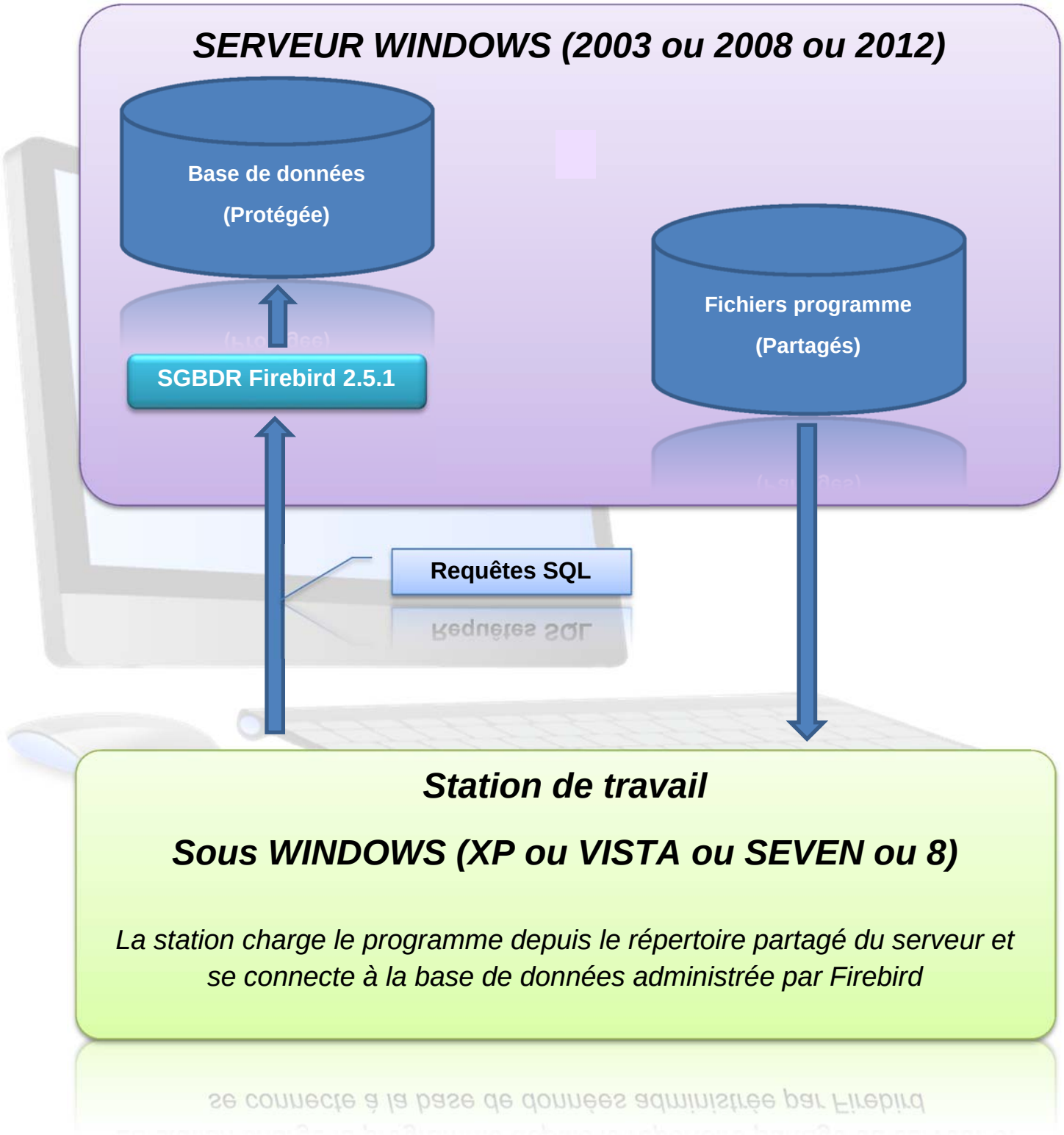
Configuration technique…

Schéma d'une installation en réseau local



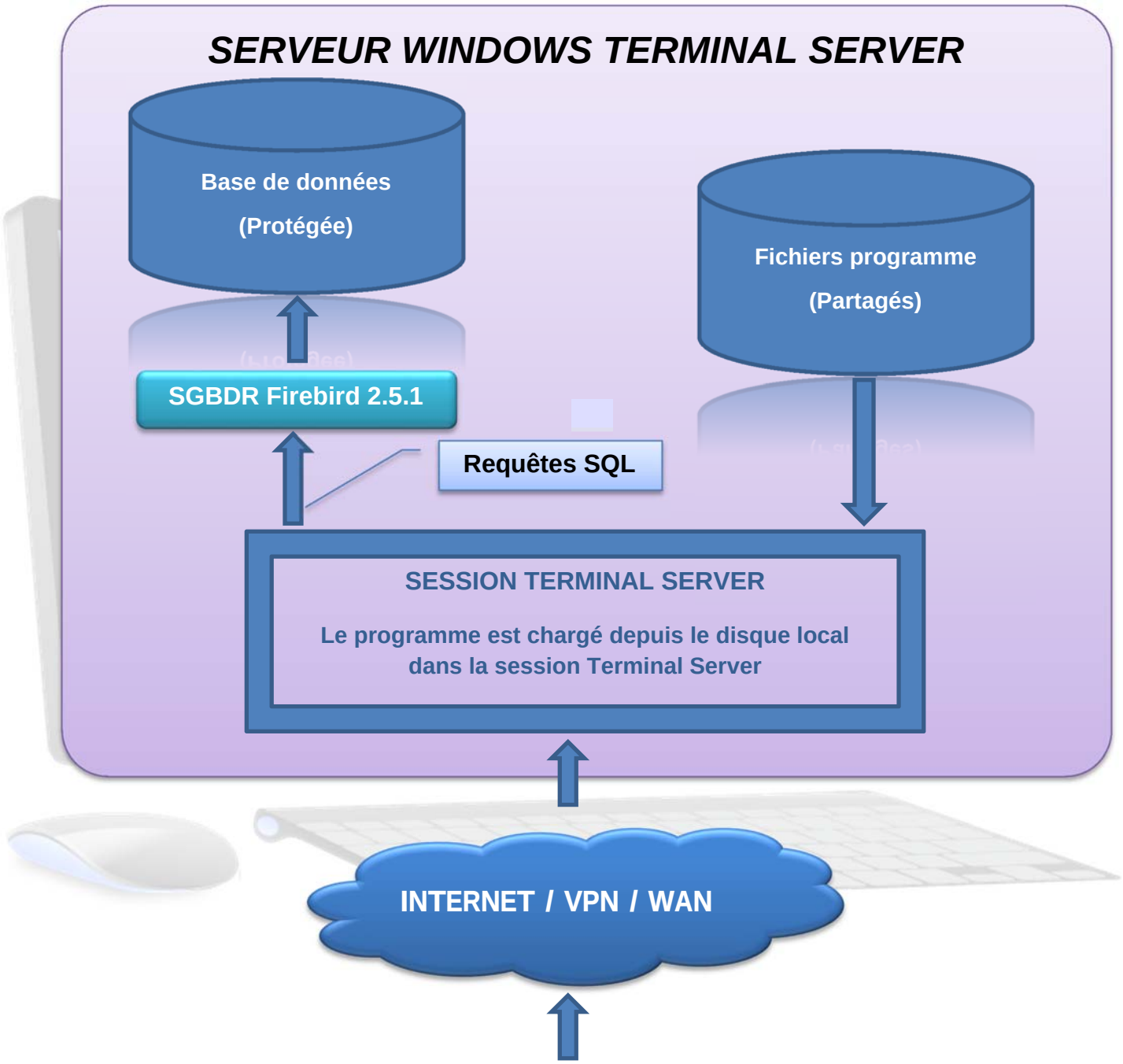
Station de travail

Sous WINDOWS (XP ou VISTA ou SEVEN ou 8)

La station charge le programme depuis le répertoire partagé du serveur et se connecte à la base de données administrée par Firebird

Configuration technique (2)…

Schéma d'une installation en accès distant via Terminal Server



Station de travail Cliente

La station se connecte à Terminal Server par le biais d'une connexion réseau distante

