

PARTIE 4

**ANNEXES EN
TÉLÉCHARGEMENT**

@ Check-lists en téléchargement

Les Check-listes sont conçues pour être utilisées
conjointement avec l'ouvrage publié aux éditions Eyrolles :
Lotus Domino 7 Administration

Check-list de planification du domaine

Initialisation du projet

A l'issue de cette phase, le contour du domaine applicatif Domino est connu, le groupe projet est constitué.

Etape	Objet	OK
1	Détermination du contour du domaine applicatif Domino : un problème et sa solution <ul style="list-style-type: none"> – courrier électronique à améliorer/développer – gestion du fax, du courrier reçu, des messages téléphoniques – informations difficilement accessibles – informations incohérentes – communication et partage d'informations à améliorer – communication avec les clients, fournisseurs, partenaires – ... 	
2	Modèle organisationnel de l'entreprise : <ul style="list-style-type: none"> – dispersion géographique – utilisateurs nomades – autonomie des filiales, bureaux... – ... 	
3	Culture informatique et ressources <ul style="list-style-type: none"> – Culture informatique des utilisateurs – Ressources techniques disponibles – Sous-traitance de la compétence technique ? de la formation ? – ... 	
4	Création du groupe projet	
	4.1 Identification du décisionnaire	
	4.2 Identification du chef de projet	
	4.3 Identification des architectes de l'infrastructure Domino	
	4.4 Identification des ressources affectées au projet : techniques, formateurs, représentants des utilisateurs	
	4.5 Identification des compétences non disponibles	
5	Définition des méthodes de conduite et de suivi de projet	
	5.1 Information des utilisateurs	
	5.2 Détermination des points de contrôle	
	5.3 Détermination du mode de suivi d'avancement : réunions, outils	
	5.4 Détermination de ce qui doit être surveillé : dates, budgets, actions...	

Analyse de l'existant

A l'issue de cette phase, la façon dont Domino apporte une réponse aux problèmes est connue, les matériels requis (serveurs) sont connus, l'emplacement et les tâches des serveurs sont définis, les modifications de l'architecture réseau sont identifiées.

Etape	Description	OK
1	Solution Domino retenue en vue de résoudre les problèmes identifiés dans le domaine applicatif. <ul style="list-style-type: none"> – Bases bibliothèques – Bases Kiosques d'informations – Messagerie – Workflow – Bases de suivi d'activité – Bases de discussion – Connexions aux bases de données de l'entreprise – Connexions à des applicatifs (ERP) – Utilisation de la réplication de bases sur serveurs – Utilisation de la réplication de bases sur portables – Accès à des bases depuis des navigateurs – Recherche de progiciels applicatifs – Tolérance de panne : serveurs en grappe 	
2	Types d'accès aux bases de documents (par applications) : <ul style="list-style-type: none"> – Accès centralisé – Accès décentralisé sur des serveurs locaux – Accès distant depuis des portables – Rôles des utilisateurs : lecture, création et modification – Accès par des utilisateurs externes (clients, fournisseurs...) 	
3	Identifier l'architecture matérielle et OS actuelle	
4	Déterminer les modifications à apporter à l'architecture pour installer les serveurs Domino et les clients Notes	
5	Contraintes pouvant affecter le déploiement <ul style="list-style-type: none"> – Coûts – Modification de l'architecture actuelle (changement d'OS) – Logiciels de maintenance : sauvegarde, anti-virus... – Délais 	
6	Détermination des rôles des serveurs Domino <ul style="list-style-type: none"> – Serveur en grappe – Courrier – Application – Service : firewall, pivot – Tâche HTTP 	
7	Réseau <ul style="list-style-type: none"> – Identification des protocoles – Topologie LAN et WAN : contraintes de bande passante – Détermination de la topologie de réseau Domino (DNN) 	

Détermination de l'architecture du domaine

A l'issue de cette phase, la topologie de propagation des informations (réplication et messagerie), le plan de nommage Notes (clients et serveurs), la politique de sécurisation de l'accès à Domino et les annuaires utilisés par la messagerie sont déterminés.

Etape	Description	OK
1	Détermination de la topologie de réplication	
	1.1 Détermination de l'emplacement des répliques	
	1.2 Détermination des fréquences de réplication	
2	Détermination de la topologie de routage de courrier	
	2.1 Détermination des domaines Domino	
	2.2 Nom du/des domaines Internet de messagerie associés	
	2.3 Découpage du domaine en réseaux nommés Domino	
	2.4 Choix des clients de messagerie : Notes, Internet	
	2.5 Choix des protocoles utilisés : NRPC, SMTP	
	2.6 Choix des serveurs connectés vers Internet	
	2.7 Accès Internet identifié et opérationnel	
	2.8 Décision de créer un domaine Domino séparé pour la DMZ	
	2.9 Choix de la passerelle SMTP : chez le fournisseur d'accès Internet ou en DMZ	
3	Utilisation de SSL et de S/MIME pour le courrier et/ou l'authentification	
4	Choix des annuaires	
	4.1 Détermination des annuaires (filiales, partenaires...) utilisés pour le routage	
	4.2 Détermination des annuaires (filiales, partenaires...) utilisés pour l'authentification	
5	Plan de nommage	
	5.1 Nom de domaine Domino	
	5.2 Nom de l'organisation	
	5.3 Nom de serveur	
	5.4 Nom de client, adresse de messagerie Internet	

