SAGE Banque Paiement 500
-
Impacts BFC

Référence : -

Date : 18/12/2006

Version : 1.3

Auteurs : Benjamin GIRARD (DSI/BEST), David ROUSSE (DSI/BEST)

Diffusion : RSI-CI-AU, ACP, DSI/BEST/Linux, EAI

Objet du document : ce document présente les impacts techniques de la mise en œuvre de BFC sur les télétransmissions ETEBAC3 entre les délégations et le Trésor Public.

Table des mises à jour du document

Version	Date	Objet de la mise à jour
1.0	25/10/2006	1ère version du document
1.1	17/11/2006	Mise à jour suite au pilote à la DR14
1.2	27/11/2006	Ajout de la partie sur Samba
1.3	18/12/2006	Mise à jour suite à certains retours de DR

Sommaire

1 Introduction

Ce document traite des modifications de paramétrages à apporter en délégations du fait du passage de la GCF à BFC. Ces impacts concernent la configuration SAMBA de la MCOM et la configuration des postes de travail sur lesquels le logiciel SAGE Banque Paiement 500 est installé.

Il est possible de réaliser tout de suite le paramétrage SAMBA de la MCOM. En ce qui concerne le paramétrage lié à Banque Paiement 500, il faudra le réaliser entre la date de clôture de la GCF et la date de démarrage de BFC, donc durant la dernière quinzaine de décembre 2006 (date à confirmer par l'équipe projet BFC).

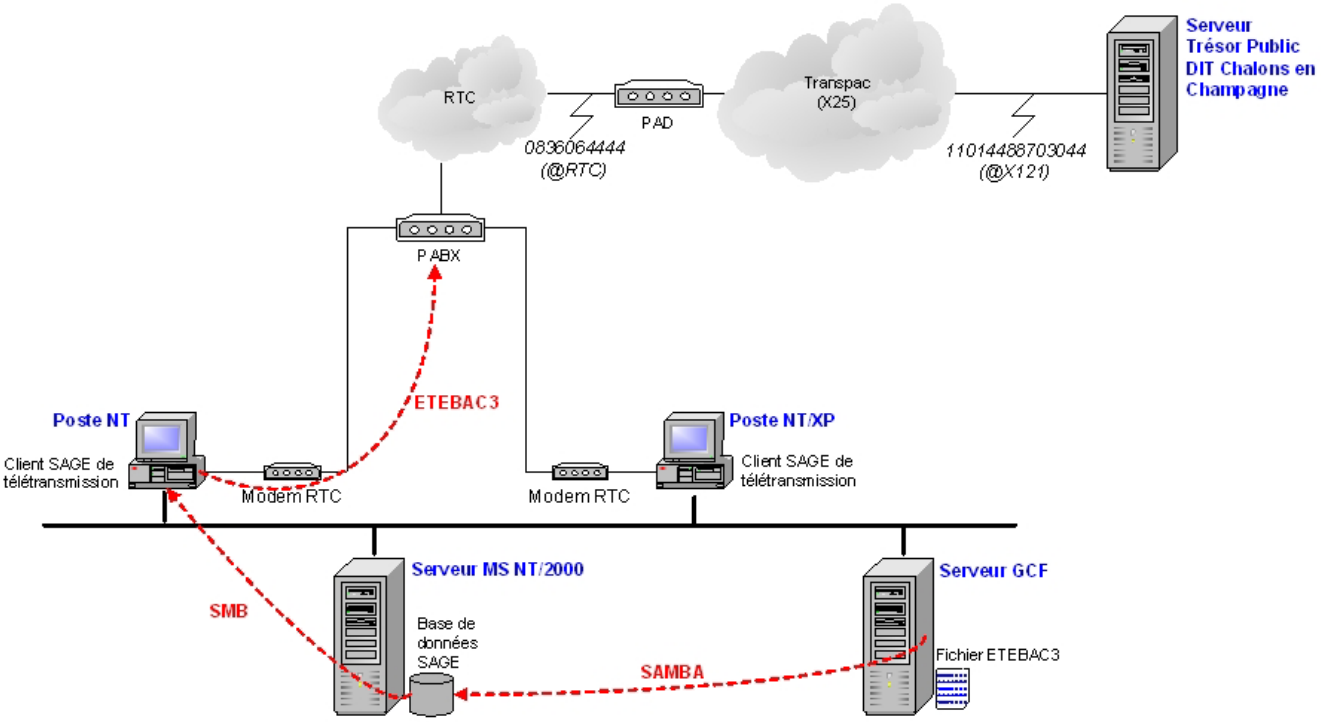
A noter enfin que pour les quelques DR qui utilisent le logiciel DVINT, le format du fichier en sortie de BFC est le même que celui de la GCF. Dans ce cas de figure Les modalités de bascule entre la GCF et BFC sont à convenir entre l'ACP et les DR concernées.

