Guide pratique de mise en œuvre de XDMCP sous Linux

Version française du Linux XDMCP HOWTO

Thomas Chao

<tomchao CHEZ lucent POINT com>

Adaptation française : Denis Berhaut

Relecture de la version française : Éric Madesclair

Préparation de la publication de la v.f. : Jean-Philippe Guérard

Version : 1.3.fr.1.0

26 janvier 2005

Historique des versions		
Version 1.3.fr.1.0	2005-01-26	DB, ÉM, JPG
Première version française.		
Version 1.3	2003-01-02	TC
Ajout d'informations pour la configuration de Red Hat 7.3 & 8.0, Mandrake 8.2 & 9.0, SuSE et mise à jour de contenu.		
Version 1.2	2002-03-15	TC
Ajout d'informations sur la configuration de Linux Red Hat 7.2, Mandrake 8.1 et Slackware 8.0 ainsi que sur le transfert de X11 sous SSH.		
Version 1.1	2001-03-20	TC
Révision et ajout de RH 7.0.		
Version 1.0	2000-11-01	TC
Première révision et diffusion.		

Résumé

Ce guide pratique explique comment utiliser ensemble un gestionnaire d'affichage X (xdm, kdm et gdm) et XDMCP (le protocole de contrôle du gestionnaire d'affichage X) pour fournir une solution de terminaux X et une plate-forme d'exécution efficace d'applications X à distance. Ce document met l'accent sur la configuration d'une connexion X avec XDMCP.

Table des matières

1. Introduction

XDMCP signifie « protocole de contrôle du gestionnaire d'affichage X » ; c'est un protocole réseau. Il constitue un moyen de faire tourner un terminal X sur votre PC (ou votre MAC) en utilisant le serveur X qui fournira une interface client-serveur entre le matériel d'affichage (la souris, le clavier et les affichages vidéo) et l'environnement de l'ordinateur, tout en offrant l'infrastructure d'affichage et une interface d'application standardisée (référence issue de la page d'accueil du projet Xfree86). Le terminal X peut être affiché dans une fenêtre individuelle ou dans de multiples fenêtres, en fonction des capacités logicielles et de la configuration de votre système d'affichage X.

Je recherche toujours la meilleure façon d'utiliser Linux, que ce soit à la maison au travail. L'un de ses avantages entre tous est sa capacité à réutiliser les vieux systèmes (tels que des 486 et des Pentium, Pentium II) comme terminaux X (en utilisant les applications Win32 telles que Exceed (de Hummingbird), Reflection X, X-Win32 or X-ThinPro ; sous MAC, essayez eXodus) pour s'exécuter à distance sur n'importe lequel de vos PC. J'ai découvert avec une certaine surprise qu'il y a beaucoup de documents sur Internet qui peuvent vous aider à le configurer, mais pas sous forme de guide pas à pas !Voici pourquoi j'en suis venu à écrire ce document qui m'a paru être une manière de partager mes expériences avec tous les utilisateurs. En utilisant X et XDMCP, vous pouvez bâtir pour la maison ou le travail une bonne solution, fiable et bon marché.

1.1. Limitations de responsabilité

Aucune responsabilité légale ne sera acceptée quant au contenu de ce document. L'utilisation des concepts, exemples et autres contenus du document s'effectue à vos risques et périls. Dans la mesure où il s'agit d'une nouvelle édition de ce document, il peut comporter des erreurs ou des inexactitudes, évidemment susceptibles d'endommager votre système. Procédez prudemment, et bien que cela soit improbable, le ou les auteurs refusent toute responsabilité à ce sujet.

Sauf mention spécifique, les droits d'auteur sont la possession de leurs propriétaires respectifs. L'utilisation d'un terme dans ce document ne doit pas être considérée comme ayant une influence sur la validité d'une quelconque marque déposée ou marque de services.

Le fait de nommer un produit ou une marque ne doit pas être considéré comme une recommandation.

Nous vous recommandons fortement d'effectuer une sauvegarde de votre système avant toute installation importante et d'effectuer des sauvegardes à intervalles réguliers.

1.2. Nouvelles versions de ce document

Vous trouverez la plus récente version française de ce document à l'adresse :
http://www.traduc.org/docs/howto/lecture/XDMCP-HOWTO.html.

La plus récente version originale de ce document est disponible à l'adresse :
http://tldp.org/HOWTO/XDMCP-HOWTO/index.html.

1.3. Commentaires et réactions

Les commentaires sur ce document sont bienvenus. Sans vos suggestions et autres apports, ce document n'existerait pas. Envoyez-moi (en anglais) vos ajouts, commentaires et critiques à l'adresse suivante : <`tomchao CHEZ lucent POINT com`>.