	5.5	Normes de noms de groupes de sécurité et de diffusion de messages	
Etape	Description		OK
6	Règles de sécurité		
	6.1	Sécurité physique des serveurs	
	6.2	Sécurité physique des stations clientes, portables	
	6.3	Méthodes d'authentification : Notes, identifiant et mot de passe, SSL, politique de mot de passe	
	6.4	Utilisateurs accédant les serveurs, type d'accès	
	6.5	Protection des stations clientes (anti-virus, chiffrement)	
	6.6	Protection des serveurs : anti-virus et anti-spam	
	6.7	Protection réseau : firewall, proxy, chiffrement	
	6.8	Protection des bases de documents : chiffrement	
7	Migration de la messagerie existante		
	7.1	Migration des bases courrier	
	7.2	Migration des agendas	
	7.3	Migration des informations personnelles	
	7.4	Fonctions nouvelles/abandonnées	

Préparation de la mise en œuvre

A l'issue de cette phase, les standards de déploiement des serveurs et des clients sont formalisés.

Etape	Description		OK
1	Standards de serveurs		
	1.1	Organisation des bases sur les serveurs	
	1.2	Détermination des standards de tailles pour les bases	
	1.3	Détermination des standards d'installation et de configuration	
2	Standards des postes clients		
	2.1	Détermination des standards d'installation	
	2.2	Détermination des standards de configuration	

3	Plan d'installation du premier serveur et du pilote		
	3.1	Installation d'un premier serveur et de la station d'administration	
	3.2	Installation de postes clients	
	3.3	Formation des administrateurs	
	3.4	Formation des utilisateurs du pilote	
4	Plan de déploiement		
	4.1	Plan de déploiement pour les sites	
	4.2	Plan de déploiement pour les nomades	
	4.3	Formation des utilisateurs	

Check-list d'installation du premier serveur

Informations de configuration

Les informations suivantes doivent être connues :

Configuration disque. Exemple : C : (système), D : (données), journal de transaction en option (E :)	
Nom du domaine domino	
Nom du (des) domaine(s) de messagerie Internet	
Nom du serveur Domino	
Adresse IP du serveur Domino	
Adresse réseau du serveur Domino	
Adresse IP du routeur ou du firewall vers Internet	
Adresses IP des DNS si les messages ne passent pas par un serveur relais SMTP chez le fournisseur d'accès	
Nom de l'organisation Domino/Notes	
Nom du « super administrateur »	
Nom du groupe d'administrateurs	
Services Internet devant tourner sur le serveur : SMTP (obligatoire) et HTTP, POP3, LDAP	
Est-ce que des connexions à des bases relationnelles sont nécessaires (DECS) ?	
Quel est le logiciel (middleware) de connexion à la base relationnelle ?	
Serveur de fichiers (sécurisé) sur lequel seront enregistrés les fichiers ID	
Lecteur sur la station d'administration correspondant au dossier des ID sur le réseau	
Est-ce que l'authentification unique Notes/Windows est utilisée (si clients Windows XP ou Windows 2000)	
Mot de passe provisoire certificat, organisation	

Installation du logiciel

A l'issue de cette étape, le logiciel est chargé sur le serveur.

Etape	Objet	OK
1	Ouvrir le fichier readme.pdf disponible sur le CD-ROM Domino	
2	Déterminer les lecteurs sur lesquels seront installés le logiciel Domino (x :) et les bases (y :). Sur Windows 2000 et 2003, ce sont toujours des lecteurs séparés, les données étant en RAID5. Sur AS/400, ce sont des bibliothèques séparées	
3	Vérifier le niveau de l'OS en consultant le chapitre Platforms and requirements & general certifications and requirements du Readme	
4	Désinstaller Domino comme service Windows si le serveur héberge déjà une version de Domino	
5	Désinstaller une installation précédente de Domino sur le serveur – si les données ne doivent pas être conservées – en utilisant la procédure de désinstallation de l'OS et en vérifiant que x:\Lotus\Domino\ et y:\Lotus\Domino\Data sont bien supprimés	
6	Déterminer le type de logiciel Domino devant être installé : – Domino Mail Server, – Domino Utility Server, – Domino Enterprise Server.	
7	Charger le logiciel Domino à partir du CD-ROM dans x:\Lotus\Domino\ et dans y:\Lotus\Domino\Data. LODRUN sous AS/400 ou utiliser Operation Navigator	
8	Installer les mises à jour incrémentales et/ou les Fixpacks s'il y a lieu	
9	Installer le language pack french	

Configuration du serveur

Cette opération s'effectue au premier lancement du serveur et doit être conduite avec soin. En cas d'erreur, il vaut mieux reconfigurer le serveur avant d'aller plus avant.

Etape	Description	OK
1	Lancer la configuration du serveur	
2	Sélectionner SMTP	
3	Sélectionner DECS pour les connexions aux bases relationnelles	
4	Sélectionner les protocoles Internet voulus	
5	Vérifier noms : domaine, organisation, serveur, mot de passe	
6	Vérifier que le serveur est installé comme service Window	

7	Lancer le serveur Domino. STRDOMSVR sur AS/400	
8	Taper la commande LOAD UPDALL à la console du serveur	
9	Vérifier par telnet que le routeur (ou le pare-feu) accepte les sessions sur le port 25 à destination d'un domaine Internet externe	
10	Déplacer le fichier cert.id dans un répertoire protégé et prendre une copie de server.id dans le répertoire protégé	

Configuration de la station d'administration

A l'issue de cette étape, la station d'administration Windows est opérationnelle. Dérouler les étapes qui suivent :

Etape	Description	OK
1	Charger le logiciel client sur la station d'administration Windows, a priori distincte du serveur. Voir authentification unique Notes/NT	
2	Lancer la configuration du CLIENT, utilisateur « super administrateur »	

Standardisation de l'administration

Les groupes listés ici sont le minimum. La check-list sera complétée en fonction du contexte.