2 Vue d'ensemble du flux

2.1 Configuration actuelle

Le flux des virements fournisseurs et missions fonctionne actuellement ainsi :

- Source : GCF en DR (agents comptables).
- Cible : serveur du Trésor Public de Chalons en Champagne.
- Format du fichier : ETEBAC3.
- Protocole(s) de transfert : ETEBAC3.
- Réseau(x) support(s) : sur RTC puis sur Transpac (X25).
- Logiciel de télétransmission : SAGE Banque Paiement 500.
- Nature du flux : virements bancaires fournisseurs et relevés de compte.
- Volume du flux : 10 Mo mensuel pour l'ensemble des DR.
- Fréquence des télétransmissions : 1 à 3 fois par semaine et par DR environ.
- Type de transfert de données : transfert électronique.
- Moyen de validation du flux : fax envoyé par l'agent comptable de la DR vers le Trésor Public.
- En production depuis : depuis début 2003.
- Détail du flux : GCF en DR → génération du fichier ETEBAC3 et transfert via réseau vers Banque 500 → OK/NOK de l'agent comptable depuis Banque 500 → transfert via ETEBAC3 vers le Trésor Public → Trésor Public.
- Re-soumission du flux : l'agent comptable en DR régénère le fichier depuis la GCF et reprend le circuit normal.
- Contacts : Dolores Lorenzon (ACP), Sylvie Maube (DSI/BBFC), David Rousse (DSI/BEST), Jean-Yves Lopez (DSI/BEST).
- Architecture de la solution :

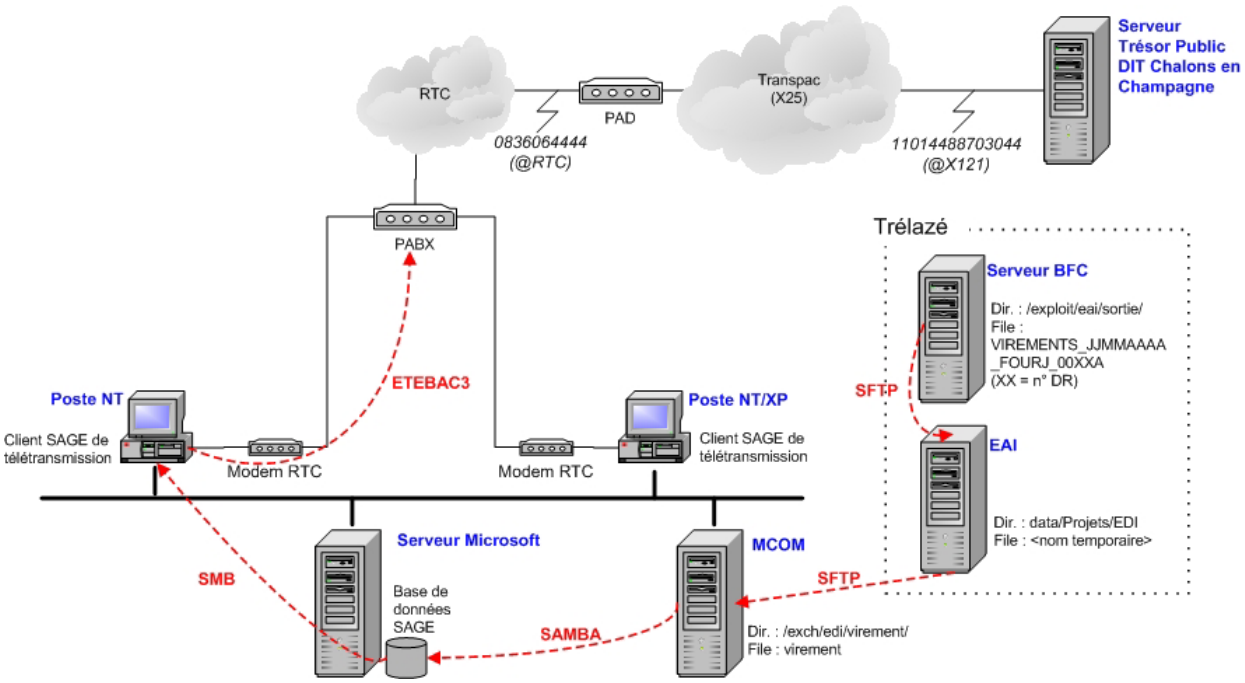


2.2 *Configuration pour BFC*

Le flux des virements fournisseurs et missions avec BFC se résume ainsi :