N'hésitez pas à faire parvenir vos commentaires et suggestions concernant l'adaptation française de ce document au projet Traduc.org à l'adresse : <`commentaires CHEZ traduc POINT org`>.

2. La procédure

Cette section détaille la procédure de configuration d'un terminal X avec XDMCP. Comme pré-requis, vous devez avoir n'importe quelle distribution Linux installée, ainsi que X.

2.1. Avant de commencer, quelques notions

Avant de commencer, il vaut mieux comprendre globalement le fonctionnement. (Vous trouverez plus de détails Ressources [p ??] ci-dessous et sur le site de Traduc.org)

D'habitude, le serveur X est lancé à partir d'un gestionnaire d'affichage X. Presque toutes les distributions Linux embarquent xdm, kdm et gdm. Le choix de l'un d'entre eux est libre. (Ce document se servira de gdm et kdm comme exemples). Le gestionnaire d'affichage constitue une interface agréable et uniforme pour les utilisateurs lambda (ouverture de session graphique, démarrage d'un gestionnaire de fenêtre, horloge, et cætera). Un gestionnaire d'affichage contrôle une série d'affichages X, qui peuvent être situés sur l'hôte local ou sur des serveurs distants. Il est bon de noter que ce qu'exécute votre environnement est le fichier `Xsession`.

Quand xdm s'exécute, il propose deux manières différentes de gérer l'affichage. Il peut gérer un serveur X qui s'exécute sur la machine locale (indiqué dans `Xservers`) et des serveurs X distants (en général des terminaux X) en utilisant XDMCP (en fonction de ce qui est indiqué dans le fichier `Xaccess` — voir les pages de manuel de xdm).

Quant à kdm (qui fait partie de l'environnement graphique KDE), c'est un remplaçant de xdm qui se configure de façon identique, à ceci près que ses fichiers sont `/etc/X11/kdm` pour Caldera, dans `/etc/kde/kdm` pour Red Hat, et dans `/usr/share/config/kdm` pour Mandrake.

Le gdm (Gestionnaire d'affichage Gnome) est une réécriture du fameux xdm. Les fonctions de gdm sont similaires à celles de xdm et kdm. Gdm (gdm) est le gestionnaire d'affichage de Gnome, et ses fichiers de configuration sont situés dans `/etc/X11/gdm/gdm.conf`. Le fichier `gdm.conf` contient un ensemble de variables et un grand nombre d'options pour gdm. Le répertoire Sessions contient un script pour chaque option de session ; chaque script appelle `/etc/X11/xdm/Xsession` avec l'option appropriée. Gdm offre des fonctions similaires à xdm et kdm, mais a été écrit à partir de zéro et ne contient aucun code originaire de XDM ou du consortium X.

Avec RH 8.0, une nouvelle interface graphique appelée « Bluecurve » apparaît. Son objectif est d'imiter l'apparence de XP. Dans ce cas, il n'y a aucune différence de configuration !

On peut trouver d'autres bonnes références pour une configuration similaire dans les documents suivants :

- Le petit guide XDM et les terminaux X, écrit par Kevin Taylor.
- Le Petit guide d'exécution à distance des applications X, une excellente référence d'approche pratique et théorique d'exécution de X à distance. Écrit par Vincent Zweije.
- Le petit guide Xterminal, écrit par Scot W. Stevenson.

2.2. Rappel de sécurité

L'utilisation de XDMCP est par définition dangereuse, ce qui fait que la plupart des distributions ont désactivé son utilisation par défaut. Si vous devez utiliser XDMCP, ne le faîtes qu'au sein de réseaux sécurisés, tels que des réseaux d'entreprises protégées par un pare-feu. Malheureusement, XDMCP utilise le port UDP 177 et TCP le port 6000 ; il n'est donc pas possible de l'utiliser nativement avec SSH. Actuellement, SSH1 et SSH2 ne permettent pas de transmettre les communications UDP de manière sécurisée.

La technique de sécurisation des connexions via SSH est appelée transfert de port X11 TCP/IP (X11 TCP/IP Port Forwarding). Rendez-vous sur Why Port Forwarding? et dans la section Ressources [p ??] pour des informations complémentaires (en anglais). Au cas où vous voudriez l'expérimenter, j'ai ajouté une petite section plus bas pour vous montrer son fonctionnement. Je vous décrirai sommairement son fonctionnement ; je laisse les autres experts et/ou les guides pratiques vous expliquer son utilisation avancée.

