Gestió Remota

Gestió remota. SSH, comandes de còpies remotes (scp, rsync) i control remot d'escriptoris (VNC, Terminal server, FreeNX).

Eines per a còpies de seguretat.

Autor: Sergi Tur Badenas

Telnet, rlogin i rsh

- **Telnet, rlogin i rsh**
  - Són les aplicacions predecessores de SSH.
  - Les comunicacions amb aquests protocols **NO** viatgen encriptades i poden ser capturades per sniffers com Ethereal.
  - La sintaxi és similar a SSH.
- **Referències**
  - http://en.wikipedia.org/wiki/TELNET
  - http://en.wikipedia.org/wiki/Rlogin
  - http://en.wikipedia.org/wiki/Remote_Shell

Autor: Sergi Tur Badenas

SSH

- **Definició**
  - Secure Shell o SSH és un conjunt d'estàndards i un protocol de xarxa que permet establir un canal segur entre una màquina local i una màquina remota.
- **Característiques**
  - Protocol del nivell d'aplicació.
  - Dos versions del protocol: SSH 1 i SSH 2. SSH es considera obsoleta perquè utilitza mecanismes que actualment ja no són prou segurs.
  - La versió 2 proveïx de mecanismes addicionals de seguretat (encriptació AES, 3DES, Blowfish, CAST128 or Arcfour, etc.)

Autor: Sergi Tur Badenas

SSH

- **Característiques**
  - Els suport per a la versió 2 amb programari lliure està disponible des de 1999 quan OpenBSD va crear OpenSSH per competir amb Secure Shell.
- **Arquitectura SSH (RFC 4251). Capes:**
  - Capa de transport (RFC 4253).
  - Capa d'autenticació d'usuaris (RFC 4252).
  - Capa de connexió (RFC 4254).
- **Referències**
  - OpenBSD
  - OpenSSH

Autor: Sergi Tur Badenas

SSH

- **Utilitats**
  - Per administrar màquines remotes de forma segura, a través d'una terminal o consola.
  - Com a base per altres protocols segurs:
    - SFTP: Alternativa segura de FTP.
    - SCP: Alternativa segura a la còpia de fitxers remots amb rcp.
    - RSYNC: Eina de còpies de seguretat remotes i gestió de mirrors.
  - Per crear túnels segurs per connexions TCP/IP. Alternativa a VPN, securització de X11, etc.
  - Execució de comandes remotes (suport SSH exec).
  - Navegar per Internet de forma segura amb SOCKS o proxies.

Autor: Sergi Tur Badenas

OpenSSH

- **Definició**
  - OpenSSH (Open Secure Shell) és un conjunt d'aplicacions de programari lliure que proveïxen de suport per sessions de comunicacions encriptades basades en el protocol SSH.
  - Alternativa lliure del programari propietari Secure Shell.
- **Programes openssh**
  - **ssh:** reemplaçament dels protocols anàlegs no segurs **rlogin** i **telnet**.
  - **scp:** reemplaçament de la comanda anàloga no segura **rcp**.
  - **sftp:** reemplaçament segur del protocol **ftp**.

Autor: Sergi Tur Badenas

OpenSSH

- **sshd:** servidor/dimoni SSH.
- **ssh-keygen:** una eina per generar parells de clau públiques/privades de tipus RSA o DSA. Utilitzades per l'autenticació d'usuaris i de hosts.
- **ssh-keyscan:** escaneja un servidor SSH per tal d'obtenir la seva clau.
- **ssh-agent:** petit dimoni que permet gestionar les còpies de claus públiques i utilitzar-les per tal d'evitar l'ús de contrasenyes en els reptes d'autenticació.
- **ssh-add:** comanda que afegeix claus al gestor de claus ssh-agent.
- **slogin:** login segur.

Autor: Sergi Tur Badenas

SSH. Instal·lació i execució

- **Instal·lació**

```
$ sudo apt-get install ssh
```

- **Instal·la dos paquets**

```
openssh-client i openssh-server
```

- **Script d'inicialització SystemV**

```
/etc/init.d/ssh
```

- **start|stop|reload|force-reload|restart**

```
$ sudo /etc/init.d/ssh start|stop|reload|status
```

- **OpenSSH a la wiki**

Autor: Sergi Tur Badenas

SSH. Ports i seguretat

- **SSH utilitza el port 22**

```
$ cat /etc/services | grep ssh
ssh             22/tcp          # SSH Remote Login Protocol
ssh             22/udp
```

- **IPTABLES**

```
iptables -A INPUT -s 192.168.1.1/0 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 192.168.1.1/0 -p udp --dport 22 -j ACCEPT
```

```
$ sudo nmap ip_servidor_ssh | grep 22
22/tcp   open  ssh
```

  - El port i altres paràmetres del servidor SSH es poden controlar al fitxer:

```
/etc/ssh/sshd_config
```


Autor: Sergi Tur Badenas

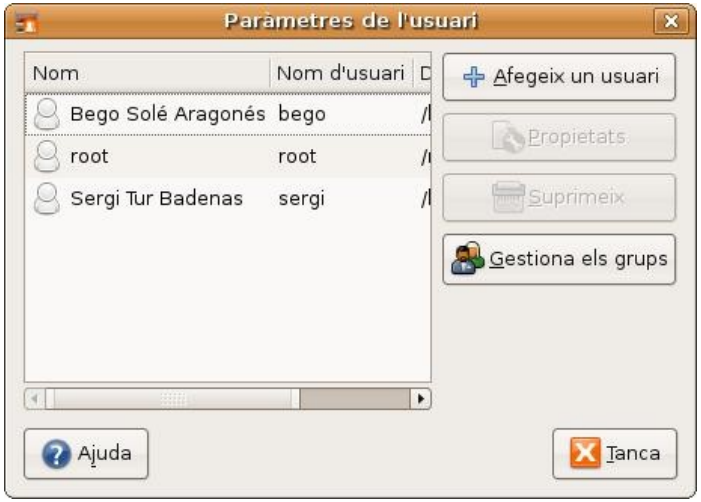
OpenSSH

- **Autenticació**
  - 4 mètodes:
    - Clau d'accés
    - Claus públiques
    - Basat en la màquina de connexió (hostbased)
    - Keyboard-interactive
    - Kerberos/GSSAPI
  - Tots aquests mètodes d'autenticació estan explicats al manual de ssh (**man ssh**).
  - Amb SSH2 amb els valors per defecte l'ordre en que s'intenten els diferents intents d'autenticació és: **hostbased, public key, keyboard-interactive i password.**

Autor: Sergi Tur Badenas

Creació usuaris

- **Exercici. Configuració d'accés remot sense contrasenya.**
  - Treballeu per parelles. Creeu un usuari per al vostre company amb permisos d'administració.
  - Podeu utilitzar la línia de comandes (**adduser**) o l'eina **Usuaris i Grups** del menú Administració de Gnome.