Dérouler les étapes qui suivent sur la station d'administration :

Etape	Description	OK
1	Créer le groupe des intrus du domaine : <i>_domaine_Intrus</i> (vide)	
2	Créer les groupes d'administration du serveur, par exemple : <i>_serveur_Acces</i> : Accès au serveur autorisé à */Org <i>_serveur_Intrus</i> : Accès au serveur interdit à _domaine_Intrus <i>_serveur_Admins</i> : Administrateurs du serveur _Les-Administrateurs <i>_serveur_AgNRest</i> : Exécuter des méthodes et des opérations non restrictives super Administrateur/Org <i>_serveur_AgPer</i> : Exécuter les agents simples et de formules */Org Lotus Notes Template Development/Lotus Notes <i>_serveur_AgRest</i> : Exécution agents LotusScript/Java restrictifs */Org Lotus Notes Template Development/Lotus Notes <i>_serveur_CreBase</i> : Création de bases autorisée à _Les Administrateurs LocalDomainServers	

	<i>_serveur_CreRepl</i> : Création de répliques autorisée à Les Administrateurs LocalDomainServers	
3	Modifier le document du serveur pour ajouter les noms de groupes et ajouter « super administrateur » dans le champ Administrateurs avec accès total	
4	Indiquer l'adresse IP du routeur ou du firewall dans les paramètres de messagerie (hôte relais pour les messages sortant du domaine Internet local) si le fournisseur d'accès offre ce service	
5	Créer le document Domaine Global – GlobalDomain – s'il n'existe pas et vérifier ou renseigner l'adresse Internet dans l'onglet (Conversion) et <i>Domaine Internet principal et local</i>	
6	Activer la recherche d'adresse Internet et préciser le format de conversion	
7	Contrôle des destinations en entrée : dans les paramètres de messagerie/Restrictions et contrôles/Contrôle SMTP en entrée indiquer le domaine Internet local dans <i>Messages provenant des domaines Internet externes autorisés uniquement vers ces domaines Internet</i>	
8	Dans les paramètres de messagerie, passer <i>Nombre de boîtes aux lettres</i> à 2	
9	Redémarrer le serveur Domino (service Windows, sous-système AS/400 Domsvr)	
10	Tester par telnet la connexion sur le port 25 du serveur Domino et envoyer un message à l'administrateur. Vérifier que le message est bien distribué	
11	Tester par telnet la connexion sur le port 25 du serveur Domino et envoyer un message à quiconque@autredomaine.com : le message doit être rejeté parce que le serveur Domino ne peut pas être relais.	
12	Depuis la station d'administration, envoyer un message à une adresse existante sur Internet et vérifier que le message est bien distribué.	
13	Créer un dossier <i>ID</i> sur le serveur de fichiers, avec trois sous-dossiers : <i>Certificats</i> , <i>Serveurs</i> et <i>Clients</i> . Le partager avec des droits d'accès réservés uniquement aux administrateurs.	
14	Déplacer le <i>cert.id</i> du dossier <i>y:\Lotus\Domino\Data</i> dans le sous-dossier <i>Certificats</i> . Le renommer en <i>Cert_Org.id</i> où <i>Org</i> est le nom de l'organisation.	
15	Copier le <i>server.id</i> du dossier <i>y:\Lotus\Domino\Data</i> dans le sous-dossier <i>Serveurs</i> . Le renommer en <i>serveur.id</i> où <i>serveur</i> est le nom du serveur	
16	Copier le <i>user.id</i> du répertoire <i>x:\Lotus\Notes\Data</i> de la station d'administration dans le sous-dossier <i>Clients</i> et le renommer <i>admin.id</i>	

17	Mapper le dossier ID sur serveur de fichiers à un lecteur réseau	
18	Mapper le dossier des bases Domino sur serveur à un lecteur réseau	
19	Standardiser les LCA des bases, selon le standard suivant applicable sauf exception signalée. <u>_Administrateur</u> (Personne) : Gestionnaire, <u>_Les_Administrateurs</u> (Groupe de personnes) : Editeur, Suppression de documents <i>LocalDomainServers</i> (Groupe de serveurs) : Editeur, <i>OtherDomainServers</i> (Groupe de serveurs) : Pas d'accès, <i>Defaut</i> : Pas d'accès, Serveur d'administration : le premier serveur	
	MAIL1.BOX et MAIL2.BOX	Défaut Déposant
	NAMES.NSF	Défaut Lecteur. <i>LesAdministrateurs</i> ont tous les rôles dont [UserCreator]
	ADMIN4.NSF	Défaut Auteur
	DDM.NSF	
	EVENTS4.NSF	
	LOG.NSF	
	REPORTS.NSF	
	STATMAIL.NSF	Défaut Déposant
	STATREP.NSF	
	WEBADMIN.NSF	Si HTTP a été sélectionné
	DECSADM.NSF	Si DECS est installé
20	Supprimer MAIL.BOX si MAIL1.BOX et MAIL2.BOX présentes	
21	Taper LOAD CATALOG à la console du serveur	
22	Régler la LCA de CATALOG.NSF	