- Source : BFC (1 fichier par DR généré automatiquement par BFC chaque jour).
- Cible : serveur du Trésor Public de Chalons en Champagne.
- Format du fichier : ETEBAC3.
- Protocole(s) de transfert : ETEBAC3.
- Réseau(x) support(s) : sur RTC puis sur Transpac (X25).
- Logiciel de télétransmission : SAGE Banque Paiement 500.
- Nature du flux : virements bancaires fournisseurs et relevés de compte (flux F51 dans BFC, BFC_S_2330 dans l'EAI).
- Volume du flux : 10 Mo mensuel pour l'ensemble des DR.
- Fréquence des télétransmissions : 1 à 3 fois par semaine et par DR environ.
- Type de transfert de données : transfert électronique.
- Moyen de validation du flux : aucun.
- En production depuis : début 2007.
- Détail du flux : BFC → génération du fichier ETEBAC3 en local (message dans le SAP Office à l'ACS pour info. de mise à dispo.) → récupération du fichier par l'EAI et dépôt sur la MCOM → transfert via réseau vers Banque 500 → OK/NOK de l'agent comptable depuis Banque 500 → transfert via ETEBAC3 vers le Trésor Public → Trésor Public.
- Re-soumission du flux : l'agent comptable en DR doit contacter l'assistance utilisateur BFC afin de remettre à disposition le fichier du jour. L'agent comptable devra indiquer dans sa demande la nature du flux (F51, BFC_S_2330). Pour information, une fois l'information remontée à l'équipe centrale BFC, il faudra que cette dernière prévienne l'équipe d'exploitation EAI pour la remise à disposition du fichier.
- Contacts : Dolores Lorenzon (ACP), Hélène Boussagol (DSI/BFC), David Rousse (DSI/BEST), Jean-Yves Lopez (DSI/BEST), Benjamin Girard (DSI/BEST), Bruno Guibert (DSI/BSU).
- Architecture de la solution[1] :

[1] Schéma donné pour une installation de SAGE de type multiposte.



3 Configuration SAMBA

3.1 Configuration actuelle

Actuellement sur la machine GCF il existe un partage SAMBA (section ***[reglements]*** du fichier ***/etc/opt/samba/lib/smb.conf*** de la machine ***durendal***) qui permet d'accéder au répertoire ***/unidata/reglements*** dans lequel le fichier ***virement*** est généré pour télétransmissions. Ce fichier est ensuite récupéré depuis les postes Windows sur lesquels SAGE Banque Paiement 500 est installé via le montage d'un lecteur réseau (***net use G: \\durendal\reglements***).

3.2 Configuration à mettre en place pour BFC

Le fichier à télétransmettre via SAGE Banque Paiement 500 n'est plus généré par la GCF mais par BFC en central (un fichier par délégation). Le transfert devient donc à présent :

1. Exécution (journalière et automatique) du flux BFC_S_2330 dans BFC.
2. Génération d'un fichier par DR sur la machine BFC.
3. Prise en compte (journalière et automatique) de fichiers par l'EAI.
4. Dépôt par l'EAI (via transfert SFTP) sur chaque MCOM des fichiers dans le répertoire ***/exch/edi/virement***.
5. Accès depuis les postes Windows au répertoire ***/exch/edi/virement*** afin de récupérer le fichier ***virement***.

Afin de mettre en œuvre cela, il est nécessaire sur votre MCOM de mettre en place un paramétrage SAMBA donc la documentation est donnée par l'équipe Linux de la DSI (Benjamin GIRARD).