2.3. Mon système

J'ai testé les configurations de GNOME (gdm) et de KDE (kdm) sur Red Hat 6.0, 6.2 et Red Hat 7.x et 8.0. J'ai eu aussi la chance de les tester sur Mandrake 7.2, 8.0, 8.2 et 9.0. Les configurations de SuSE 7.2 and Slakware 8.0 ont été testées par les utilisateurs ; merci à Peter Van Aerten et à tous ceux qui m'ont aidé à la préparation de ce guide pratique. Je désire remercier tous les utilisateurs qui m'ont aidé à réaliser ce projet. J'ai aussi essayé sur Caldera eDesktop 2.4, dont la configuration est similaire à celle de RH, à la différence qu'il utilise KDE. Je n'ai pas eu l'occasion de tester sur d'autres variantes telles que Debian ou Slackware (les utilisateurs de Slackware m'ont rapporté que le fonctionnement est identique à celui décrit dans ce document). Cependant, la configuration devrait être similaire et devrait bien fonctionner. Si vous avez réussi à configurer sur d'autres distributions que Red Hat, Caldera et Mandrake, faites-moi partager votre expérience. Je l'ajouterai à ce document.

Le PC que j'utilise est un compatible IBM, équipé d'un AMD Athlon XP 1800+, de 384 Mo de mémoire et d'un disque dur de 60 Go ATA-100. Cette machine a été mise à jour à partir d'un PC équipé d'un Intel Pentium II 500 MHz (je me suis aperçu que mon vieux PC Pentium 100 MHz marche très bien). J'utilise une carte Fast Ethernet intégrée dans ma nouvelle carte mère AMD. Sur mon vieux PC, j'utilise l'adaptateur 3Com 10/100 (3C509B), un cédérom 48X et un disque ZIP IOMEGA. J'ai aussi effectué des tests avec mon portable Toshiba Tecra 8100 connecté par carte sans fil Agere.

2.4. Pièces rapportées

J'utilise Exceed 7.0 (Exceed 6.x fonctionne aussi correctement) sur mon PC, et je les ai testé sous Windows 98 SE, Windows NT 4.0 et Windows 2000 Pro. J'ai aussi constaté que X-Win32 et X-ThinPro sont d'autres choix répandus. Il existe également beaucoup d'applications, libres ou commerciales.

2.5. Préparation du serveur

Sous RH 7.x, il faut configurer la recherche des DNS, pour permettre à certaines fonctions de réseau de fonctionner correctement (comme **telnet** qui sera utilisée pour tester la configuration). Vous pouvez saisir **`netstat -r`** ou **`arp -a`** pour vérifier la configuration des DNS ou les temps de réponse. Si vous êtes dans un petit environnement (comme à la maison ou un petit réseau d'entreprise) qui n'a pas son propre serveur DNS et qui utilise le serveur DNS du FAI, ajoutez l(es) adresse(s) des serveurs de noms dans le fichier `resolv.conf`. Si vous l'utilisez uniquement à la maison ou au labo, vous pouvez alors ajouter dans votre fichier local les noms d'hôte de toutes les stations de travail `host`.

Pour que votre serveur X accepte une session XDMCP, assurez-vous que les éléments suivants sont bien installés :

1. Installez votre OS Linux. Dans mon cas, j'ai installé Red Hat 7.3 (installation personnalisée). Si vous projetez d'utiliser SSH pour faire du transfert de port, il vous faudra installer le paquetage OpenSSH ou compiler SSH dans le kernel. De plus, RH 7.x est fourni avec un pare-feu installé par défaut (à moins que vous ne fassiez pas ce choix). Vous pourrez rencontrer des problèmes si vous n'ajoutez pas des règles à votre pare-feu ou si vous ne le neutralisez pas temporairement le temps de configurer XDMCP. Je ne détaillerai pas les règles du pare-feu dans la mesure où ce n'est pas l'objet de ce document. Je montrerai seulement comment le faire fonctionner, à charge pour vous de le régler finement.

   Avec le noyau 2.2x, vous afficherez les règles de votre pare-feu en saisissant la commande **`ipchains -L`**. Pour le désactiver temporairement, utilisez la commande **`ipchains -F`** pour effacer les règles (pas de panique, elles seront restaurées en les rechargeant ou au redémarrage). Avec le noyau 2.4x, remplacez la commande **ipchains** par **iptables**. Un utilisateur m'a indiqué qu'en ajoutant cette règle, vous n'aurez pas besoin de désactiver votre pare-feu et que vous pourrez accéder au serveur X (vous pouvez le vérifier par vous-même).

   ```
   ipchains -A input -p udp -i $extint --dport 177 -j ACCEPT
   ```

Vous devriez pouvoir utiliser la commande **iptables** de manière identique. (Vous trouverez des références à iptables dans les Ressources [p ??]).

Pour plus de détails sur les pare-feu, rendez-vous sur la page du Guide pratique de masquage IP.

Il est aussi possible d'ajouter des règles pour qu'il accepte uniquement les adresses IP des stations de travail de confiance. Vous pouvez utiliser la commande **iptables** à votre gré. Je rappelle que sa description n'est pas l'objet de ce document. J'ai de la chance dans le sens où j'utilise le pare-feu de ma société.