Pré requis pour l'installation…

Configuration minimale monoposte

- Système d'exploitation Windows 2000, XP Pro, Vista Pro, 7 ou 8 Pro
- Processeur 1 GHz - 1 Go de RAM - 1 Go d'espace disque disponible pour l'installation
- Carte graphique avec résolution minimum de 1 024x768 Lecteur Cd-Rom ou DVD
- Microsoft Word pour les fusions publipostage, Excel pour les imports de données et exports des éditions
- Microsoft Activsync. 4.5 avec XP ou Mobile 6 sous Vista et Windows 7 pour la synchro filaire Pocket PC

Pour une installation réseau local

- Réseau Ethernet 100 Mbps ou +
- Plateforme Windows de préférence. Fonctionne sous Linux, Mac et client léger Citrix
- Ne nécessite pas de serveur dédié (Windows Serveur conseillé 2003-2008-2012)

Pour une installation avec postes distants *(VPN - Terminal Server - Bureau mobile)*

- Serveur dédié sous Windows Server 2003 2008 ou 2012, disposant d'un accès sur le réseau public avec une adresse IP fixe. Il convient de définir une règle de redirection du port 3051 vers l'adresse IP du serveur.
- Processeur 2 GHz - 2 Go de Ram - 1 Go d'espace disque disponible
- Postes clients sous Windows XP Pro, Vista Pro, 7 ou 8 Pro (TSE)

Pocket PC, Smartphone, Tablettes

- Windows Mobile 6 et 6.5 sur les Pocket PC
- Navigateur web sur tous Smartphones, Tablettes et PC Portable sous Androïd Windows mobile 7 & 8 *(Développement HTML5 indisponible sur Apple iPhone et iPad tant que le moteur de base de données interne aux navigateurs (indexedDB), n'est pas supporté par iOS)*

Détails sur ce qui est installé sur le serveur

- La base de données est Firebird SQL 2.1 démarrée sous forme de service
- Le fichier de base de données Clair et Net (CN.FDB)
- Un service "Service_CNEvents" utilisé pour propager les événements du serveur vers les postes clients
- Les composants serveur Clair et Net sous la forme de DLL (objets DCOM) enregistrés dans le système
- Un processus permettant d'héberger les DLL (COM surrogate personnalisé)
- Les fichiers d'installation des postes clients des PocketPC et des Scanners

Détails sur ce qui est installé sur les postes clients

- Clair et Net client
- Une police pour les codes à barres
- Les drivers du scanner utilisé et l'utilitaire de transfert des pointages

Concernant les communications entre les différents composants

- Le client Clair et Net se connecte au serveur avec la technologie DCOM (port TCP/IP 135). Il existe toutefois un mode de secours dans le cas où DCOM n'est pas disponible : dans ce mode les DLL sont accédées par COM et doivent être partagées sur le réseau.
- Le client se connecte également au service "Service_CNEvents" avec TCP/IP sur le port 3049
- Les composants DCOM sur le serveur communiquent avec la base de données FirebirdSQL avec TCP/IP sur le port 3050
- Pour connaitre les performances en termes de com. nous donner le débit de la ligne SDSL prévue puisque ça peut aller de 512 kbits à 10 ou 20 Mbits.
- En fonction de ça et du nombre de postes on peut réfléchir à différentes options :
    - Soit installation des postes clients "standard" (nécessite une ligne assez rapide)
    - Soit installation en bureau à distance (SynchroWeb obligatoire pour Smartphone ou Tablette)

Procédures d'installation…

Procédure d'installation Serveur (Windows 2003, 2008, 2012…)

Vous devez avoir les droits administrateurs pour lancer cette installation :

- Lancer le fichier d'installation.
- Ajouter un utilisateur « cnuser » sur le domaine, mot de passe « 65)wDsr8yqsF »
- Créer un groupe « Utilisateurs ClairNet » contenant tous les utilisateurs devant utiliser Clair&Net.