3.2.1 Création de l'arborescence virement

Voici les commandes à executer pour créer l'arborescence /exch/edi/virement :

```
# mkdir -p /exch/edi/virement
# chown -R eaiadm:eaiadm /exch/edi
# chmod 710 /exch/edi (sauf à la DR05, DR16 et DR19 : 711)
# chmod 770 /exch/edi/virement
```

1.1.1 Configuration réseau

Protocole	@IP source	port source	@IP destination	port destination
icmp	IP GRAAL		IP ZEBIGBOS	
TCP	IP GRAAL	gt 1023	IP ZEBIGBOS	389
UDP	IP GRAAL	53	IP ZEBIGBOS	53
UDP	IP GRAAL	53	IP ZEBIGBOS	gt 1023
UDP	IP GRAAL	gt 1023	IP ZEBIGBOS	88
UDP	IP GRAAL	137	IP ZEBIGBOS	137
UDP	IP GRAAL	138	IP ZEBIGBOS	138
TCP	IP GRAAL		IP ZEBIGBOS	749
UDP	IP ZEBIGBOS	88	IP GRAAL	gt 1023
UDP	IP ZEBIGBOS	137	IP GRAAL	137
TCP	IP POSTE CLIENT		IP GRAAL	445

1.1.2 Mise en place du partage samba

1.1.2.1 Introduction

Il existe deux types de *niveau de sécurité* pour Samba, à savoir *share-level* (niveau du partage) et *user-level* (niveau de l'utilisateur). La sécurité au niveau du partage peut être implémentée d'une seule manière alors que la sécurité au niveau de l'utilisateur peut elle être mise en oeuvre de quatre manières différentes. On appelle *modes de sécurité* les différentes manières d'implémenter un niveau de sécurité.

Nous utiliserons le *niveau de sécurité user-level* que nous implementerons avec le *mode de sécurité Active Directory.*

L'utilisateur qui voudra se connecter au partage samba sera authentifié auprés de l'Active Directory par graal en utilisant winbind et en s'appuyant sur le protocole kerberos .

1.1.2.2 Pre-requis:

Vérifier la présence des rpms suivant avec la commande « rpm -qa | grep -i nom-du-rpm »:

- samba-common-3.0.10-1.4E.9
- samba-3.0.10-1.4E.9
- system-config-samba-1.2.21-1
- samba-client-3.0.10-1.4E.9
- pam-devel-0.77-66.17
- pam_smb-1.1.7-5
- pam_krb5-2.1.8-1
- pam-0.77-66.17
- krb5-libs-1.3.4-33
- krb5-devel-1.3.4-33
- krb5-auth-dialog-0.2-1
- krb5-workstation-1.3.4-33
- glibc-2.3.4-2.25

- openldap-2.2.13-6.4E
- openldap-devel-2.2.13-6.4E

Nous avons besoins d'installer en plus les rpms suivants:

- nss_ldap-226-17.i386.rpm
- nscd-2.3.4-2.25.i386.rpm

1.1.2.3 Mise en place des fichiers de configuration sur Graal

Dans cette partie de la doc « xy » correspond à votre numéro de DR.
Nous allons configurer les 4 fichiers nécessaires au bon fonctionnement de samba en mode ADS :

- **/etc/krb5.conf**

Sauvegardez votre fichier original :

```
# mv /etc/krb5.conf /etc/krb5.conf.orig
```

Puis copiez le contenu ci dessous dans le fichier /etc/krb5.conf

```
# vi /etc/krb5.conf
```

Les valeurs en rouge sont les valeurs à customiser par DR.

```
[logging]
        default = FILE:/var/log/krb5libs.log
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = AD.DRxy.CNRS.FR
        dns_lookup_realm = false
        dns_lookup_kdc = false

[realms]
        AD.DRxy.CNRS.FR = {
                admin_server = xyZEBIGBOS.AD.DRxy.CNRS.FR:749
                default_domain = AD.DRxy.CNRS.FR
                kdc = xyZEBIGBOS.AD.DRxy.CNRS.FR:88
        }

[domain_realm]
        .ad.drxy.cnrs.fr = AD.DRxy.CNRS.FR
        ad.drxy.cnrs.fr = AD.DRxy.CNRS.FR

[kdc]
        profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
        pam = {
                debug = false
                ticket_lifetime = 36000
                renew_lifetime = 36000
                forwardable = true
                krb4_convert = false
```

```
}
```

Editez le fichier /etc/hosts et rajoutez les lignes suivantes :

```
# vi /etc/hosts
        127.0.0.1       graal    graal.ad.drxy.cnrs.fr
        ip-zebigbos     xyzebigbos.ad.drxy.cnrs.fr        xyzebigbos
```

Maintenant, nous devons nous assurer que la connexion à l'Active Directory est possible. Pour ce faire, nous allons tester la communication grâce à la commande d'initialisation :

```
# kinit user@AD.DRxy.CNRS.FR
```

Le résultat nous demande un mot de passe. Si celui-ci est valide, nous nous retrouverons en mode saisie qui indique que tout s'est bien passé.