Préparation de l'enregistrement des clients Notes

Dérouler les étapes qui suivent :

Etape	Description	OK
1	Vérifier l'existence ou créer la base CERTLOG.NSF (Certification Log) et standardiser sa LCA	
2	Attribuer des mots de passe multiples au fichier CERT.ID pour que chaque personne qui doit enregistrer des utilisateurs et les administrer	

	puisse y accéder avec son mot de passe. Attribuer des mots de passe multiples pour le fichier ID du super administrateur (admin.id) dans le dossier partagé	
3	Modifier le certificateur pour que les fichiers ID créés soient envoyés à une base de sauvegarde – mail\SauveID.NSF (_Sauvegarde des fichiers ID) – et que l'autorité de restauration soit le super administrateur	
4	Prendre une copie de sauvegarde du CERT.ID et de ADMIN.ID sur disquette et la mettre dans une enveloppe avec les mots de passe puis déposer l'enveloppe au coffre	
5	Modifier la LCA de la base mail\SauveID.NSF (_Sauvegarde des fichiers ID) afin que _Les_Administrateurs aient un accès <i>Editeur</i>	
6	Créer une politique subordonnée à l'organisation	
7	Créer un document de paramètres d'enregistrement : – mots de passe – quotas des bases – nom du serveur de messagerie – nom du serveur d'enregistrement – Format MIME pour les messages envoyés à des adresses Internet introuvables lors de l'envoi	
8	Créer un document de paramètres de bureau pour préciser que le mot de passe doit avoir une longueur minimum	
9	Créer un document de paramètres de sécurité Modifier la LCE d'administration et créer une entrée avec la signature de super administrateur qui doit avoir tous les droits. Laisser à l'utilisateur le droit de modifier sa propre LCE pour le moment	
10	Rattacher les paramètres à la politique	

Création du premier compte d'administrateur

L'administrateur est supposé utiliser la station qui a été configurée pour le super administrateur. S'il dispose d'une station personnelle séparée, charger le logiciel et configurer le poste puis aller à l'étape 9.

Dérouler les étapes qui suivent :

Etape	Description	OK
1	Créer un compte client Notes pour le premier administrateur Le fichier ID doit être sur le dossier réseau <i>ID\Clients\</i> Ajouter ce compte dans le groupe <i>_Les_Administrateurs</i> Définir le mot de passe Internet	
2	Copier le fichier ID sur la station d'administration. Il sera nommé <i>pnom.id</i> dans ce qui suit	

3	Copier-coller le document site <i>Bureau</i> , puis renommer le premier en <i>Admin</i>	
4	Dans le document site <i>Admin</i> , dans l'onglet (Avancé), dans ID utilisateur à employer, indiquer le fichier ID du super administrateur, par exemple <i>sadmin.id</i> dans le dossier réseau <i>ID\Clients</i>	
5	Dans le document site <i>Bureau</i> , dans l'onglet (Avancé), dans ID utilisateur à employer, indiquer le fichier ID <i>pnom.id</i> dans le dossier local. Modifier les informations de l'onglet (Général) et de l'onglet (Messagerie) pour qu'elles correspondent à l'utilisateur	
6	Vérifier en changeant de site – de <i>Bureau</i> à <i>Admin</i> et inversement – que le mot de passe demandé correspond bien à l'ID attendu et que la base courrier ouverte est bien celle de l'utilisateur en cours	
7	Modifier la LCE du poste pour l'utilisateur correspondant à <i>pnom.id</i> pour la mettre en conformité avec la LCE administrative	
8	Vérifier que le nouvel administrateur peut afficher les tâches en cours sur le serveur et voir le contenu des MAILn.BOX (comme Gestionnaire)	
9	Modifier les préférences d'administration pour _Administrateur Serveur d'enregistrement ID certificateur Paramètres de fichier ID : utiliser le dossier réseau <i>ID\</i> Domaine Internet Profil de configuration utilisateur : laisser vide	
10	Modifier les préférences d'administration pour le compte d'administrateur à l'identique	

Tâches de maintenance

Ce sont les tâches minimum à installer sur le serveur. Dérouler les étapes qui suivent :

Etape	Description	OK
1	Créer un document papier qui listera toutes les tâches planifiées du serveur avec l'heure d'exécution	
2	Noter les tâches dont le déclenchement vient du fichier NOTES.INI (Lignes avec <i>ServerTasksAtx=</i>) Design : 1h du matin Catalog : 1h du matin Updall : 2h du matin Statlog : 5h du matin	
3	Noter les tâches dont le déclenchement vient du document du serveur ou du document de configuration du serveur : Requêtes journalières admin process : minuit Requêtes différées admin process : minuit (le dimanche) Mise à jour du cache agent : minuit	

4	Si le serveur ne tourne pas à 4h du matin, créer une ligne MAILCOMPACTHOUR dans le fichier NOTES.INI du serveur. Noter l'heure de compactage des mail.box : 4h ou la nouvelle heure.	
5	Créer un document programme pour compacter les bases courrier : onglet (Configuration), puis Serveur/programme <Nom de programme> : COMPACT Ligne de commande : mail\ -S 10 -B Exécution : 4h30 tous les jours	
6	Créer un autre document programme : <Nom de programme> : COMPACT Ligne de commande : names.nsf -S 10 -b Exécution : 6h00 le dimanche	
7	Créer un autre document programme : <Nom de programme> : COMPACT Ligne de commande : log.nsf -S 10 -B Exécution : 6h45 le dimanche	
8	Créer un autre document programme : <Nom de programme> : COMPACT Ligne de commande : admin4.nsf -S 10 -b Exécution : 7h00 le dimanche	
9	Positionner les sauvegardes des bases dans le planning des tâches serveur	
10	Vérifier dans le journal du serveur la bonne exécution des tâches	

Le tableau sera complété et ajusté à l'usage. Le journal du serveur donne les informations de début et de fin de tâche.

