaliases1_bind_dn = cn=PasserellePureBox
ldapaliases1_bind_pw = xxxxxxxxx
```

L'utilisateur de connexion et le mot de passé correspondent à ce qui a été saisi précédemment dans l'annuaire du domaine DMZ.

Le filtre de requête s'interprète de la façon suivante :

– search_base : Recherche à partir de la racine. Une recherche dans une unité d'organisation serait possible mais n'est pas utilisée ici,

– query_fliter : recherche des documents de type Personne ET une correspondance sur la partie nom propre (CN) OU sur l'adresse de messagerie (mail).

Modification topologie de routage de courrier

Le routage du courrier se fait depuis un serveur d'intranet – ici CASSIOPEE/SRV/TSOFT – directement vers une passerelle SMTP. La modification de configuration consiste :

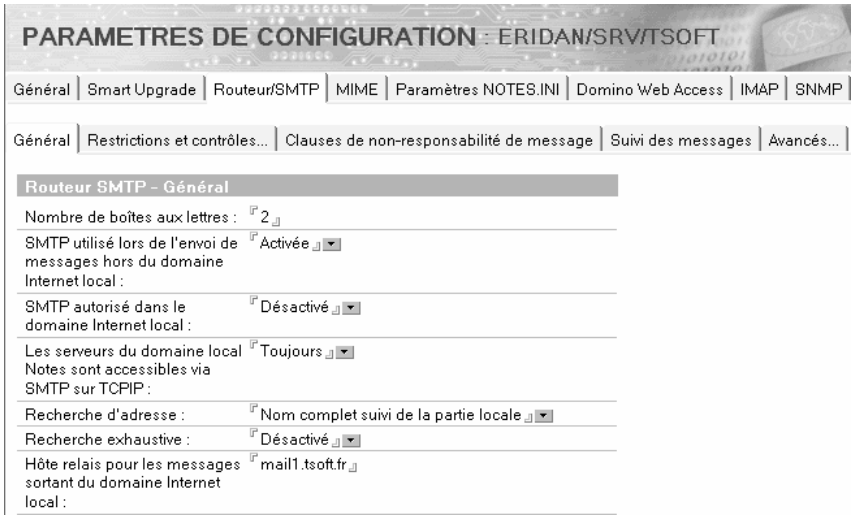
– A activer l'envoi et la réception de messages SMTP sur le serveur de DMZ, ici ERIDAN/SRV/TSOFT
– A envoyer les messages entrants du domaine Domino DMZ vers le domaine Domino d'intranet, ici TSOFT,
– A envoyer les messages sortants du domaine Domino d'intranet, ici TSOFT, vers le domaine Domino DMZ pour envoi vers l'Internet.

Activation serveur SMTP sur serveur Domino DMZ

- Modifier le document du serveur de DMZ, ici *ERIDAN/SRV/TSOFT*

Numéro de version du serveur :	Release 7.0.1FP1
Tâches de routage :	Routage du courrier
Tâche d'écoute SMTP :	Activée
Numéro(s) de téléphone du serveur :	
Nombre de CPU :	1
Système d'exploitation :	Windows/2000 5.0 Intel Pentium

- <Tache d'écoute SMTP> : sélectionner *Activée*
- Modifier le document de configuration du serveur
- Cliquer (Routeur/SMTP), puis (Général)
- <SMTP utilisé lors de l'envoi de messages hors du domaine Internet local> : sélectionner Activée
- <Hôte relais pour les messages sortant du domaine Internet local> : taper l'adresse de la passerelle SMTP, ici *mail1.tsoft.fr*. Ce peut être aussi l'adresse IP



- Cliquer (Restrictions et contrôles), puis (Contrôle SMTP en entrée)
- <Autoriser uniquement l'envoi aux domaines Internet suivant> : taper le ou les domaines Internet de messagerie gérés en intranet, ici tsoft.fr

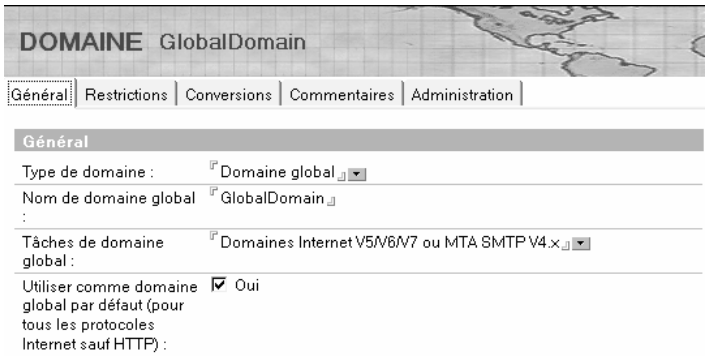
- <Autoriser uniquement les connexions de ces hôtes/adresses IP Internet SMTP> : taper l'adresse de la passerelle SMTP, ici *mail1.tsoft.fr* ou son adresse IP

Le contrôle de l'existence des destinataires étant fait dans l'annuaire, il n'y a pas lieu de l'ajouter ici.