2. Configuration du réseau. Vous pouvez utiliser les commandes **ping**, **ftp** et **telnet** pour tester le fonctionnement de votre réseau. Pour des raisons de sécurité, le démon de la commande **telnet** est désactivé sur RH 7.x et versions ultérieures. Pensez à l'activer si vous désirez l'utiliser pour effectuer vos tests. Vous pourrez toujours le désactiver (avec la commande **ntsysv**) lorsque vous en aurez terminé. Il est aussi bon de se souvenir que les règles du pare-feu sont actives. Ajoutez vos propres règles ou désactivez les temporairement (comme mentionné plus haut) pour permettre l'exécution de ces commandes.

3. Configuration de X

   Ne configurez pas X avec une résolution plus haute que celle dont les utilisateurs distants pourront disposer. Testez le serveur X en saisissant soit **startx** soit **telinit 5**. Assurez-vous que X fonctionne correctement.

4. Créez les comptes indispensables (et les groupes associés) pour les utilisateurs devant accéder par le terminal X.

2.6. Procédures à suivre

J'ai utilisé les étapes suivantes pour configurer le serveur X afin qu'il accepte les requêtes XDMCP :

1. Dans un environnement grahique Linux, les polices utilisées sont soit celles du serveur X (xfs), soit celles dont le chemin est spécifié dans les fichiers de configuration XF86Config ou XF86Config-4. .Si vous prévoyez d'utiliser le serveur de polices xfs (cliquez ici pour voir les avantages de xfs), pour RH 6.2 et Mandrake 8.x et 9.0, modifiez le fichier `/etc/rc.d/init.d/xfs` et apportez-y les modifications suivantes. Changez tout ce qui suit (cela concerne le port du serveur de polices) :

   ```
   daemon xfs -droppriv -daemon -port
             -1
   ```

   en:

   ```
   daemon xfs -droppriv -daemon -port
             7100
   ```

   Dans la Mandrake 7.2, le port est déjà 7100. De plus, sur la RH 7.x, l'écoute sur un port TCP est à présent désactivée par défaut pour des raisons de sécurité ! Si vous désirez paramétrer le serveur de polices de X, suivez les étapes

   Changez la ligne suivante du fichier `/etc/rc.d/init.d/xfs` :

```
daemon xfs -droppriv -daemon
```

en :

```
daemon xfs -droppriv -daemon -port 7100
```

Puis, dans `/etc/X11/fs/config`, mettez cette ligne en commentaires :

```
# Ne pas écouter sur les ports TCP (pour des raisons de sécurité)
#no-listen = tcp
```

Si vous changez ou ajoutez le port, utilisez cette commande pour redémarrer votre serveur de polices X (nécessite les droits de root) :

```
service xfs restart
```

Le port 7100 n'est pas obligatoire. Vous pouvez choisir un autre port, dans la mesure où vous aurez vérifié soigneusement que ce port n'occasionne pas de conflit. Il est de bon ton de consulter votre administrateur Linux avant de le faire, afin qu'il sache que le port est utilisé ! Les différentes distributions Linux peuvent placer xfs dans différents répertoires sous /etc/rc.d. Si c'est le cas, vous pouvez le rechercher.

2. Modifiez `/etc/X11/xdm/xdm-config` en effectuant les modifications suivantes : Par défaut dans la plupart des distributions Linux, cette ligne est active, ce qui fait qu'il n'écoute pas les connexions XDMCP. Ceci pour des raisons de sécurité. Pour Caldera et en utilisant kdm, le fichier est situé en `/etc/X11/kdm`. Trouvez cette ligne :

   ```
   DisplayManager.requestPort: 0
   ```

   et mettez la en commentaire comme ceci :

   ```
   ! DisplayManager.requestPort: 0
   ```

   Rappelez vous que ceci n'affecte pas gdm. La configuration de gdm se trouve dans la section suivante.

3. Dans le fichier `/etc/X11/xdm/Xaccess` modifiez ce qui suit. (cela permet à tous les hôtes de se connecter). Pour Caldera, et en utilisant kdm, le fichier est situé en `/etc/X11/kdm`. Changez les droits d'accès en 644 (chmod 644) :

   ```
   #* # any host can get a login window
   ```

   en :

   ```
   * # any host can get a login window
   ```

   La configuration ci-dessus est en mode Diffusion (Broadcast), qui permet d'établir la liste de tous les serveurs X écoutant les demandes de prise en charge de connexion X et en mesure de l'effectuer. Si vous désirez n'autoriser que certaines connexions, utilisez la section **CHOOSER** du même fichier. Vous trouverez un exemple dans les Ressources [p ??] .