Autor: Sergi Tur Badenas

SSH. Connexió a màquines remotes

- **Segueix un esquema similar al del correu electrònic:**

```
usuari@nom_maquina_remota
    sergi.tur@upc.edu
```

  - Exemple

```
ssh sergi.tur@www.upc.edu
ssh sergi@192.168.1.1
sergi@casa:~$ ssh 192.168.1.1
```

  - Si no posem l'usuari, intenta connectar amb l'usuari que estem utilitzant actualment.
- **Exercici**
  - Proveu de connectar-vos a la màquina remota del company amb les dades de l'usuari que heu creat.

Autor: Sergi Tur Badenas

Autenticació per claus públiques

Generació de claus

```
$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/sergi.tur/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sergi.tur/.ssh/id_dsa.
Your public key has been saved in /home/sergi.tur/.ssh/id_dsa.pub.
The key fingerprint is:
9b:06:0f:d2:6b:15:43:42:84:1a:c2:e1:81:fc:e4:12 sergi.tur@casa
```

```
$ cd ~/.ssh/
$ ls -la
.....................................
-rw-------  1 sergi.tur sergi 1196 2006-07-01
19:31 id_dsa
-rw-r--r--  1 sergi.tur sergi 1116 2006-07-01
19:31 id_dsa.pub
$cat /etc/id_dsa.pub
```

- Amb la opció **-t** es poden generar altres tipus de claus com **rsa**.

Autor: Sergi Tur Badenas

Autenticació per claus públiques

- **Configuració de les claus**

```
$ scp id_dsa.pub sergi.tur@ip_company:~/.ssh
sergi.tur@ip_company's password:
id_dsa.pub                                    100% 1116   1.1KB/s   00:00
$ ssh sergi.tur@ip_company
sergi.tur@ip_company's password:
.....
Last login: Sat Jul  1 09:18:38 2006
......
ip_company$ cd .ssh/
ip_company$ cat id_dsa.pub >> authorized_keys
ip_company$ exit
logout
Connection to ip_company closed.
$ ssh sergi.tur@ip_company
Last login: Sat Jul  1 19:42:02 2006 from .......
.....................
ip_company$
```


Autor: Sergi Tur Badenas

Autenticació per claus públiques

- **Configuracions alternatives**
  - El cas anterior és vàlid en cas d'utilitzar les configuracions, noms i camins de fitxers per defecte.
  - Per configuracions alternatives podem utilitzar el fitxer **~/.ssh/config:**

```
$ cat ~/.ssh/config
Host feina
  Hostname 147.83.98.70
  IdentityFile
~/.ssh/sergitur
  Port 22

Host *
  ForwardX11 yes
```

```
$ ssh feina
connected to feina
feina$
```


Autor: Sergi Tur Badenas

Fitxers de configuració

- **Fitxers de configuració**
  - Per user basis: **~/.ssh/ssh_config**
  - Per host basis: **/etc/ssh/ssh_config**
- **Paràmetres**
  - **ForwardX11.** Activa/desactiva el suport gràfic.
  - **IdentityFile.** Estableix el camí a la clau pública.
  - **Port.** Estableix el número de port.
- **Ajuda**
  - **man ssh_config**

Autor: Sergi Tur Badenas

Exemple Fitxers de configuració

- **Exercici. Accés via SSH a IPCOP**
  - IPCOP utilitza el port no estàndard **222**.
  - Una opció és connectar-se amb el paràmetre -p 222.
  - Creeu una entrada al fitxer de configuració de SSH per al vostre usuari (**~/.ssh/config**) que us permeti entrar a l'IPCOP sense posar usuari ni contrasenya i simplement executant:

```
$ ssh ipcop
```

```
$ cat ~/.ssh/config
Host ipcop
  Hostname ip_del_ipcop
  IdentityFile ~/.ssh/sergitur
  Port 222
```


Autor: Sergi Tur Badenas

Autenticació per màquines

- **Configuració de la màquina remota**
  - Fitxers **/etc/hosts.equiv** o **/etc/ssh/shosts.equiv** (per host basis)
  - Fitxers **~/.rhosts o ~/.shosts** (per user basis)
  - 3 condicions per accedir a la màquina remota:

    1) La IP o nom dns de la màquina que intenta accedir ha d'existir als fitxers indicats.

    2) L'usuari de la màquina que intenta connectar-se ha d'existir a la màquina remota i en cas de configuració basada en usuari ser el mateix.

    3) El servidor ha de poder verificar la clau d'host del client que intenta connectar-se (veieu la secció autenticació d'hosts).
  - Alguns problemes de seguretat com IP o DNS spoofing desaconsellen utilitzar aquest mètode.
  - Tots els exemple d'autenticació s'han fet per **SSH 2.**

Autor: Sergi Tur Badenas

Autenticació de servidors

- **Característiques**
  - SSH manté de forma automàtica una base de dades que conté les identificacions de tots els hosts que s'han utilitzat alguna vegada.
  - El fitxer que emmagatzema aquesta informació és **~/.ssh/known_hosts.**
  - Addicionalment el fitxer **/etc/ssh/ssh_known_hosts** conté la informació dels servidors a nivell de màquina.
  - Evita atacs tipus **man-in-the-midle** que poden utilitzar **trojans** que suplantin a la màquina remota (es desactiva l'autenticació amb contrasenya).