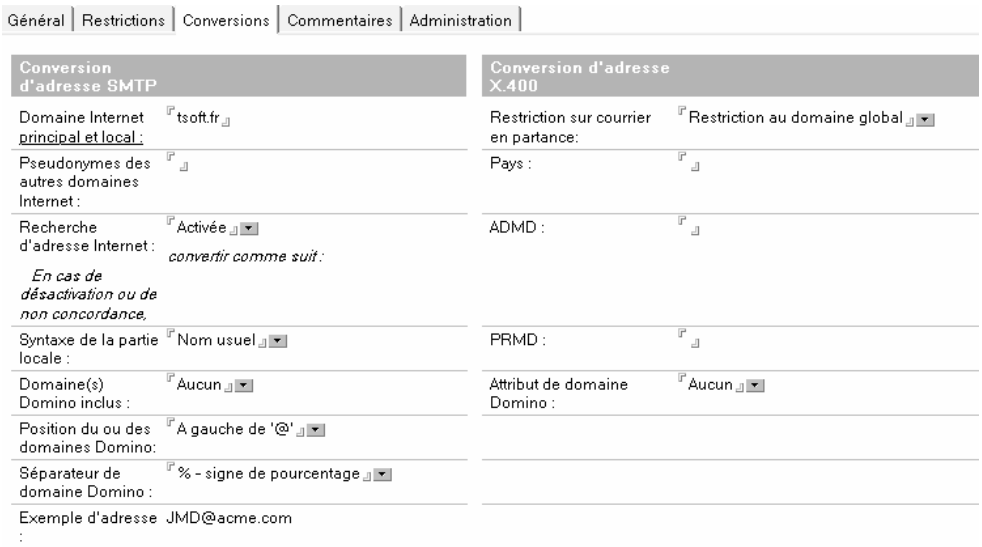
Configuration du routage de courrier en DMZ

Les messages reçus pour le domaine Internet interne sont envoyés vers le serveur d'intranet.

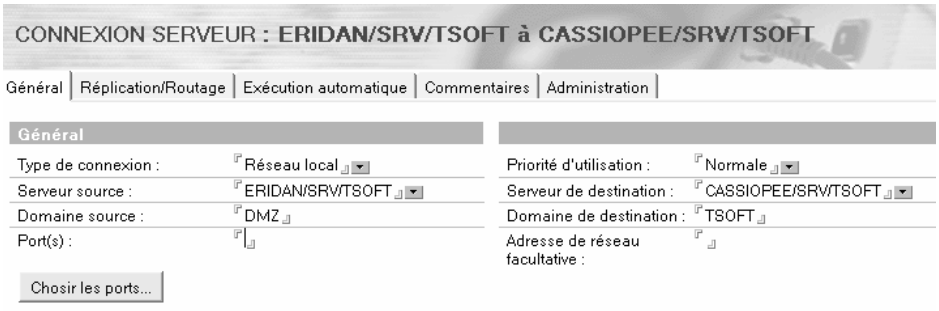
- Cliquer (Configuration)
- Cliquer *Messagerie/Domaines*



- Cliquer (Nouveau domaine)
- <Type de domaine> : sélectionner Domaine Global
- Compléter les champs comme indiqué
- Cliquer (Conversion)
- <Domaine Internet principal et local> : taper le nom du domaine Internet principal géré en intranet, ici tsoft.fr
- <Recherche d'adresse Internet> : sélectionner Activée

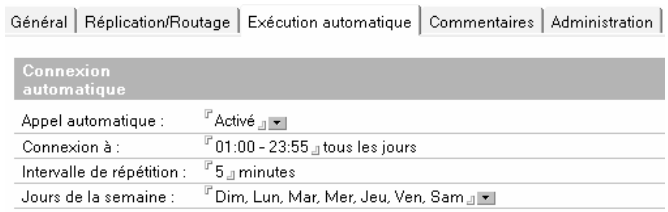


Pour plus ample information, se reporter à la conversion des adresses dans ↳Module Messagerie.