La commande suivante permet de voir le ticket kerberos récupéré :

```
# klist
```

Si vous obtenez le message *« Cannot find KDC for requested realm while getting initial credentials »,* cela veut dire que graal n'arrive pas à entrer en contact avec votre kdc (ici votre AD). Il faut vérifier qu'il arrive bien à récuperer l'IP. A défaut vous pouvez remplacer xyZEBIGBOS.AD.DRxy.CNRS.FR par l'ip de xyzebigbos

- **/etc/pam.d/system-auth**

Sauvegardez votre fichier original :

```
# mv /etc/pam.d/system-auth /etc/pam.d/system-auth.orig
```

Puis copiez le contenu ci dessous dans le fichier /etc/pam.d/system-auth

```
# vi /etc/pam.d/system-auth
```

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.

auth required /lib/security/$ISA/pam_env.so
auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok
auth sufficient /lib/security/$ISA/pam_krb5.so use_first_pass
auth required /lib/security/$ISA/pam_deny.so

account required /lib/security/$ISA/pam_unix.so broken_shadow
account sufficient /lib/security/$ISA/pam_succeed_if.so uid < 100 quiet
account [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_krb5.so
account required /lib/security/$ISA/pam_permit.so

password requisite /lib/security/$ISA/pam_cracklib.so retry=3 type=
password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password sufficient /lib/security/$ISA/pam_krb5.so use_authtok
password required /lib/security/$ISA/pam_deny.so

session required /lib/security/$ISA/pam_limits.so
session required /lib/security/$ISA/pam_unix.so
session optional /lib/security/$ISA/pam_krb5.so
```

- **/etc/nsswitch.conf**

remplacer les lignes

```
passwd: files
shadow: files
group: files
```

par

```
passwd: files winbind
shadow: files winbind
group: files winbind
```

- **/etc/samba/smb.conf**

Sauvegardez votre fichier original :

```
# mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

Puis copiez le contenu ci dessous dans le fichier /etc/samba/smb.conf

```
# vi /etc/samba/smb.conf
```

Les valeurs en rouge sont les valeurs à customiser par DR.

```
[global]
        workgroup = DRxy
        server string = Graal
        netbios name = graal
        hosts allow = xx.yy.zz.

        security = ADS
        password server = xyZEBIGBOS.AD.DRxy.CNRS.FR
        realm = AD.DRxy.CNRS.FR
        encrypt passwords = yes
        wins server = ip-wins1 ip-wins2 …

        allow trusted domains = yes
        client use spnego = yes

        # log level = 3 passdb:5 auth:10
        log file = /var/log/samba/%m.log
        max log size = 50

        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        dns proxy = no

        idmap uid = 16777216-33554431
        idmap gid = 16777216-33554431

        load printers = no
        show add printer wizard = no

[Virement]
        browseable = yes
        printable = no
        writable = yes
        path = /exch/edi/virement
        comment = Repertoire de depot des fichiers de virement
        public = no
        valid users = "@DSI\PJT-SAMBAGRAAL"
        force group = eaiadm
```

Explication pour les valeurs en rouge :

- workgroup = nom de votre domaine (ex : DRxy)
- host allow = adresse ip ou adresse réseau autorisées à se connecter (pas obligatoire)
- password server = nom de votre serveur AD en majuscule (ex: xyZEBIGBOS.AD.DRxy.CNRS.FR)
- realm = c'est le realm de kerberos (ex : AD.DRxy.CNRS.FR)
- wins server = adresse de vos serveur wins (ex : ip de votre serveur AD)
- valid users = mettre le groupe windows autorisé à acceder au partage, il s'agit normalement du groupe reglement. Vous devez donc avoir pour ce champs :

  valid users = «@DRxy\reglement»

Attention !! Si vous utilisez déjà samba pensez à récupérer vos anciens partages!!
Pour tous ces partages il faut créer un groupe dans l'AD contenant les utilisateurs autorisés.
Ensuite il faut définir le champs « valid users » adéquate.