Etape	Description	OK
11	Créer une <i>event notification</i> sur la statistique Mail.Dead : onglet (Configuration), puis Statistiques & événements/Monitors/Statistic. Envoyer une alerte par courrier à <i>_Les_Administrateurs</i> si mail.dead > 0	
12	Créer une <i>event notification</i> sur la statistique Mail.Waiting : envoyer une alerte par courrier à <i>_Les_Administrateurs</i> si mail.waiting > 0	
13	Vérifier que la tâche COLLECT tourne sur le serveur	
14	Vérifier la période de collecte des statistiques dans l'onglet (Configuration), puis Statistiques & événements/Server Statistic Collector : une périodicité de 360 minutes est suffisante pour les statistiques, de 15 minutes pour les alarmes	

Check-list d'installation d'un serveur additionnel

Ce document liste toutes les étapes de l'installation et de la configuration d'un serveur additionnel. A l'issue de ces étapes :

- Le serveur additionnel est prêt à fonctionner,
- L'administration est conforme aux standards du domaine,
- La réplication minimum est en place,
- Le routage du courrier dans le domaine est opérationnel.

Plan de nommage

A l'issue de cette phase, les règles de nommage des serveurs et les règles de gestion sont connues.

Etape	Description	OK
1	Création d'unités d'organisation propres aux serveurs s'il y a lieu : séparation de la gestion des serveurs et des utilisateurs	
2	Détermination du serveur d'enregistrement du nouveau serveur : serveur devant fournir l'annuaire du domaine à la configuration	
2	Nom Notes du serveur Domino	
3	Adresse IP du serveur Domino	
4	Adresse réseau du serveur Domino (serveur.domaine.com)	
5	Services Internet devant tourner sur le serveur : SMTP, HTTP, IMAP, POP3, LDAP, IIOF, SSL	
6	Est-ce que des connexions à des bases relationnelles sont nécessaires ? Si oui, installer DECS, ou LEI (vendu séparément)	
7	Quel est le logiciel (middleware) de connexion à la base relationnelle ? Exemple : Client access DB2	
8	Serveur partitionné (par exemple AS/400)	
9	Serveur faisant partie d'une grappe	

Enregistrement du serveur avec le certificat

A l'issue de cette étape, le document serveur est créé dans l'annuaire, le fichier ID est disponible et les groupes de sécurité sont prêts.

Etape	Description	OK
1	Créer les groupes d'administration du serveur, par exemple : _serveur_Acces : Accès au serveur autorisé à */Org _serveur_Intrus : Accès au serveur interdit à _domaine_Intrus _serveur_Admins : Administrateurs du serveur Les-Administrateurs _serveur_AgNRest : Exécuter des méthodes et des opérations non restrictives super Administrateur/Org	

Etape	Description	OK
	<p><i>_serveur_AgPer</i> : Exécuter les agents simples et de formules */Org Lotus Notes Template Development/Lotus Notes</p> <p><i>_serveur_AgRest</i> : Exécution agents LotusScript/Java restrictifs */Org Lotus Notes Template Development/Lotus Notes</p> <p><i>_serveur_CreBase</i> : Création de bases autorisée à _Les_Administrateurs LocalDomainServers</p> <p><i>_serveur_CreRepl</i> : Création de répliques autorisée à _Les_Administrateurs LocalDomainServers</p>	
2	<p>Enregistrer le serveur avec le certificat d'organisation ou d'unité d'organisation selon le cas</p> <ul style="list-style-type: none"> – le fichier ID du serveur est créé sur serveur de fichier, dans un dossier réservé aux fichiers ID de serveur, – le fichier ID n'est pas enregistré dans l'annuaire Domino du domaine, – le fichier n'a pas de mot de passe, – les administrateurs du serveur sont <i>_serveur_Admins</i> 	
3	Modifier le document du serveur pour ajouter les noms de groupes	
4	Ajouter le super administrateur pour l'accès complet	
5	Créer un document de configuration pour ce serveur	
6	Si le serveur est connecté vers l'Internet pour la messagerie, indiquer l'adresse IP du routeur ou du firewall dans les paramètres de messagerie (hôte relais pour les messages sortant du domaine Internet local) si le fournisseur d'accès offre le service de relais SMTP	
7	Contrôle des destinations en entrée : dans les paramètres de messagerie/Restrictions et contrôles/Contrôle SMTP en entrée, indiquer le domaine Internet local dans <i>Messages provenant des domaines Internet externes autorisés uniquement vers ces domaines Internet</i>	
8	Dans les paramètres de messagerie, passer <i>Nombre de boîtes aux lettres</i> à 2 si le serveur abrite des bases de messagerie	
9	Répliquer l'annuaire vers le serveur qui fournira l'annuaire du domaine au serveur additionnel	

Installation du logiciel

A l'issue de cette étape, le logiciel Domino est chargé sur le serveur.