- Créer un document de connexion dans l'annuaire du domaine DMZ
- <Serveur source> : c'est nécessairement le serveur DMZ puisque le document de connexion est dans l'annuaire names.nsf du domaine DMZ, ici *ERIDAN/SRV/TSOFT*
- <Serveur de destination> : de préférence, le serveur avec lequel il y a une connexion directe, ici *CASSIOPEE/SRV/TSOFT*
- <Domaine source> : taper le nom du domaine Domino de DMZ, ici *DMZ*
- <Domaine de destination> : taper le nom de domaine Domino d'intranet, ici *TSOFT*

- <Tâche de routage> : sélectionner Routage de courrier (port 1352)
- <Envoi immédiat si> : taper 1 pour que les messages n'attendent pas

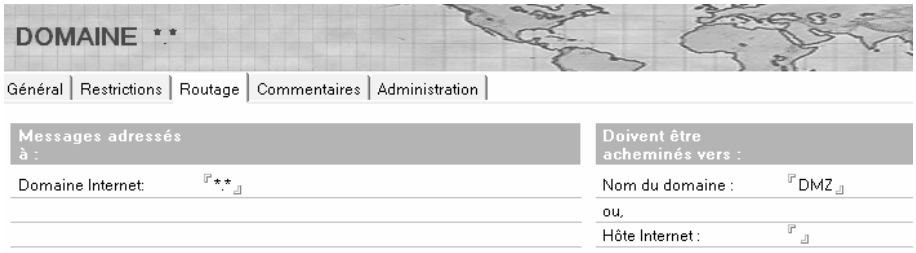


- Choisir une plage horaire et un intervalle de répétition

Configuration du routage en intranet

Les messages vers Internet doivent transiter par le domaine DMZ.

- Créer un document de connexion dans l'annuaire du domaine d'intranet, ici TSOFT
- <Serveur source> : de préférence, le serveur d'intranet avec lequel il y a une connexion directe, ici *CASSIOPEE/SRV/TSOFT*
- <Serveur de destination> : c'est le serveur en DMZ, ici *ERIDAN/SRV/TSOFT*
- <Domaine source> : taper le nom de domaine Domino d'intranet, ici *TSOFT*
- <Domaine de destination> : taper le nom du domaine Domino de DMZ, ici *DMZ*
- Compléter les champs des onglets (Réplication/Routage) et (Exécution automatique) sur le modèle du document de connexion créé précédemment
- Cliquer (Configuration)
- Cliquer *Messagerie/Domaines*
- Ouvrir le document *Domaine SMTP étranger*



- Cliquer l'onglet (Routage)
- <Nom du domaine> : remplacer *TheInternet* par *DMZ*

Le domaine Domino DMZ est maintenant vu comme passerelle SMTP vers Internet.

Désactivation SMTP sur le serveur d'intranet

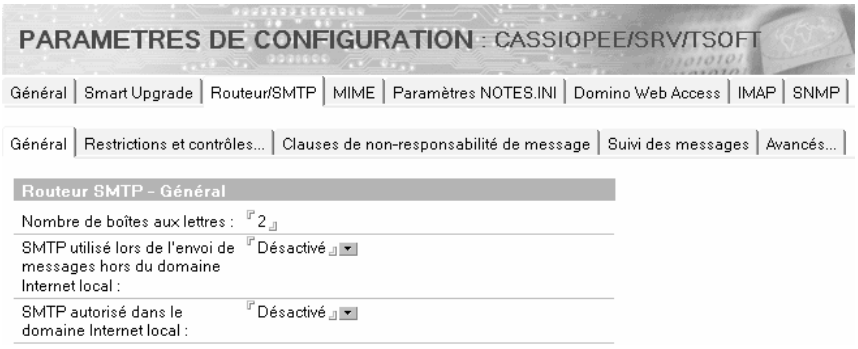
- Vérifier que les messages entrants d'Internet arrivent bien en passant par le serveur Domino en DMZ.