4. J'utilise gdm par défaut ainsi que l'invite de connexion gdm pour permuter KDE et GNOME. Pour gdm, éditez le fichier `/etc/X11/gdm/gdm.conf`. Ce qui suit active XDMCP, en le faisant écouter les requêtes. Pour kdm (si vous avez choisi KDE comme gestionnaire d'affichage lors de l'installation), éditez le fichier `/usr/share/config/kdm/kdmrc` pour Mandrake et

`/etc/kde/kdm/kdmrc` pour Red Hat ou `/opt/kde2/share/config/kdm/kdmrc` pour Slackware version (KDE2). Modifiez cette ligne :

```
[xdmcp]
# false peut être remplacé par 0 dans certaines distributions
Enable=false
```

en :

```
# true peut être remplacé par 1 dans certaines distributions
Enable=true
```

Assurez-vous que `Port=177` est présent à la fin de ce bloc.

5. À présent, éditez le fichier `/etc/inittab` et modifiez la ligne suivante :

```
id:3:initdefault:
```

en:

```
id:5:initdefault:
```

Dans la Slackware, le mode graphique (X11) est `4` et non `5`.

Ceci fait passer la connexion du mode ligne de commande en mode graphique. Vous pouvez utiliser la commande **telinit** pour effectuer un test avant de modifier cette ligne. Utilisez soit **telinit 3** pour passer au niveau 3, ou **telinit 5** pour passer au niveau 5 en mode graphique (vous pouvez essayer cette commande sur la deuxième machine reliée par telnet à votre serveur).

6. Assurez-vous que les attributs de sécurité du fichier `/etc/X11/xdm/Xservers` sont fixés à 444 (chmod 444).

7. Localisez `/etc/X11/xdm/Xsetup_0` et exécutez **chmod 755** sur ce fichier.

8. Éditez le fichier `XF86Config` (si vous utilisez Xfree86 4.x, le fichier se nomme `XF86Config-4`) situé en `/etc/X11` et modifiez la ligne :

```
FontPath "unix/:-1"
```

en :

```
FontPath "unix/:7100"
```

Si vous décidez d'utiliser un port différent du traditionnel port 7100, assurez-vous de le modifier à la fois dans le fichier `/etc/rc.d/init.d/xfs` et ici !

Afin de vous économiser du temps et de l'énergie, je vous recommande d'ajouter le chemin des polices (FontPath) dans les fichiers de configuration XF86Config et XF86Config-4. Si vous n'êtes pas certain de la disponibilité des polices, vous pouvez utiliser cette commande pour le vérifier (avec les droits de root) :

```
chkfontpath --list
```

Les polices suivantes constituent quelques exemples de référence. Assurez-vous de disposer de ces polices avant d'éditer ces chemins.

```
FontPath "/usr/X11R6/lib/X11/fonts/75dpi/"
FontPath "/usr/X11R6/lib/X11/fonts/misc/"
FontPath "/usr/X11R6/lib/X11/fonts/CID/"
FontPath "/usr/X11R6/lib/X11/fonts/Speedo/"
FontPath "/usr/X11R6/lib/X11/fonts/100dpi/"
FontPath "/usr/X11R6/lib/X11/fonts/Type1/"
```

9. (Il *n'est pas nécessaire* d'effectuer cette modification. Vous pouvez laisser les paramètres par défaut, cependant je préfère ce réglage. En cas de doute, laissez-les tels quels). Modifiez cette ligne à la fin du fichier `/etc/inittab` :

   ```
   x:5:respawn:/usr/bin/gdm
   ```

   Si vous décidez de ne pas modifier cette ligne, tant mieux ! Ce n'est pas une étape nécessaire, mais une préférence personnelle !

À présent, vous allez pouvoir effectuer un test.

Un autre point à connaître (qui a été demandé par certains), est la manière d'afficher le message au chargement avec **Willing to manage**. D'après ce que je sais, cette opération est possible dans xdm en ajoutant ce qui suit au fichier `/etc/X11/xdm/xdm-config`.

```
DisplayManager.willing: su noboby -c /etc/X11/xdm/Xwilling
```

Le script Xwilling devant être présent sur votre système.

Pour gdm, ajoutez cette ligne au fichier `/etc/X11/gdm/gdm.conf` dans la section `[security]` :

```
Willing=/etc/X11/gdm/Xwilling
```

Vous trouverez ici un exemple du script Xwilling à titre de référence. La décision d'ajouter ou non ce script vous appartient. Ce n'est pas une étape nécessaire ici !

2.7. Tests

Pour tester si votre XDMCP fonctionnant avec le serveur X est prêt à accepter les connexions, suivez ces étapes. Je trouve qu'il est plus aisé d'utiliser le serveur X et un autre poste pour effectuer les tests.

1. (Re)lancez X (situé dans le niveau d'exécution n°5). Si vous ne savez pas trop comment le faire, redémarrez simplement votre système (ce n'est cependant pas nécessaire si vous savez comment le redémarrer en ligne de commande. C'est toute la beauté de Linux, comparée à Windows).