Modifier l'objet DCOM CNServer comme suit :

- Menu Démarrer -> Exécuter -> dcomcnfg
- Services de composants -> ordinateurs -> Poste de travail -> configuration DCOM
- Faire un clic-droit sur l'objet CNServer -> Propriétés : onglet identité
- Saisir l'utilisateur « domaine/cnuser », mot de passe « 65)wDsr8yqsF »
- Appliquer et fermer

Ensuite dans la barre d'outils de dcomcnfg, cliquer sur le bouton « configurer le poste de travail » pour vérifier que les propriétés par défaut sont :

- DCOM activer sur cet ordinateur
- Internet COM « désactiver »
- Niveau d'authentification = Connecter
- Niveau d'emprunt d'identité = Identifier

Dans l'onglet « Sécurité COM » :

- Cliquer dans « Autorisations d'accès » sur le bouton « Modifier »
- Ajouter, dans la liste des utilisateurs, le groupe des utilisateurs de Clair&Net et leur donner les droits d'accès local et distant. Pas les 2 lignes habituelles offrant les 2 options indiquées sur ce serveur 2003
- Cliquer dans « Autorisation d'exécution et d'activation » sur le bouton « Modifier »
- Ajouter, dans la liste des utilisateurs, le groupe des utilisateurs de Clair&Net et leur donner les droits d'exécution et d'activation distante. Idem ci-dessus
- Faire de même en cliquant sur le bouton « Modifier les limites »
- Pour que les utilisateurs puissent installer le client, partager le répertoire d'installation
- Si besoin, il faut ouvrir « configurer le pare-feu » en mettant le port 135 comme accessible, ainsi que l'application « custdllhost.exe » située dans le répertoire « system32 » de Windows
- Indiquer quel est le pare feu sur ce serveur et créer l'exception

Installation des postes clients du domaine

Depuis le poste client :

- Aller sur le serveur dans le répertoire partagé et dans le répertoire Install Client et lancer le fichier «inst_client.exe»
- Vérifier dans le fichier « client.ini », dans le répertoire d'installation, que le domaine est bien celui du serveur
- Configuration du pare-feu : Pas de pare-feu géré par win2000

Ajouter dans les exceptions :

- Le port 135 en TCP : DCOM
- Créer l'exception sur le pare feu installé pour l'application cnclient.exe
- Il peut être nécessaire d'ajouter l'utilisateur cnuser dans les droits d'accès DCOM du poste client
- Pas d'accès DCOM sur Win 2000

Recommencer cette opération sur chaque poste client…

Cas particuliers pour les machines WORKGROUP.

Aucun changement sur les postes clients par rapport à la version domaine. Sur le serveur :

- L'utilisateur « cnuser » doit être créé en local
- Il faut créer tous les utilisateurs des postes clients qui utiliseront le logiciel (même nom, même mot de passe : le mot de passe doit être différent de vide et de « admin »)
- Les comptes doivent avoir les mêmes droits en tout cas sous Vista
- Donner les droits d'accès DCOM à tous les utilisateurs « locaux »
- Aller dans le panneau de configuration -> outils d'administration -> stratégie de sécurité locale -> stratégies locales –> options de sécurités et vérifier que l'accès réseau « modèle partage et de sécurité pour les comptes locaux » est bien sur la valeur : « Classique : les utilisateurs locaux s'authentifient eux-mêmes »

Autre solution pour les WORKGROUP.

- Choisir un poste en tant que serveur
- Effectuer une installation de type serveur sur chaque machine

Configurer les postes clients comme suit :

- Aller dans le répertoire d'installation de Clair&Net, le répertoire SERVEUR, et modifier le fichier «database.ini» : database_host=adresse_IP_du_serveur.
- Aller dans le répertoire de firebird (c:\program files\firebird\firebird1_5\ et modifier le fichier «aliases.conf» : SERVICE_DATABASE = adresse_IP_serveur:SERVICE_DATABASE
- Redémarrer le « service_cnevents ».

Cela a pour inconvénient les points suivants :

- Les mises à jour doivent être effectuées sur chaque poste
- Les modèles de documents des contrats commerciaux sont « local » à chaque poste

Autre solution pour les WORKGROUP à partir de la version 3.0.0.39 :

- Faire une installation serveur sur le poste désigné comme serveur
- Aller dans le répertoire d'installation de Clair&Net, le répertoire SERVEUR, et modifier le fichier database.ini » : database_host=adresse_IP_du_serveur.

Dans le pare-feu du serveur ajouter les exceptions des ports :

- 3050 TCP (Firebird)
- 3049 TCP (service_cnevents)
- Partager le répertoire d'installation de Clair & Net

Sur les postes client :

- Créer un lecteur réseau sur le répertoire partagé du réseau
- A partir de ce lecteur, aller dans le répertoire install_client et double cliquer sur le fichier inst_client_WrkGrp.