Si c'est le cas :

- Modifier le document du serveur d'intranet actuellement en liaison avec la passerelle SMTP, ici CASSIOPEE/SRV/TSOFT
- Désactiver la tâche d'écoute SMTP

Pour désactiver l'envoi direct des messages vers Internet :

- Modifier le document de configuration du serveur d'intranet, ici CASSIOPEE/SRV/TSOFT

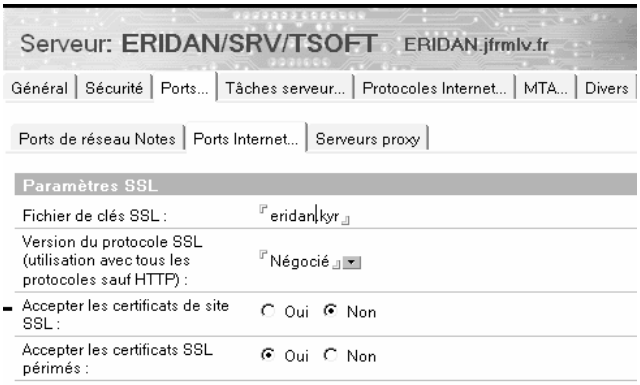


- <SMTP utilisé lors de l'envoi de messages hors du domaine Internet local> : sélectionner *Désactivé*
- Redémarrer le serveur
- Vérifier qu'un message envoyé vers Internet arrive bien à son destinataire

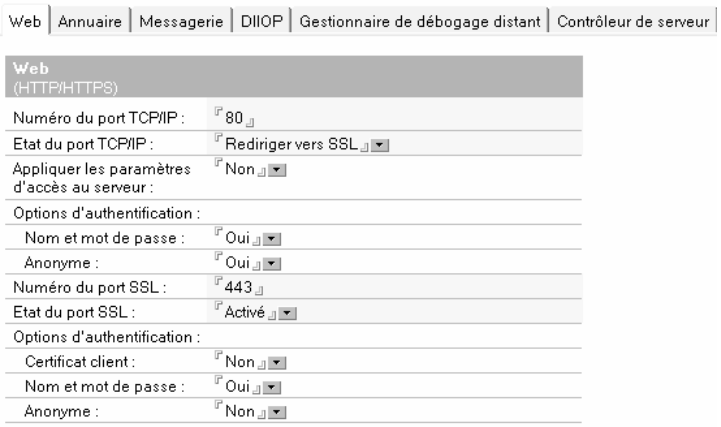
Configuration HTTPS pour l'accès distant aux bases courrier

Un jeu de clé SSL est créé et signé pour le serveur en DMZ avec un certificat SSL auto-généré interne ↳Aide Domino Administrator/Sécurité/Sécurité SSL. Ici le jeu de clés est représenté par deux fichiers eridan.kyr et eridan.sth signés avec un certificat SSL TSOFT.

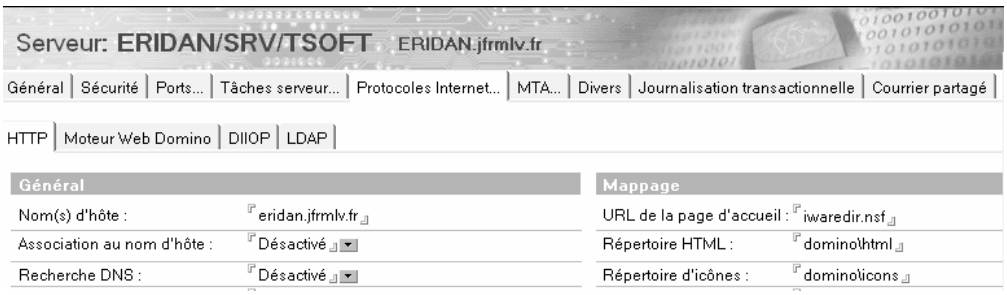
- Installer le jeu de clé – eridan.kyr et eridan.sth – dans le répertoire Domino\Data du serveur ERIDAN



- Modifier le document serveur de ERIDAN/SRV/TSOFT
- Cliquer sur l'onglet (Ports…), puis (Ports Internet…)
- <Fichier de clés SSL> : taper le nom du jeu de clé, ici eridan.kyr



- <Etat tu port TCPIP> : sélectionner *Rediriger vers SSL*
- <Options d'authentification><Anonyme> : sélectionner *Non*



- Cliquer sur l'onglet (Protocoles Internet), puis (HTTP)
- <URL de la page d'accueil> : taper le nom de la base de redirection Domino Web Access, ici IWAREDIR.NSF
- Créer la base de redirection ↳Module Messagerie.
- Vérifier que HTTP est présent dans le NOTES.INI du serveur dans la ligne `ServerTasks=`

Réplication des bases courrier en DMZ

Une base courrier accédée en DMZ doit répliquer dans les deux sens : de serveur de messagerie vers serveur DMZ et réciproquement. L'utilisateur récupère ainsi ses messages envoyés, classés et supprimés.

- Modifier la LCA des bases concernées depuis le serveur de messagerie de l'utilisateur : LocalDomainServers doit être Editeur avec le droit de supprimer les documents
- Copier par Windows les bases concernées vers le serveur de DMZ en conservant le nom du dossier mail et celui de la base
- Créer un document de réplication par serveur de messagerie dans l'annuaire du domaine Domino DMZ :
  – Le serveur Domino DMZ est le serveur source
  – Le serveur cible est un serveur de messagerie
  – Le mode est Push-Pull (défaut)
  – Taper le nom du dossier mail sur le serveur Domino DMZ, normalement *mail*
  – Activer la réplication toutes les trente minutes