Autor: Sergi Tur Badenas

Autenticació de servidors

- ## Primera connexió a un servidor

```
$ ssh sergi.tur@10.0.2.2
The authenticity of host 'tjener (10.0.2.2)' can't be established.
RSA key fingerprint is ab:37:e2:3f:6f:16:27:5e:9a:02:a1:e1:9a:34:7f:69.
Are you sure you want to continue connecting (yes/no)?yes
password:
```

- ## Man-in-the-middle warning

```
$ ssh sergi.tur@10.0.2.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
f2:92:1d:da:81:2a:d7:16:0a:48:f0:43:20:1c:f4:b5.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending key in ~/.ssh/known_hosts:5
Password authentication is disabled to avoid man-in-the-middle attacks.
X11 forwarding is disabled to avoid man-in-the-middle attacks.
Permission denied (publickey,password,keyboard-interactive).
```

- ## Solució:

```
sed -i '5d' ~/.ssh/known_hosts
```


Autor: Sergi Tur Badenas

Altres comandes ssh. scp

```
dpkg -L openssh-client |grep bin
/usr/bin
/usr/bin/ssh
/usr/bin/scp
/usr/bin/ssh-add
/usr/bin/ssh-agent
/usr/bin/ssh-keygen
/usr/bin/ssh-keyscan
/usr/bin/sftp
/usr/bin/ssh-copy-id
/usr/bin/ssh-argv0
/usr/bin/slogin
```

- **SSH proporciona altres comandes**
  - Possiblement la més important és scp.
  - **scp** és una comanda idèntica a **cp** amb l'única diferència que permet copiar fitxers entre diferents màquines utilitzant el protocol segur SSH.

```
scp Path_fitxer_origen usuari@maquinaremota:Path_fitxer_destinacio

scp usuari@maquinaremota:Path_fitxer_origen Path_fitxer_destinacio
```

```
scp sergi.tur@192.168.1.1:~/fitxer.txt .vmare
```


Autor: Sergi Tur Badenas

DSH

DSH. Distributed Shell

- Permet executar comandes via SSH en grups de màquines al mateix temps.
- Instal·lació:

```
$ sudo apt-get install dsh
```

- Configuració:
  - Nivell usuari: Carpeta **~/.dsh/group/**groupname
  - Nivell màquina: Carpeta **/etc/dsh/group/**groupname
  - Els fitxers d'aquesta carpeta contenen grups de màquines (una per línia).

DSH a la wiki

Autor: Sergi Tur Badenas

DSH

Utilització de DSH

```
$ dsh -r ssh -g aula 'apt-get --yes install joe'
```

- DSH no té cap interacció. És important assegurar-se (utilitzant paràmetres com -- yes) que no hi ha interrupcions a l'executar les comandes.
- Perquè l'automatització sigui real, cal utilitzar autenticació de clau pública per tal d'evitar les contrasenyes a totes les màquines del grup.

```
$ cat /etc/dsh/group/aula
pc01
pc02
pc03
pc04
pc05
pc06
pc07
pc08
pc09
pc10
pc11
pc12
pc13
```


Autor: Sergi Tur Badenas

X11. X Window System

X Window System

- X, X11 o X Window System és un protocol de xarxa i de pantalla que proveeix d'un sistema de finestres (entorn gràfic) a dispositius de mapes de bits.
- Proveeix un sèrie d'eines estàndard per crear aplicacions amb interfície gràfica d'usuari (GUI) en sistemes Unix-like.
- També és suportat per la majoria de sistemes operatius de forma directa (MacOS, OpenVMS) o mitjançant aplicacions extres (Windows).
- Va aparèixer el 1984 al MIT.
- Actualment (des de 2004, abans XFree86) la implementació de referència és la de la Xorg.Foundation

Autor: Sergi Tur Badenas

X11. Arquitectura client-servidor

Arquitectura client/servidor

- **Servidor**: terminal de l'usuari (on s'executa l'entorn gràfic).
- **Clients**: aplicacions (remotes).
- El sistema client-servidor està vist des de la perspectiva de les aplicacions (en comptes de l'usuari). Les aplicacions són clients del servidor X.

Configuració

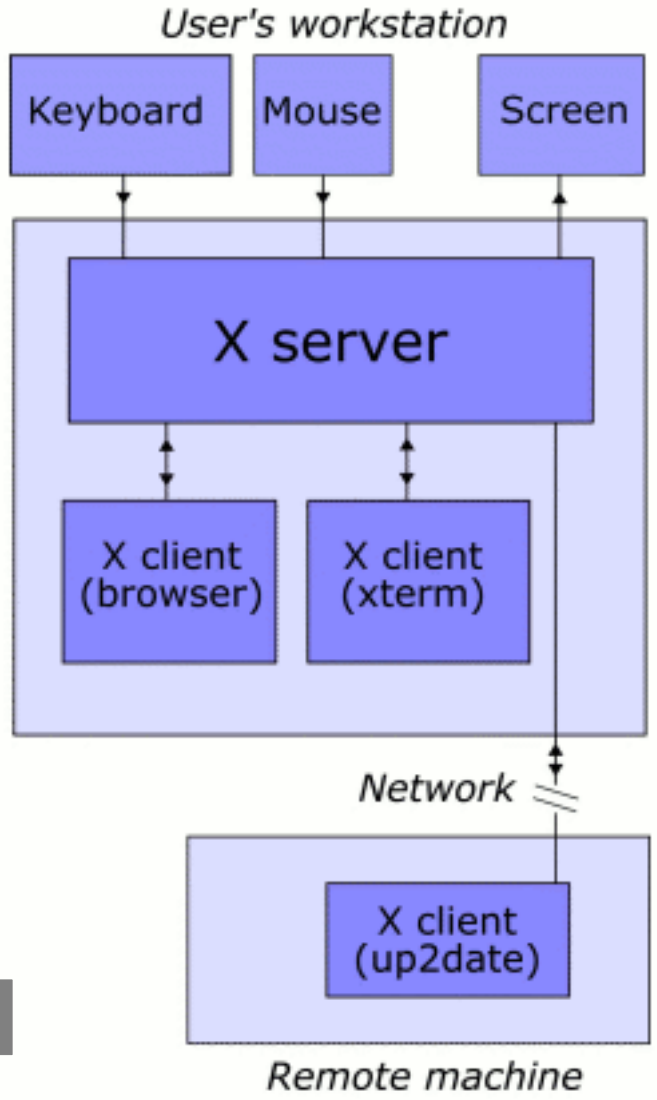
- Variable d'entorn DISPLAY.
- La majoria d'aplicacions X tenen un paràmetre anomenat **-display**.