Etape	Objet	OK
1	Ouvrir le fichier readme.pdf disponible sur le CD-ROM Domino	
2	Déterminer les lecteurs sur lesquels seront installés le logiciel Domino (x :) et les bases (y:). Sur NT et Windows 2000, ce sont habituellement des lecteurs séparés. Sur AS/400, ceci n'est pas applicable.	
3	Vérifier le niveau de l'OS en consultant le Chapitre 2 (Platforms and	

Etape	Objet	OK
	requirements & general certifications and requirements) du Readme.	
4	Désinstaller Domino comme service NT si le serveur héberge déjà une version de Domino 4.x qui ne doit pas être conservée : C:\Notes\ntsvinst -d	
5	Désinstaller une installation précédente de Domino sur le serveur – si les données ne doivent pas être conservées – en utilisant la procédure de désinstallation de l’OS et en vérifiant que x:\Lotus\Domino\ et y:\Lotus\Domino\Data sont bien supprimés.	
6	Déterminer le type de logiciel Domino devant être installé : – Domino Mail Server, – Domino Utility Server, – Domino Enterprise Server.	
7	Charger le logiciel Domino à partir du CD-ROM dans x:\Lotus\Domino\ et dans y:\Lotus\Domino\Data. LODRUN sous AS/400.	

Configuration du serveur additionnel

Cette opération s’effectue au premier lancement du serveur et doit être conduite avec soin. En cas d’erreur, il vaut mieux reconfigurer le serveur avant d’aller plus avant.

Etape	Description	OK
1	Lancer la configuration du serveur	
2	Sélectionner les services Internet devant tourner sur le serveur	
3	Sélectionner DECS pour les connexions aux bases relationnelles	
4	Le fichier ID est accessible depuis le serveur, le serveur fournissant l’annuaire du domaine est actif	
5	Vérifier que le serveur est installé comme service NT	
6	Lancer le serveur Domino. STRDOMSVR sur AS/400	
7	Si SMTP tourne sur le serveur, vérifier par telnet que le routeur (ou le firewall) accepte les sessions sur le port 25 à destination d’un domaine Internet externe	
8	Tester par telnet la connexion sur le port 25 du serveur Domino et envoyer un message à quiconque@autredomaine.com : le message doit être rejeté parce que le serveur Domino ne peut pas être relais	
9	Vérifier l’accès complet au serveur avec l’identifiant de super administrateur	

Réplication minimum et routage de courrier

A l'issue de cette étape, la réplication minimum fonctionne pour administrer le domaine et le routage de courrier fonctionne. Dérouler les étapes qui suivent :

Etape	Description	OK
1	Créer sur le pivot un document de réplication avec le serveur additionnel pour répliquer names.nsf , admin4.nsf et events4.nsf ou ajouter le serveur additionnel dans le groupe de serveurs compris dans un document de réplication existant	
2	Créer un document de connexion de routage de courrier du serveur additionnel vers le pivot si le serveur additionnel est seul dans le réseau nommé Domino	
3	Créer un document de connexion de routage de courrier symétrique du pivot vers le serveur additionnel	

Check-list de mise en production d'une base

Ce document liste les étapes de réception et de mise en exploitation d'une base Notes accédée depuis des clients Notes et/ou des navigateurs. A l'issue de ces étapes :

- La base Notes est installée sur les serveurs et opérationnelle,
- Les répliques sur postes clients mobiles sont installées.

Sécurité d'accès

Les consignes de mise en exploitation doivent contenir les éléments de réponse aux postes du tableau. A l'issue de cette phase, les consignes de réglage de la LCA et de distribution des clés de chiffrement sont connues.

Etape	Description	OK
1	LCA. Droit d'accès par défaut de la base	
2	LCA. Droit d'accès Lecteur. Quel(s) groupe(s) d'utilisateurs ?	
3	LCA. Droit d'accès des utilisateurs devant créer des documents (normalement Auteur). Quel(s) groupe(s) d'utilisateurs ?	
4	LCA. Droit d'accès Editeur : quel groupe d'utilisateurs ?	
5	LCA. Droit d'accès de <i>Anonymous</i> ?	
6	LCA. Droit d'accès maximum des navigateurs ?	
7	LCA. Rôles : tableau des rôles et affectation à des groupes d'utilisateurs.	
8	LCA. Est-ce que l'application doit répliquer sur des postes mobiles ? Est-ce qu'une LCA cohérente est requise ?	
9	Sécurité. Champs Lecteurs. Est-ce que les champs Lecteurs sont utilisés dans les documents de la base ?	
10	Sécurité. Champs Lecteurs. Comment les serveurs voient-ils les documents : rôle spécial ? Présence dans un groupe pré-défini ?	
11	Sécurité. Champs Lecteurs. Comment est-il prévu de dépanner un utilisateur qui ne voit plus un document ?	
12	Sécurité. Chiffrement. Est-ce que le chiffrement par clé simple est utilisé ? Quel est le nom de la clé ?	
13	Sécurité. Chiffrement. Quel est l'utilisateur – a priori, ce n'est pas le concepteur – détenteur de la clé de chiffrement ?	
14	Sécurité. Chiffrement. Un fichier ID dont le mot de passe est inscrit contient la clé de chiffrement et se trouve au coffre	

Réglage des agents

A l'issue de cette phase, l'utilisation de l'ID administratif de signature des bases est validée, les réglages des documents serveurs et de configuration serveurs vérifiés.