Une fois la configuration de samba terminée, il faut redémarrer le service :

```
# service smb restart
```

1.1.2.4 Activation de winbind

Lors de l'installation de graal nous avons désactivé winbind.
Voici les commandes à executer pour le relancer:

```
# chkconfig winbind on
# service winbind start
```

Rem : A chaque fois que le fichier smb.conf est modifié et que samba est relancé, il faut penser à relancer winbind

1.1.2.5 Intégration de graal dans l'Active Directory

Assurez vous de disposer d'un compte windows permettant l'ajout de machine dans le domaine.
Pour joindre le serveur Graal à votre domaine, saisissez la commande suivante :

```
# net ads join -U user
```

Au bout de quelques minutes vous devriez voir Graal dans votre voisinage réseau windows et plus particulièrement dans le domaine DRxy.

Normalement les personnes appartenant au groupe « règlement » pourront alors se connecter au partage samba « virement » sans avoir à saisir de mot de passe. Le fait d'être authentifié sur leur poste suffira. Les personnes n'appartenant pas au groupe « règlement » ne seront pas acceptées.

4 Configuration des postes SAGE

4.1 Configuration actuelle

Le script ***moveGCF.bat*** suppose qu'un lecteur réseau soit mappé vers le partage SAMBA appelé ***reglements*** sur la machine ***durendal***. Le script, appelé par l'intermédiaire de SAGE Banque Paiement 500, permet de déplacer le fichier ***virement*** présent sur durendal dans ***F:\DRxy\Tresor\TRVIR.VIG*** (ou ***C:\SAGE500\DRxy\Tresor\TRVIR.VIG*** en monoposte). Les utilisateurs autorisés à accéder au partage ***reglements*** sur la machine ***durendal*** sont ceux présents dans le groupe Windows appelé ***reglement***[2].

4.2 Configuration à mettre en place pour BFC

Au niveau de l'***Active Directory*** Windows, il convient de vérifier que le groupe mentionné dans la configuration SAMBA du partage sur la MCOM (valeur de ***valid users*** de la section ***[Virement]*** du fichier ***/etc/samba/smb.conf*** de la machine ***graal***) existe bien dans l'AD et contient les utilisateurs habilités à utiliser le logiciel SAGE Banque Paiement 500.

Il est également nécessaire de vérifier que le ou les poste(s) sur lesquels SAGE Banque Paiement 500 est installé peuvent accéder à la MCOM sur le port 445. Si tel n'est pas le cas, faire ouvrir le filtre réseau en conséquence :

```
telnet graal.dr***x***.cnrs.fr 445
```

Sur tous les postes clients sur lesquels SAGE Banque Paiement 500 est installé, faire :

[2] Configuration par défaut proposée par la DSI lors de la mise en place de SAGE, le groupe Windows peut avoir été modifié, la valeur est en fait celle de la variable ***valid users*** de la section ***[reglements]*** du fichier /etc/opt/samba/lib/smb.conf de durendal.

a) Ouvrir une session avec le compte de l'utilisateur.
b) Ouvrir un explorateur et regarder quel le nom de lecteur associé au partage ***reglements*** de ***durendal*** (en cas de doute sur la lettre, éditer le fichier ***moveGCF.bat***, le nom de lecteur est celui indiqué dans la variable ***source***[3] du script). **Par défaut (script fourni par la DSI), le nom de lecteur est G:**
c) Ouvrir une console DOS et taper :

```
net use /delete g:
net use g: /persistent:yes \\graal.dr***x***.cnrs.fr\virement
```

d) Redémarrer le poste (ouvrir la session avec le compte de l'utilisateur), ouvrir un explorateur Windows et vérifier que le lecteur *G:* est monté, et qu'il est accessible.

5 Contacts

Pour toute question, merci de bien vouloir contacter l'assistance utilisateur de la DSI.

[3] Dans la variable ***source*** du script moveGCF.bat, ***G:***\ correspond au lecteur Windows mappé vers le partage SAMBA alors que ***virement*** représente le nom du fichier déposé par l'EAI. Donc dans la nouvelle configuration proposée par la DSI, on aura un partage SAMBA sur la MCOM appelé ***virement***, mappé sur la lettre G:, et un fichier ***virement*** déposé par l'EAI dans ce répertoire.