2. Si vous n'avez pas procédé à la modification des règles de votre pare-feu, il vous faut le désactiver temporairement par le commande **`iptables -F`** (ou **`ipchains -F`**).

3. Vérifiez que l'invite de connexion apparaît. Vérifiez que la résolution d'affichage et que la souris fonctionnent. Connectez-vous depuis la console pour voir si l'accès en local est possible. Si oui, ne vous déconnectez pas.

4. Paramétrez Exceed (ou tout autre logiciel de client graphique (X)) pour soit appeler cette machine (par son adresse IP ou son nom DSN totalement qualifié), soit pour utiliser le paramètre de diffusion de XDMCP (XDMCP-Broadcast) et essayez de vous connecter au serveur X. Vous devriez voir apparaître l'écran de la session X et l'invite de connexion.

3. Transfert X11 à l'aide de SSH

Comme je l'ai expliqué précédemment, utiliser XDMCP pour afficher une interface graphique via Internet est fondamentalement un non-sens, car les données ne sont pas chiffrées lors de leur passage sur Internet. Une des manières de renforcer la sécurité du transfert est de recourir à SSH par appel de X11 dans un tunnel sécurisé ou par transfert de port. SSH (Secure Shell, « interpréteur de commandes sécurisé » a été développé en 1995 par Tatu Ylonen pour remplacer les telnet, ftp, scp, rcp, rlogin, rsh, etc, par nature non sécurisés. La première chose à savoir est que le transfert X11 avec SSH est différent de votre façon habituelle et non sécurisée de faire tourner un fenêtrage X.

Avant de commencer cette configuration, il vous faut des informations complémentaires. Premièrement, il faut que le paquetage SSH soit installé. Dans Linux, il s'agit des paquetages OpenSSH. Vérifiez dans votre distribution les paquetages à installer (certaines l'installent par défaut). Deuxièmement, il vous faut un client SSH Windows (client SSH Windows (des versions pour d'autres systèmes d'exploitation tels que MAC, sont aussi disponibles). Je recommande PuTTY. C'est un merveilleux client SSH libre. Vous pouvez le télécharger de ce lien. N'oubliez pas de télécharger la documentation et de la lire soigneusement. Un autre bon client SSH libre est Tera Term Pro + TTSSH, qui constitue une extension SSH à Tera Term. Celui-ci est un client SSH édité par SSH.com (gratuit pour des utilisations non commerciales). Je vais procéder de nouveau par étapes, de façon à vous permettre de suivre facilement.

1. Ouvrez le programme **putty.exe** en double-cliquant dessus. Cela va lancer l'interface. Premièrement, renseignez les informations de connexion dans le champ “Host Name (or IP address)” avec le nom de l'hôte distant ou son adresse IP et sélectionnez SSH (SSH utilise le port 22). Dans la fenêtre “Category”, trouvez la branche “Connection”. Dans SSH, développez-la et vous verrez la fenêtre “Tunnels”. Cliquez sur “Enable X11 forwarding” (autoriser le transfert de port). Il configurera l'affichage graphique par défaut à `localhost:0`. À présent, retournez à la fenêtre “Session” et sauvegardez cette session sous le nom de votre choix. J'utilise normalement le nom d'hôte pour me rappeler facilement où je désire me connecter.

2. Dans l'exemple d'Exceed, voici comment faire. (Pour les autres clients X, la configuration est analogue). Ouvrez Xconfig de votre répertoire Exceed. Dans votre écran Screen Definition (définition de l'écran), passez le “Window mode” à “Multiple” et sauvegardez-le. Appelez ensuite votre icône “Communication” et définissez le mode “Startup” à “Passive”.

3. C'est terminé. Afin d'effectuer les tests, nous allons d'abord utiliser PuTTY (ou un autre client SSH) pour se connecter sur le serveur. À la première connexion, il vous demandera si vous désirez conserver la clé de sécurité. (“Yes” (oui) est le choix par défaut). Une fois connecté, lancez Exceed. Il demeurera en tâche de fond. Vous pouvez à présent exécuter n'importe quelle application X ; l'application X devrait être transmise à travers SSH à votre écran local. Par exemple :

   ```
   $ xclock &
   ```

Vous devriez voir Xclock tourner sur votre écran local.

Vous constatez à présent la différence : vous ne voyez pas toutes vos fenêtres graphiques. Vous exécutez simplement vos applications une par une et elles sont routées via SSH vers votre écran local. Ce qui fait qu'il vous faut connaître la commande de chaque application à lancer. Tous les contrôles s'effectuent à l'intérieur de la fenêtre du client SSH. Pour moi, la sécurité est plus importante que ce léger inconvénient !