Etape	Description	OK
1	Agents. Type Exécuter des méthodes et des opérations non restrictives ?	
2	Agents. Type LotusScript/Java restrictifs ?	
3	Agents. Activés par utilisateur Web ?	
4	Agents. Activés par utilisateur Editeur ?	
5	Agents. Est-ce qu'une signature administrative unique est suffisante pour satisfaire à la sécurité d'exploitation ?	
6	Agents. Gestionnaire d'agents. Quels sont les paramètres de délais d'exécution requis ? Paramètres NOTES.INI du serveur AMGR_DOCUPDATEEVENTDELAY AMGR_NEWMAILAGENTMININTERVAL AMGR_NEWMAILEVENTDELAY AMGR_DOCUPDATEAGENTMININTERVAL	
7	Agents. Est-ce qu'il y a des agents locaux tournant sur les postes clients ?	
8	Agents. Gestionnaire d'agents. Est-ce que les serveurs satisfont aux réglages des agents ?	
9	Quels sont les droits applicables aux agents lancés depuis un navigateur : droit de l'utilisateur ou droit du signataire de l'agent ?	
10	En fonction du nombre de navigateurs connectés, combien faut-il prévoir d'agents Web simultanés ? Faut-il prévoir une analyse de charge ?	

Adressage par routeur de messagerie

Dans une application de workflow, une base peut recevoir des documents acheminés par le routeur de messagerie. Si ce n'est pas le cas, cette étape peut être omise. A la fin de cette étape, les réglages pour que la base soit connue du routeur de messagerie et les agents courriers opérationnels sont connus.

Etape	Description	OK
1	Quel est le nom de destinataire de la base dans l'application ?	
2	Si le nom n'est pas conforme au standard, peut-il être paramétré ?	
3	Création d'un document Base Courrier en arrivée	
4	Agents. Est-ce qu'il y a des agents de type Prédistribution ? Si oui : – Vérifier que les paramètres de messagerie du serveur/Contrôles de distribution/Agents de prédistribution sont bien <i>Activés</i> – Vérifier que le paramètre du NOTES.INI AMGR_DISABLEMAILLOOKUP permet aux agents de fonctionner après signature	

Réplication sur serveurs et clients

A l'issue de cette étape, les consignes de mise en œuvre de la réplication de serveur à serveur et de client à serveur sont connues.

Etape	Description	OK
1	La base doit-elle répliquer sur plusieurs serveurs ?	
2	Quel est le serveur d'administration de la base ? A priori, ce devrait être un serveur pivot	
3	Quels sont les droits d'accès des serveurs satellites ? A priori, ce devrait être Editeur pour tous	
4	Quelle est la fréquence de réplication minimum pour que la propagation des modifications se fasse avec un délai acceptable ?	
5	Faut-il modifier les paramètres de réplication entre serveurs (non recommandé) : – réplication partielle d'un ensemble de documents – formule de réplication	
6	La base doit-elle répliquer sur des postes clients mobiles ?	
7	La LCA est-elle cohérente ?	
8	Quels sont les paramètres de réplication à modifier sur les postes clients : – réplication partielle d'un ensemble de documents – formule de réplication	
9	Comment installer la réplique de la base sur le poste client ? – Paramètres de bureau – Politiques existantes adaptées	
10	La quantité d'information transitant par réplication serveur-client est-elle compatible avec les capacités des postes ?	
11	Faut-il prévoir le chiffrement des données sur le port TCP/IP des postes clients mobiles ?	

Installation sur serveur et performances

A l'issue de cette étape, les réglages à effectuer dans les propriétés de chaque réplique de la base sur serveur sont connus.

Etape	Description	OK
1	Dossier d'installation de la base	
2	Utilisation d'un lien base (base en dehors de \Domino\Data\)	
3	Utilisation d'un lien vers un répertoire en dehors de \Domino\Data\	
4	Marqueurs de non lus utilisés dans l'application ? Si non, cocher : <i>Ne pas gérer les marqueurs de non lus</i> (Propriétés de la base)	
5	Toujours cocher : Optimiser les images.bmp dans les tableaux (Propriétés de la base)	
6	Données confidentielles ? Si non, cocher :	

Etape	Description	OK
	<i>Ne pas écraser l'espace disponible</i> (Propriétés de la base)	
7	Pas de suivi des accès aux documents, pas d'archivage Notes ? Si oui NE PAS cocher : <i>Gérer la propriété LastAccessed</i> (Propriétés de la base)	
8	Base avec peu de transactions de modifications ? Si oui, cocher : <i>Désactiver la journalisation des transactions</i> (Propriétés de la base)	
9	Le concepteur a prévu de gérer la récupération des documents de la corbeille ? Si oui, cocher <i>Autoriser la récupération des suppressions</i> (Propriétés de la base)	
10	Le concepteur n'a pas prévu de gérer des hiérarchies de documents ? Si oui, cocher : <i>Ne pas gérer les hiérarchies de réponses spécialisées</i> (Propriétés de la base)	
11	La base n'est pas candidate à des abonnements de la part des utilisateurs (pour être averti des nouveautés). Si oui, cocher : <i>Ne pas autoriser les contrôles des titres</i> (Propriétés de la base)	
12	Le concepteur le demande explicitement. Cocher : <i>Autoriser davantage de champs dans la base</i> (Propriétés de la base)	
13	Cocher Utiliser la compression LZ1 pour les rattachements	
14	La base réplique sur peu de serveurs en pivot/satellite (moins de cinq serveurs) : Limiter nombre d'entrées dans champ \$UpdatedBy à 5 Limiter nombre d'entrées dans champ \$Revisions à 5	
15	Le concepteur a prévu de gérer la récupération des documents de la corbeille ? Si oui, renseigner : <i>Délai d'expiration \$Undelete (en heures)</i> (Propriétés de la base)	
16	Cocher <i>Autoriser le verrouillage de documents</i> si ceci est prévu par le concepteur	
17	La base est-elle multilingue ? Comment l'utilisateur définit-il sa langue préférée ?	