Pour les accès distants :

- Il suffit d'avoir une connexion VPN du poste client au serveur
- Enlever le pare-feu Windows

Installation Pocket Clair&Net : Pré requis - ActiveSync 4.0 ou supérieur

Si l'installation des différents composants (.NET CF, SQL Mobile, et CN) se fait une carte mémoire, il faut copier les DLL SQL Mobile dans le répertoire de ClairNet sur la carte.

Message d'erreur possible :

« EOleSysError : Accès refusé » : Le serveur refuse la connexion du poste client :

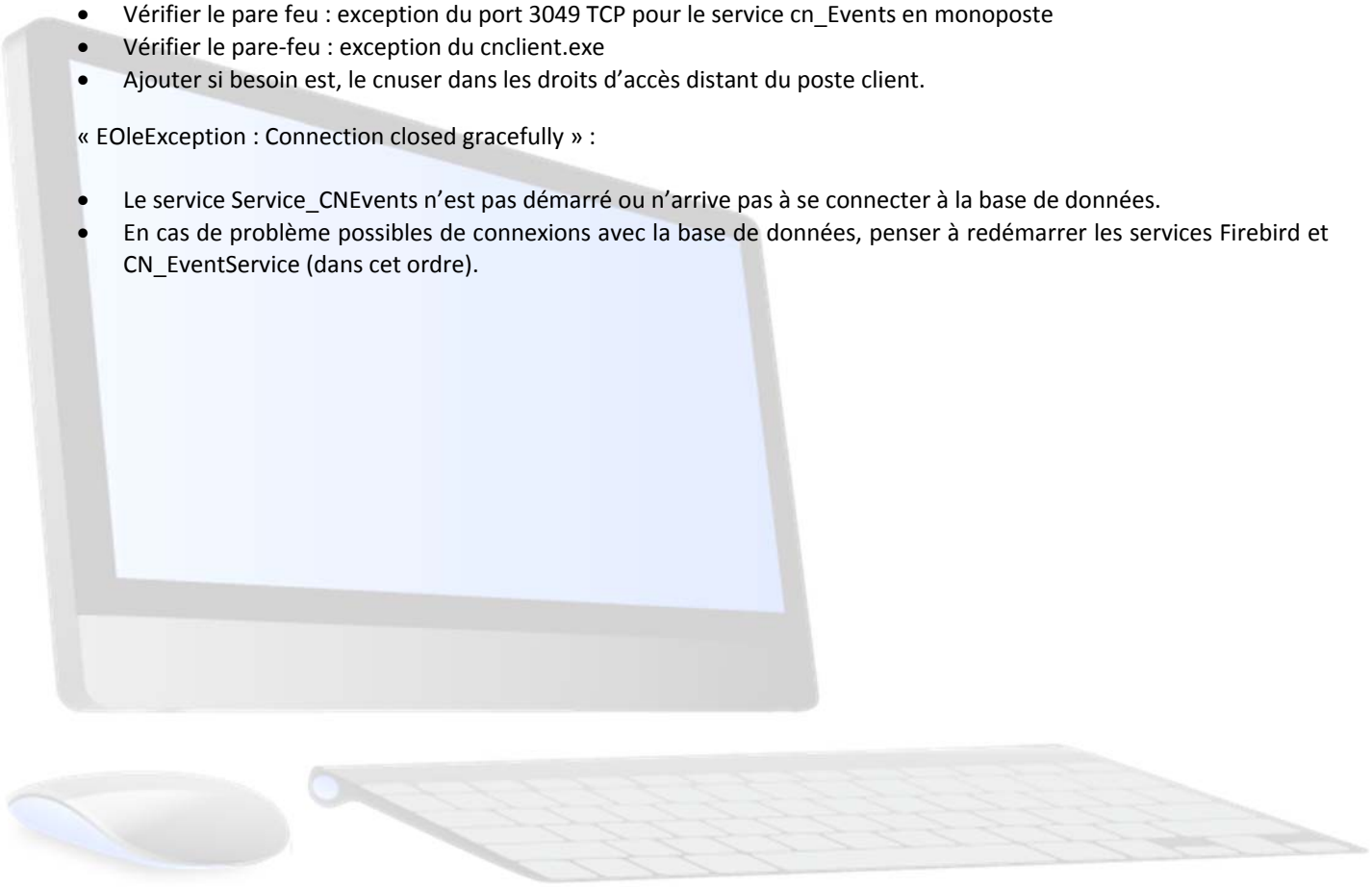
- Vérifier sur le serveur que le CustDllHost.exe ne tourne pas (le terminé si il est présent)
- S'assurer que l'utilisateur Windows du poste client fait bien parti du groupe « Utilisateurs Clair&Net » Vérifier le mot de passe du cnuser