Si vous utilisez X-Win32 et que vous désirez mettre en œuvre SSH et le transfert de port, vous pouvez avoir recours à cette référence pour le configurer.

4. Dépannage

- Si X ne veut pas démarrer et est cassé :

  Si X est cassé et que la connexion échoue, dans la plupart des cas les messages d'erreur suivants s'affichent :

  ```
  _ FontTransSocketUNIXConnect : Can't connect: errno = 111
  failed to set dafault font path 'unix:-1'
  Fatal server error:
  could not open default font 'fixed'
  ```

  Il est probable que xfs ne trouve pas le bon port du serveur de polices ou que le chemin des polices n'est pas configuré correctement. Pour résoudre le problème, vérifier les étapes 1 et 8 ci-dessus. Vérifiez que la configuration pointe vers le port 7100 et assurez-vous que les polices suivantes sont installées (si ce n'est pas le cas, réinstallez les paquetages des polices de Xfree86 à partir de votre cédérom). Vérifiez la liste dans le fichier `XF86Config` (si vous utilisez Xfree86, le fichier est `XF86Config-4`) situé dans le répertoire `/etc/X11` :

  ```
  FontPath "/usr/X11R6/lib/X11/fonts/75dpi/"
  FontPath "/usr/X11R6/lib/X11/fonts/misc/"
  FontPath "/usr/X11R6/lib/X11/fonts/CID/"
  FontPath "/usr/X11R6/lib/X11/fonts/Speedo/"
  FontPath "/usr/X11R6/lib/X11/fonts/100dpi/"
  FontPath "/usr/X11R6/lib/X11/fonts/Type1/"
  ```

  Saisissez en mode ligne de commande **startx** (en local) pour redémarrer le serveur X (ou utilisez la commande **telinit 5** pour définir le niveau d'exécution). Pour redémarrer xfs, utilisez la commande de l'étape 1.

  J'ai constaté que dans la RH 7.3 que si mon xfs n'est pas démarré, la connexion avec Exceed plantera si j'utilise GNOME. (Avec KDE, le fonctionnement est correct et le GNOME de la Mandrake n'est pas affecté). Après avoir corrigé et redémarré xfs, ça marche bien !

- Si Exceed ne répond pas (vous avez un écran blanc) :

  Dans ce cas, il est très probable que xdm (ou gdm, en fonction de celui qui est déclaré dans `/etc/inittab`) ne démarre pas correctement. Essayez la commande : **ps -ef | grep gdm** (ou xdm ou kdm, mettez le bon dans la commande). De plus, si votre système est configuré pour utiliser udp avec XDMCP, vous pouvez saisir **netstat -l | grep xdmcp**. Vous devriez voir ceci :

```
udp 0 0 *:xdmcp *:*
```

Si le processus n’est pas lancé, vérifiez les étapes de la configuration ci-dessus (assurez-vous qu’il n’y a pas de faute de frappe et que le chemin déclaré est correct). Redémarrez X à l’aide de la commande **telinit 5**. Si XDMCP n’est pas configuré pour utiliser udp, suivez l’étape 2 ci-dessus.

Il est aussi possible que la configuration de votre DNS soit incorrecte et/ou que votre pare-feu soit actif. Vous pouvez facilement l’établir en appelant simplement votre hôte par **ping** ou **telnet** ; si la réponse est longue à arriver, c’est que vous avez un problème avec votre DNS. Si avec **telnet** vous recevez en retour un un message « `Connection Refused` », alors c’est que le problème vient du pare-feu (dans la mesure où votre démon telnet est déjà lancé !) Voyez la section située plus haut pour plus d’informations sur la manière de résoudre ce problème.

- Ordinateur de type PC Box avec PPPoE (PPP par Ethernet) :

  Un utilisateur de PPPoE m’a rapporté que si vous utilisez PPPoE, il se peut que vous rencontriez des difficultés avec XDMCP. Après l’avoir désinstallé, il devrait être capable de faire tourner XDMCP. N’ayant pas d’environnement pour effectuer un test, je vous laisse le soin de le tester vous-même.

- Exportation d’affichage de Linux à Linux :

  Si vous utilisez une autre station sous Linux avec X, vous n’aurez pas besoin d’XDMCP pour gérer votre affichage. En fait, vous pouvez exporter l’affichage de votre PC. À cet effet, il vous faut autoriser une autre station à se connecter au serveur X. Sans cela, les messages d’erreur les plus fréquents que vous obtiendrez seront :

  ```
  xlib: Connection refused (error 111): unable to connect to X server
  xlib: No such process (error 3): Server error
  ```

  Pour résoudre le problème, saisissez la commande ci-dessous :

  ```
  $ xhost +
  $ export DISPLAY=adresse_IP_de_votre_machine:0.0
  ```

  Souvenez-vous bien qu’il faut autoriser l’accès par la commande **`xhost -`** une nouvelle fois. Une chose à retenir est que vous n’en avez pas besoin si vous utilisez un PC comme terminal X avec XDMCP. Le besoin existe si vous utilisez une connexion Linux vers Linux ou Linux vers UNIX.