Autor: Sergi Tur Badenas

X11. Arquitectura client-servidor

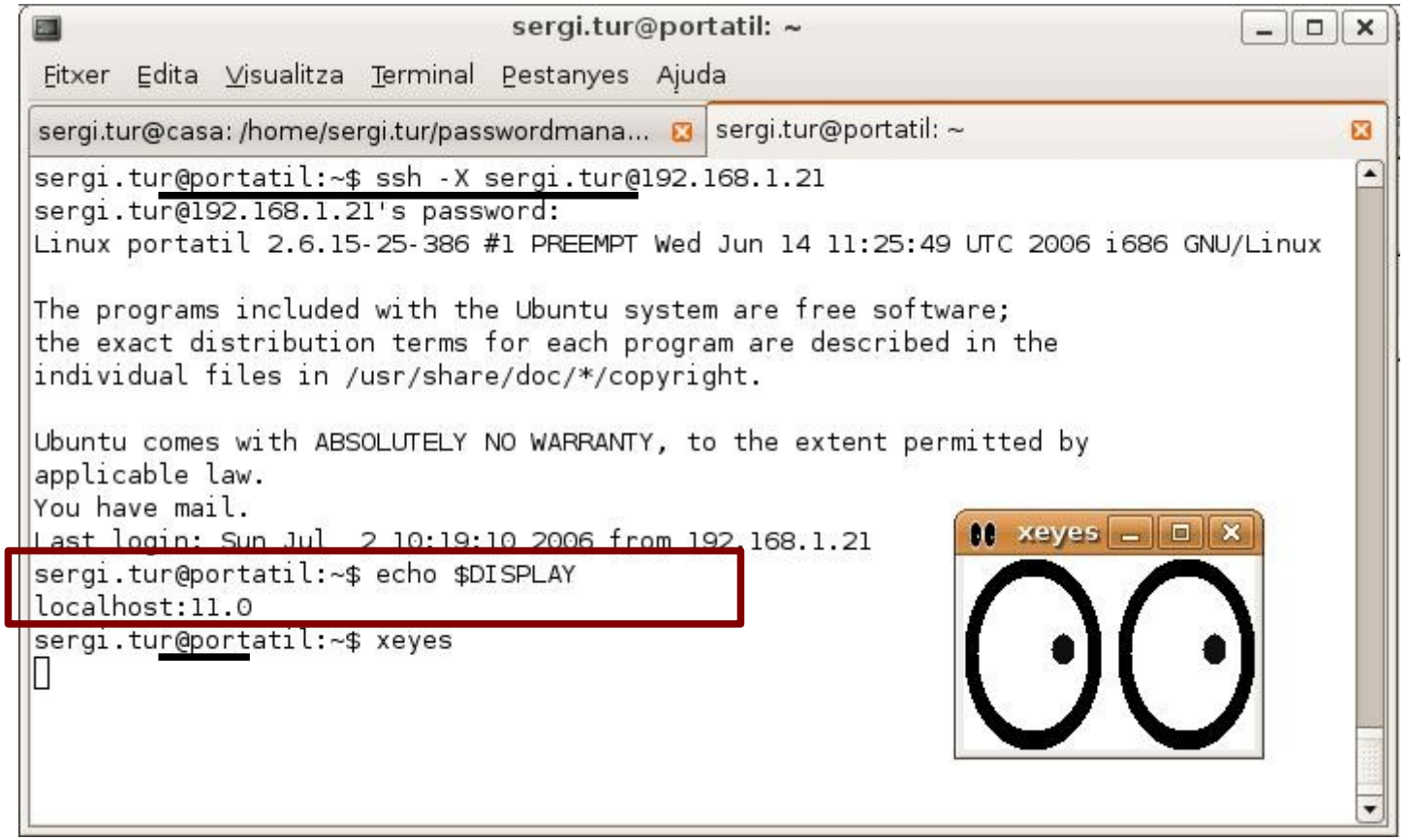
- **El servidor X s'encarrega:**
  - de la interfície amb l'usuari a través de perifèrics d'entrada i sortida:
    - Entrada: Ratolí i Teclat
    - Sortida: Pantalla (Targeta gràfica)
- **Configuració**
  - Fitxer /etc/X11/xorg.conf

```
$ sudo dpkg-reconfigure xserver-xorg
```



Autor: Sergi Tur Badenas

X11 Forwarding



X11 Forwarding

- La variable DISPLAY es canvia per redireccionar la sortida de les X a la màquina local.

Autor: Sergi Tur Badenas

DISPLAY

- El normal és que el servidor X només escolti peticions a través d'un socket local:

```
$ echo $DISPLAY
:0.0
$ sudo netstat | grep X11
unix  3 [ ]     STREAM  CONNECTED  231319   /tmp/.X11-unix/X0
$ ls -l /tmp/.X11-unix/X0
srwxrwxrwx 1 root root 0 2007-01-28 09:10 X0
```

- Amb X11Forwarding, SSH prepara tot el necessari per tal que la nostra màquina sigui el servidor X on s'executaran les aplicacions clients de la màquina remota.

Autor: Sergi Tur Badenas

RSYNC

Característiques

- Rsync és una aplicació per a sistemes UNIX-like que sincronitza fitxers i directoris entre ordinadors.
- Rsync minimitza el tràfic de xarxa utilitzant compressió i copiant només les diferències entre dos “repositoris” a sincronitzar.
- El port que utilitza rsync és 873 (quan funciona com a servidor).
- Rsync pot utilitzar el protocol SSH per tal que les comunicacions durant la sincronització siguin segures.

Autor: Sergi Tur Badenas

RSYNC

Exemple

```
$ rsync -e ssh -cavz ~/docs/ExamensPAAU sergi.tur@192.168.1.21:~/docs
building file list ... done
ExamensPAAU/
ExamensPAAU/Angles/
ExamensPAAU/Angles/pau_angl02j2.zip
.............................
$ rsync -e ssh -cavz ~/docs/ExamensPAAU sergi.tur@192.168.1.21:~/docs
building file list ... done

sent 6611 bytes  received 20 bytes  884.13 bytes/sec
total size is 36465899  speedup is 5499.31
```

- -c (checksum): Controla quins fitxers han canviat.
- -a (archive): Manté els permisos i propietaris del fitxer.
- -v (verbose)
- -z: Comprimeix les dades abans d'enviar-les per la xarxa.

Autor: Sergi Tur Badenas

Controls remot d'escriptoris

Característiques

- Són sistemes que envien els events de teclat i ratolí d'una màquina local a una màquina remota i retornen a la màquina local la sortida visual (entorn d'escriptori).
- Actualment hi ha múltiples aplicacions i protocols de “Desktop Sharing”, per a diferents plataformes o independents de la plataforma, propietaris i lliures, etc.
- Arquitectura client-servidor.