« L'application ne peut pas déterminer le nombre de connexion autorisé » : Le client refuse la connexion du serveur :

- Vérifier le pare-feu : exception du port 135 TCP
- Vérifier le pare feu : exception du port 3049 TCP pour le service cn_Events en monoposte
- Vérifier le pare-feu : exception du cnclient.exe
- Ajouter si besoin est, le cnuser dans les droits d'accès distant du poste client.

« EOleException : Connection closed gracefully » :

- Le service Service_CNEvents n'est pas démarré ou n'arrive pas à se connecter à la base de données.
- En cas de problème possibles de connexions avec la base de données, penser à redémarrer les services Firebird et CN_EventService (dans cet ordre).



Pré requis pour l'installation…

Accès mobile et distant aux progiciels :

La mise en place de ces recommandations est à la charge du client.

Accès distant aux applications bureau :

Avoir un serveur TSE accessible depuis Internet (nécessite une IP Fixe)
En option : Utiliser un VPN pour se connecter au serveur TSE.
En option : Il est préférable, mais pas nécessaire, de différencier le serveur TSE du serveur d'application.

Accès mobile (via tablette) :

Une redirection du port 3051 est à effectuer vers l'adresse IP du serveur où est installée l'application. Chaque fournisseur d'accès Internet a sa propre interface d'administration. Il est conseillé de s'adresser au service technique de son fournisseur d'accès internet pour paramétrer l'accès distant.

Pégase :

Pour pouvoir se connecter à Pégase Mobile depuis une tablette, il faut utiliser un navigateur internet. Cette application peut être utilisée par tous les navigateurs de dernière génération : IE, Chrome, Firefox, Safari, Android browser.

Les adresses de connexion à l'application sont les suivantes :

- http://nom_domaine_serveur:3051/pegase/ (utilisation externe et aussi interne) ou…
- http://nom_serveur:3051/pegase/ (utilisation interne entreprise) ou…
- http://ipfixe_serveur:3051/pegase/ (utilisation interne et externe)

Cette application nécessite que l'appareil mobile dispose d'un accès internet au moment de réaliser les saisies.

Clair' & Net' :

Pour pouvoir utiliser l'application de contrôle qualité (mobile), il faut utiliser un navigateur internet. Les navigateurs supportés sont IE, Chrome et Firefox (en dernière génération). Les plateformes Apple (iOS) ne sont pas encore supportées.

Le fonctionnement de l'application Clair' & Net' Mobile est en mode complètement déconnecté (comme le fonctionnement d'un PDA).

L'utilisation de l'application se fait en 2 phases :

- une première phase de synchronisation des données
- une phase d'exploitation des données (réalisation d'un contrôle qualité).

Seule la phase de synchronisation des données nécessite une connexion du mobile au serveur selon plusieurs méthodes :

- Synchronisation interne à la société ou l'utilisateur se trouve dans les locaux de l'entreprise, connecté par un réseau WiFi à partir duquel le serveur et le mobile communiquent grâce à l'adresse IP du serveur qui doit être fixe.
- Synchronisation externe à la société, (partout dans le monde) le procédé est identique à Pégase, le serveur doit être accessible depuis l'extérieur, soit via une adresse IP fixe ou un nom de domaine. L'appareil mobile doit disposer d'un accès internet au moment du transfert des données.

Les adresses de connexion à l'application sont les suivantes :

- Interne - http://nom_serveur:3051/clairnet/ ou http://ipfixe_serveur:3051/clairnet/
- Externe - http://nom_domaine_serveur:3051/clairnet/ ou http://ipfixe_serveur:3051/clairnet/

Pour le fonctionnement de l'application mobile, il est obligatoire qu'entre 2 phases de synchronisation, l'adresse avec laquelle le mobile se connecte au serveur reste identique.