  Si vous utilisez un grand nombre de stations Linux sous X et que vous désirez pouvoir choisir à quel serveur X vous connecter, il vous faudra décommenter ce qui suit dans le fichier `/etc/X11/gdm/gdm.conf` :

  ```
  [daemon]
  Chooser=/usr/bin/gdmchooser --disable-sound --disable-crash-dialog
  ...
  [xdmcp]
  Enable=1
  HonorIndirect=1
  ```

- J'ai un message d'erreur `Signal 11` :

  Le message d'erreur `Signal 11`, nommé également `Segmentation Fault` (Erreur de segmentation), peut parfois avoir pour cause un problème matériel ou logiciel. Si vous rencontrez ce problème en démarrant votre serveur X, il vous faudra régler ce problème avant de configurer XDMCP. Malheureusement, un tel problème n'est pas facile à régler, en raison de nombreuses causes possibles. Pour plus d'informations, rendez-vous sur ce site (en anglais) consacré à l'erreur 11 lors de la compilation du noyau SIG 11 while compiling the Kernel.

5. XDMCP et GDM (le Gestionnaire d'affichage Gnome)

Ce qui suit est tiré du Manuel de référence du Gestionnaire d'Affichage Gnome :

GDM est également compatible avec le protocole de gestionnaire d'affichage X (XDMCP) pour la gestion des affichages distants. GDM écoute le port UDP 177 et répond aux requêtes QUERY (vers un hôte) et aux requêtes BROADCAST (appel général au réseau) en envoyant un paquet WILLING à l'initiateur de la requête. Il est également possible de configurer GDM pour qu'il honore les requêtes indirectes et qu'il présente un écran de choix d'hôtes à l'affichage distant. GDM mémorisera le choix de l'utilisateur et transmettra les requêtes sous-jacentes au gestionnaire retenu. GDM est uniquement compatible avec le système d'authentification MIT-MAGIC-COOKIE-1. Les autres possibilités ont peu de valeur ajoutée, et aucun effort n'a été consacré à leur mise en œuvre. Dans la mesure où il est très facile de lancer une attaque en déni de service contre le service XDMCP, GDM comporte quelques dispositifs pour s'en protéger. Pour plus d'informations, référez vous à la section de référence de XDMCP ci-dessous.

Même si GDM tente de berner les attaquants potentiels, nous vous conseillons cependant de faire en sorte que votre pare-feu bloque le port 177, à moins que vous n'en ayez réellement besoin. GDM protège des attaques en déni de service ; il n'en demeure pas moins que le protocole X est encore non sécurisé par nature, et qu'il devrait être utilisé uniquement dans des environnements protégés. Même si votre affichage est protégé par un dispositif, les événements de X et donc les caractères tapés au clavier lorsque vous saisissez votre mot de passe passeront en clair à travers le réseau. Il est enfantin de les capturer. Il vous faut aussi savoir que les dispositifs de sécurité, s'ils sont placés dans un répertoire monté par NFS, sont susceptible d'être écoutés.

6. Ressources

Quelques références complémentaires sur le sujet :

- Votre page de manuel locale de xdm.
- Votre page de manuel locale de gdm.
- Configuration de XDM
- Configuration du gestionnaire de ressources X (en anglais)
- xdmcp sur udp
- Documentation XDMCP pour quasi-terminaux

- Faut-il mettre en œuvre XDMCP ? (en anglais)
- Terminaux X (en anglais)
- Accéder à des terminaux X à partir de Windows : Cygwin (en anglais)
- Installer et configurer X-Win32
- Apprivoiser le gestionnaire d'affichage X (en anglais)
- Pourquoi recourir au transfert de port ? (en anglais) ; Transfert de port (en anglais) ; SSH : Transfert X11
- Gestionnaire d'affichage GNOME (en anglais)
- aperçu d'un pare-feu basé sur ip-tables en 10 minutes (en anglais) ; Initiation aux commandes iptables (en anglais)
- Comment sécuriser les services de votre système (en anglais) (Debian)
- Guide pratique de configuration du gestionnaire de connexion KDM

7. Auteurs

Auteur actuel : Thomas Chao, Lucent Technologies. <`tomchao CHEZ lucent POINT com`>

8. Traducteurs

Traducteur version française : Denis Berhaut. <`denis POINT berhaut CHEZ free POINT fr`>

Relecteur version française : Éric Madesclair. <`eric TIRET m CHEZ wanadoo POINT fr`>

9. Droits d'utilisation