Protocols més importants

- **X11 Forwarding, XDMCP, sistemes X11.**
- **VNC**
- **RDP**
- **NoMachine Technology. FreeNX**
- **LTSP. Utilitzat per terminals tontos**

Autor: Sergi Tur Badenas

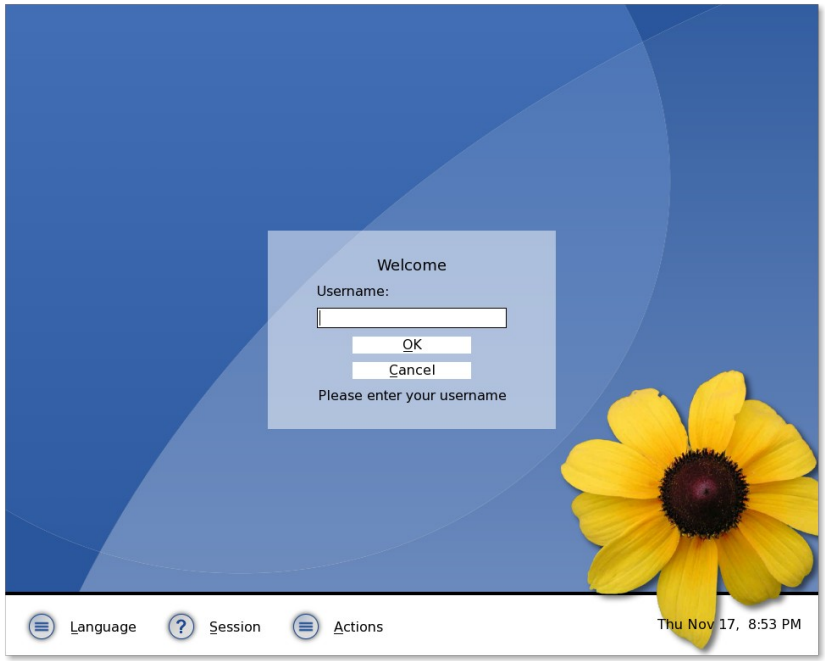
XDMCP

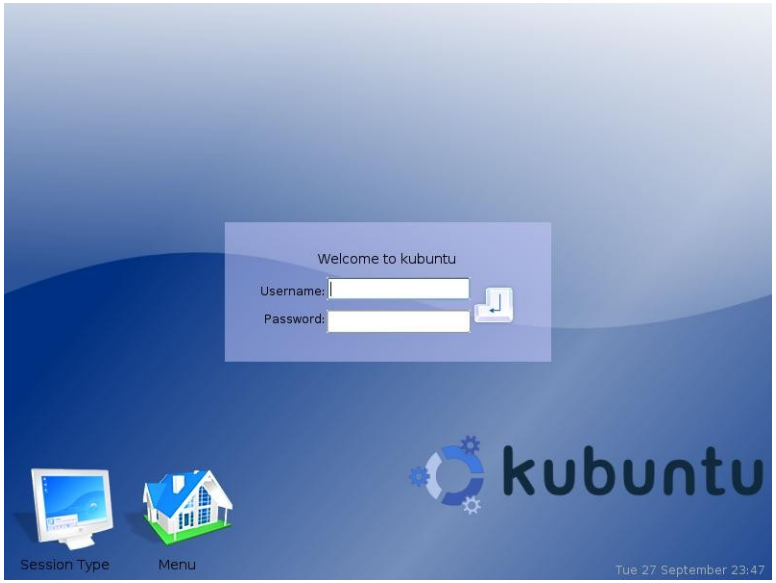
Característiques

- XDM: X Display Manager. Controla les X. Dues opcions:
  - Normals (Xs en local)
  - Màquines remotes: **XDMCP**
- Les comunicacions no són encriptades per tan és un mètode insegur. Per aquesta raó està desactivat per defecte.
- Cada entorn d'escriptori té el seu propi XDM:
  - Gnome: GDM
  - KDE: KDM

Autor: Sergi Tur Badenas

XDMs, KDM, GDM





Autor: Sergi Tur Badenas

VNC

Virtual Network Computing (VNC)

- És un sistema basat en RFB (Remote FrameBuffer).
- VNC és independent de la plataforma i trobem implementacions de clients i servidors per a tots el SO.
- Suporta connexió de múltiples clients alhora.
- El codi font original de VNC és codi obert sota llicència GNU/GPL (GNU General Public License).
- VNC va ser desenvolupat pels laboratoris AT&T.

- **VNC a la wiki**

Autor: Sergi Tur Badenas

VNC

```
$ sudo apt-cache search vnc
krdc - Remote Desktop Connection for KDE
krfb - Desktop Sharing for KDE
libvncauth-dev - Virtual network computing authentication headers
and static lib
libvncauth0 - Virtual network computing authentication library
tsclient - front-end for viewing of remote desktops in GNOME
vino - VNC server for GNOME
vnc-common - Virtual network computing server software
xvncviewer - Virtual network computing client software for X
conspy - Remote control of Linux virtual consoles
directvnc - VNC client using the framebuffer as display
gnome-rdp - Remote Desktop Client for the GNOME Desktop
iprelay - User-space bandwidth shaping TCP proxy daemon
kcemirror - Windows CE remote control tool like VNC
libsvncpp-dev - Subversion C++ library (development files)
libsvncpp0c2a - Subversion C++ shared library
libvncserver-dev - easy API to write one's own VNC server
linuxvnc - VNC server to monitor a tty
rfb - VNC Server for X11 - exports current display
svncviewer - virtual network computing client software for SVGA
tightvncserver - virtual network computing server software
tkvnc - Displays a list of (defined) machines to start VNC to
vnc4-common - Virtual network computing server software
vnc4server - Virtual network computing server software
vncommand - VNC server which monitors a specified program
vncserver - Virtual network computing server software
vncsnapshot - A utility that takes JPEG snapshots from VNC servers
vtgrab - A VNC like console monitoring
x11vnc - VNC server which uses your current X11 session
x2vnc - A dual-screen hack - link a MS-Windows and X display
.......
```

Paquets ubuntu:

- vino
- vnc-common
- xvncviewer
- tsclient

Recomanats:

- krdc
- krfb

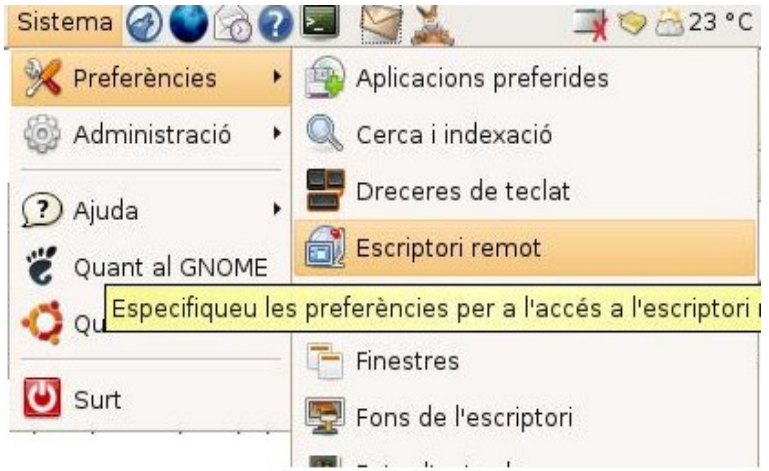
Autor: Sergi Tur Badenas

VNC

tsclient

vino

vino-preferences



Autor: Sergi Tur Badenas

VNC

- **Exercici**
  - Per parelles, permeteu l'accés al vostre escriptori de forma remota amb les preferències de vino. Recordeu reiniciar les X amb la combinació de tecles **Ctrl+Alt+Backspace**.
  - Accediu a l'escriptori remot del vostre company amb l'aplicació **tsclient**.
- **Utilitats**
  - Substituir el projector de transparències o el projector digital del professor.

Autor: Sergi Tur Badenas

RDP

Remote Desktop Protocol (RDP)

- RDP és un protocol multicanal que permet connectar-se a computadores remotes Windows.
- Hi ha clients per a gairebé totes les plataformes.
- Suport 24 bits, encriptació de 128bits, suport àudio remot, impressores, sistema de fitxers.

Inconvenients

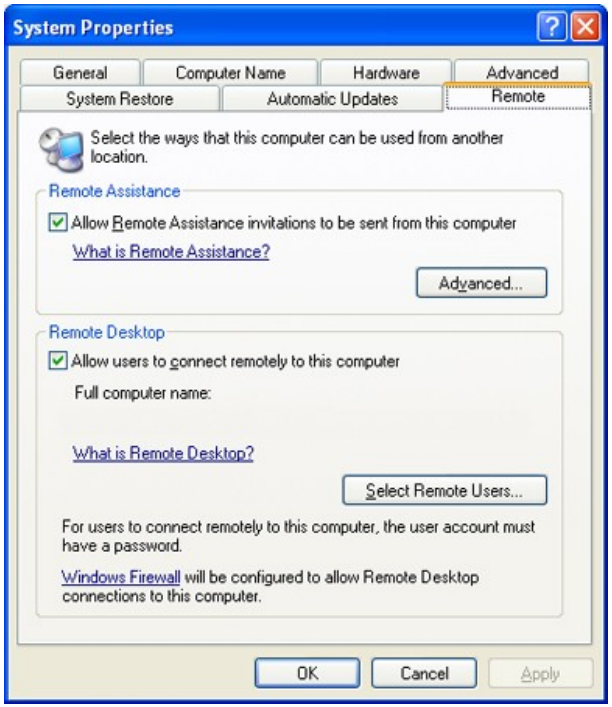
- Només disponibles per Windows XP professional.
- Protocol lent.

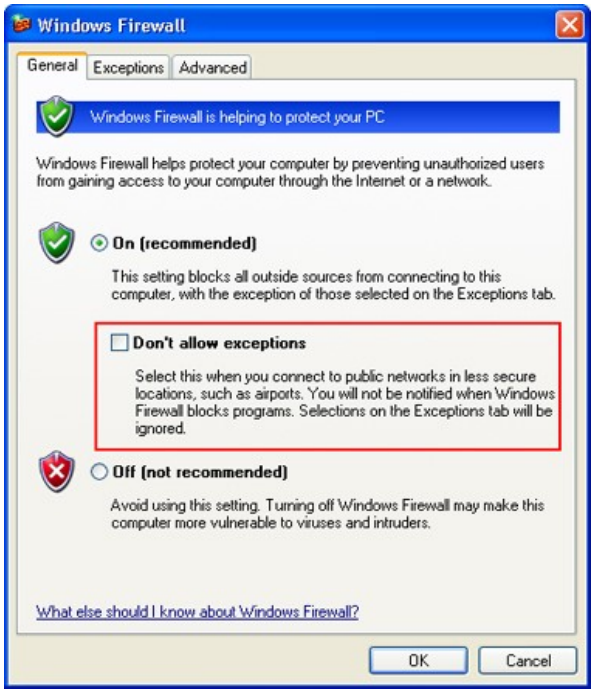
Autor: Sergi Tur Badenas

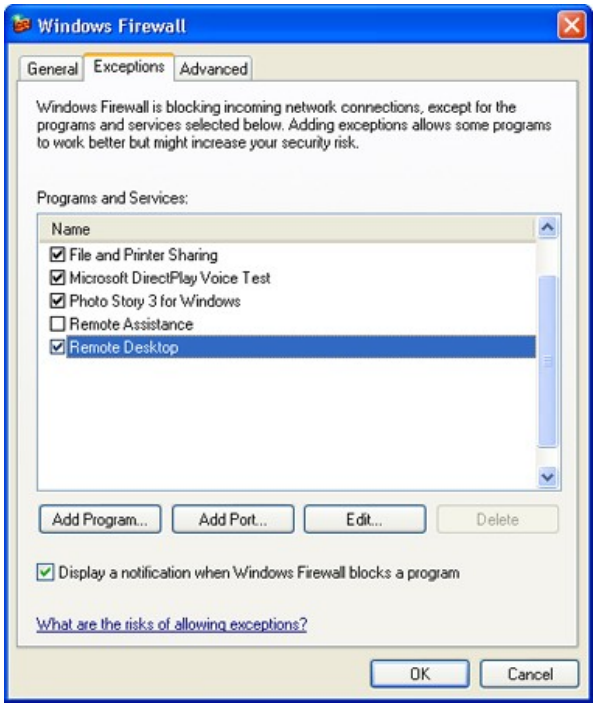
RDP

Configuració Windows XP professional

- Cal habilitar permís per a connexions remotes i configurar el firewall.