Journalisation des transactions

Si la base évolue peu, la journalisation des transactions a été désactivée et cette étape peut être sautée. A l'issue de cette étape, le paramétrage de la journalisation des transactions est vérifié pour cette base.

Etape	Description	OK
1	Planifier la tâche COMPACT dans un document programme, ou pendant l'arrêt du serveur, avec le paramètre -b (pour conserver le DEBID). Exemple : LOAD COMPACT Dossier\ -S 20 -b	
2	La journalisation des transactions est activée sur le serveur	
3	La journalisation des transactions est activée pour la base	
4	L'utilitaire de sauvegarde fonctionne	

Etape	Description	OK
5	La restauration complète d'une base suivie d'une reconstitution à partir des transactions est testée et fonctionne	
6	La restauration d'un document perdu fonctionne	

Abonnement et indexation

A l'issue de cette phase, les paramètres d'indexation et d'abonnement des utilisateurs aux nouveautés sont vérifiés.

Etape	Description	OK
1	La base fait-elle partie de l'index de domaine ? Si oui : – le serveur est-il inclus dans la liste prise en charge par l'indexeur de domaine, – la propriété <i>Inclure dans l'indexation multibase</i> est cochée	
2	La base doit-elle être indexée localement ? Si oui : – elle ne fait pas partie normalement de l'index de domaine – est-ce que les pièces attachées doivent être indexées ? – est-ce que l'index est construit sur des mots ou des phrases ?	
3	Est-ce que les utilisateurs peuvent s'abonner à la base ? Si oui, – la propriété <i>Ne pas autoriser le contrôle de titres</i> est désactivée – le document du serveur Paramètres de sécurité autorise l'utilisation des contrôles ? – les préférences utilisateur des postes clients indiquent <i>Vérifier les abonnements</i>	

Création d'une base

La base à mettre en exploitation est normalement livrée sous forme d'un modèle (fichier d'extension .NTF) qui ne comprend que la structure de la base (la partie programmation). Les consignes déroulées précédemment sont mises en œuvre. A l'issue de cette étape, la base est prête à fonctionner sur les serveurs. Une base contenant des documents et récupérée de l'extérieur peut suivre le même chemin, la création de la base étant remplacée par une copie de la base.

Etape	Description	OK
1	Installer le modèle sur le poste local d'administration	
2	Signer le modèle avec un ID administratif de signature (ID de serveur ou ID de super administrateur)	
3	Créer la base sur le serveur pivot qui sera aussi serveur d'administration de la base	
4	Créer une copie de la base sur le serveur si ce n'est pas un modèle qui a été fourni	
5	Régler la LCA de la base	
6	Régler les propriétés de la base	
7	Régler les paramètres de réplication	

Etape	Description	OK
8	Créer des répliques sur les serveurs satellites	
9	Créer ou modifier les documents de réplication planifiée	
10	Régler les propriétés de la base sur chaque serveur satellite	
11	Régler les paramètres de réplication sur chaque serveur satellite	
12	Publier la base en créant un lien base dans les paramètres de bureau	
13	Indexer la base si nécessaire sur chaque serveur	
14	Vérifier les messages envoyés par Agent manager afin de détecter les anomalies	
15	Créer une réplique de la base sur les portables en modifiant les paramètres de bureau voulus	

Mise à niveau d'une base

La mise à niveau d'une base se fait en transmettant un nouveau modèle à l'administrateur. Des consignes de migration des documents existants peuvent accompagner une mise à niveau. A l'issue de cette étape, l'application a été mise à jour sur les serveurs.

Etape	Description	OK
1	Installer le modèle sur le poste local d'administration	
2	Signer le modèle avec un ID administratif de signature (ID de serveur ou ID de super administrateur)	
3	Donner un nom au modèle (<i>xyzNouvelleVersion</i>) : – dans l'onglet de structure des propriétés de la base modèle	
4	Modifier le nom du modèle (<i>xyzNouvelleVersion</i>) dans la base en exploitation sur le serveur pivot qui est aussi serveur d'administration de la base : – dans l'onglet structure des propriétés de la base en exploitation	
5	Désactiver la réplication de la base en exploitation	
6	Prendre une sauvegarde de la base en exploitation	
7	Modifier la structure de la base en exploitation sur le serveur pivot qui est aussi serveur d'administration de la base : – par mise à jour de la structure depuis le modèle en <i>Local</i>	
8	Appliquer les outils de migration de documents de la base	
9	Vérifier le fonctionnement de la base	
10	Activer à nouveau la réplication de la base en exploitation : les modifications de structure sont répercutées par réplication	