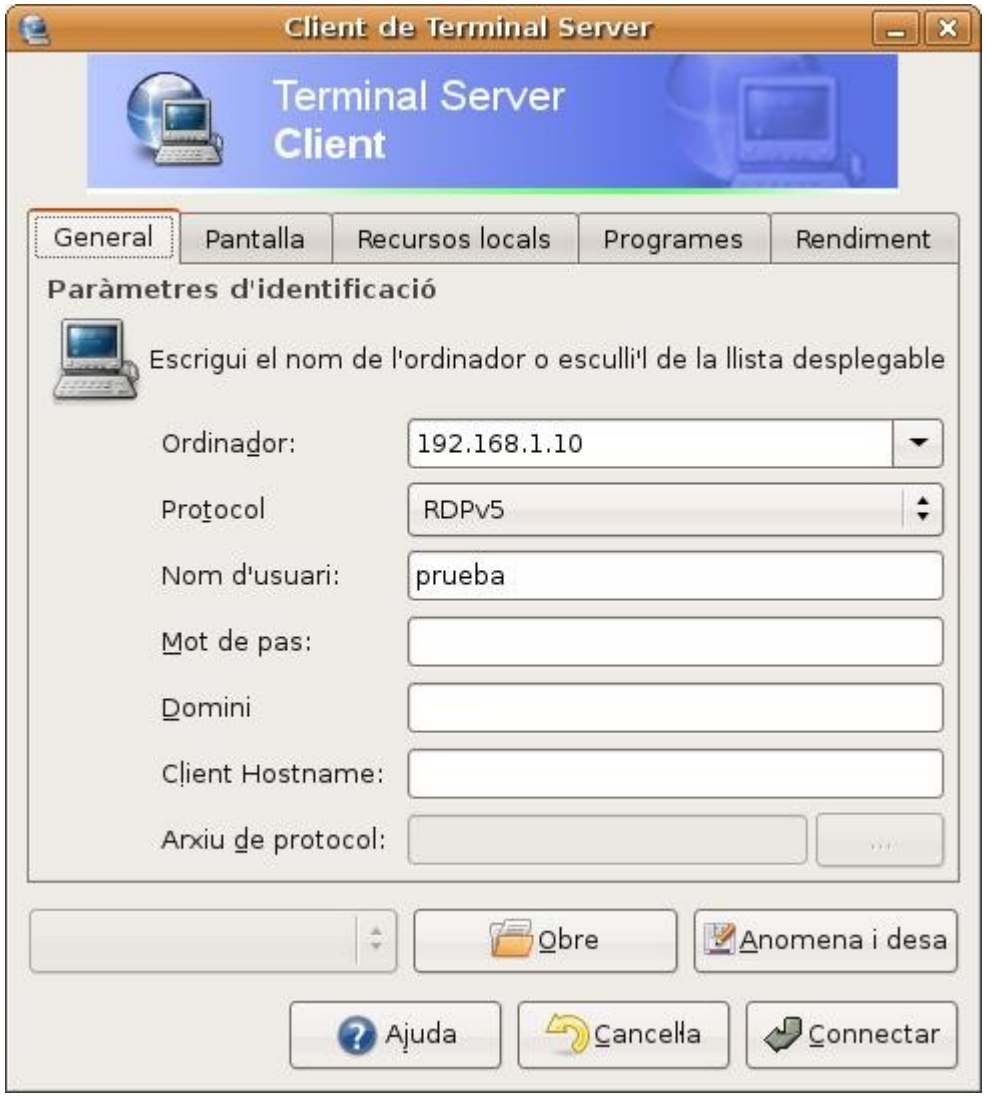




Autor: Sergi Tur Badenas

RDP

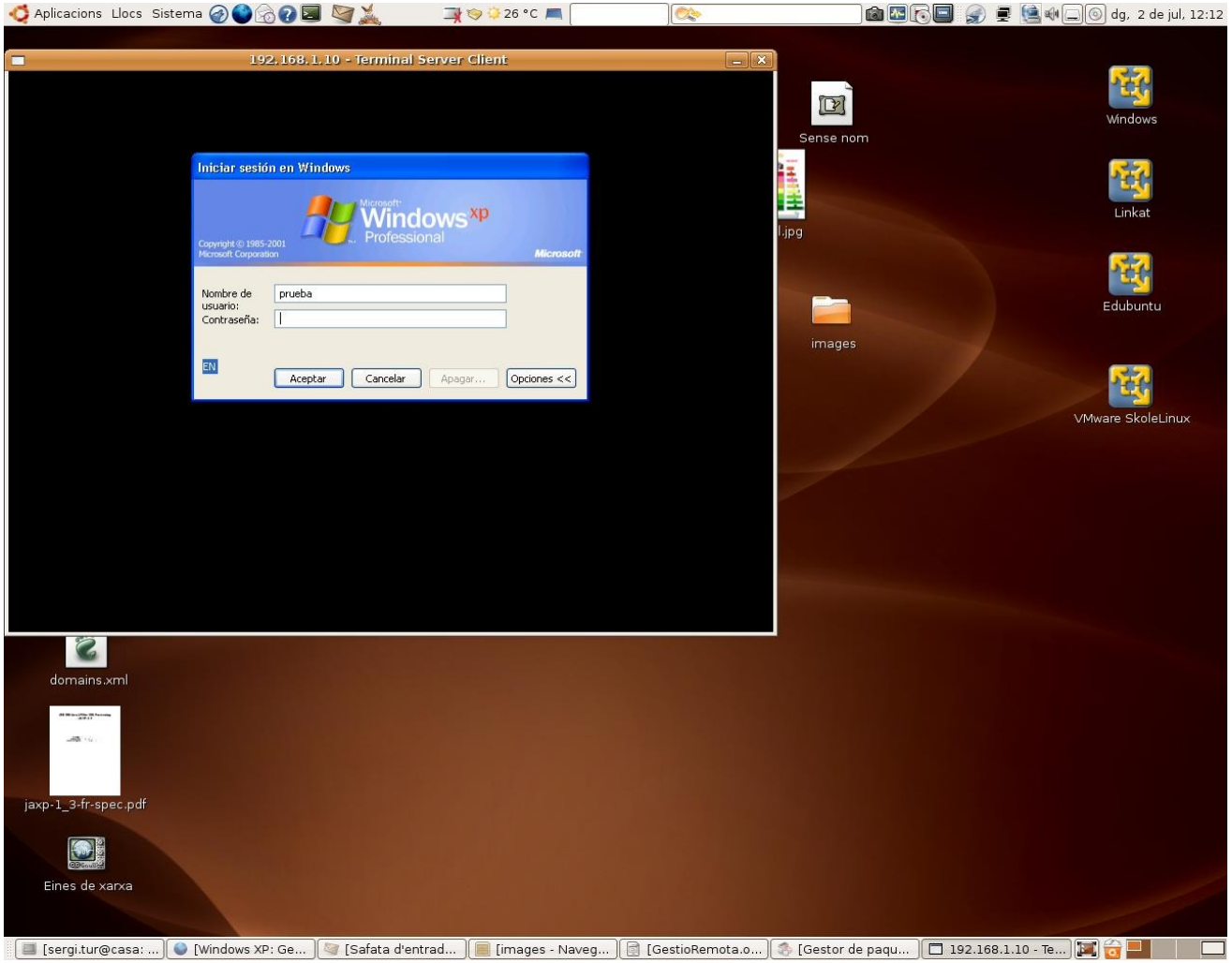
Connexió amb tsclient



Autor: Sergi Tur Badenas

RDP

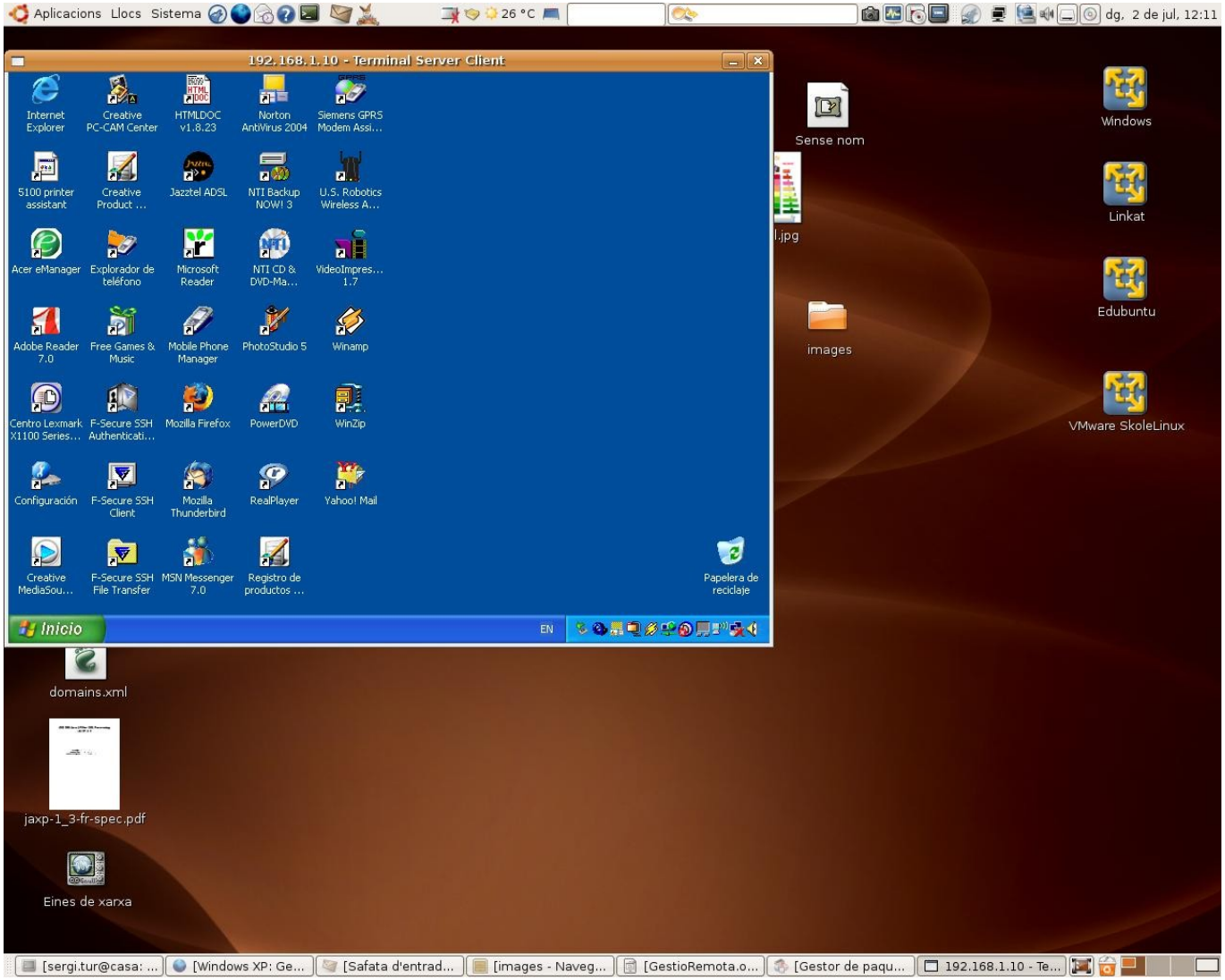
Connexió amb tsclient



Autor: Sergi Tur Badenas

RDP

Connexió amb tsclient



Autor: Sergi Tur Badenas

NoMachine. FreeNX

NoMachine Technologies

- Desenvolupat per la companyia italiana de programari NoMachine.
- Pot fer de túnel per a connexions VNC i RDP.
- Òptim per amples de banda limitats.
- Les llibreries principals de NX han estat alliberades per NoMachine sota llicència GPL.
- FreeNX és una implementació lliure del servidor NX.

Avantatges

- A l'encriptar X11 directament i utilitzar cache té un rendiment molt superior a VNC o RDP.
- Protocol segur. Utilitza SSH com a mode de transport.

Autor: Sergi Tur Badenas

NoMachine. FreeNX

- **Instal·lació**
  - Opció 1. Repositoris de tercers.

```
$sudo joe /etc/apt/sources.list
......
......
#FreeNX
deb http://www.linux.lk/~anuradha/nx/ ./

$sudo apt-get update
$sudo apt-get install nxserver freenx
```

  - Opció 2. Instal·lació des de la web de no machine.
- **Exercici**
  - Seguiu els passos de la wiki dels curs per instal·lar Freenx des de la web de NoMachine

Autor: Sergi Tur Badenas

NoMachine. FreeNX

- **Connexió:**

- **Exercici**
  - Utilitzeu l'assistent per crear una nova connexió al PC d'un company.

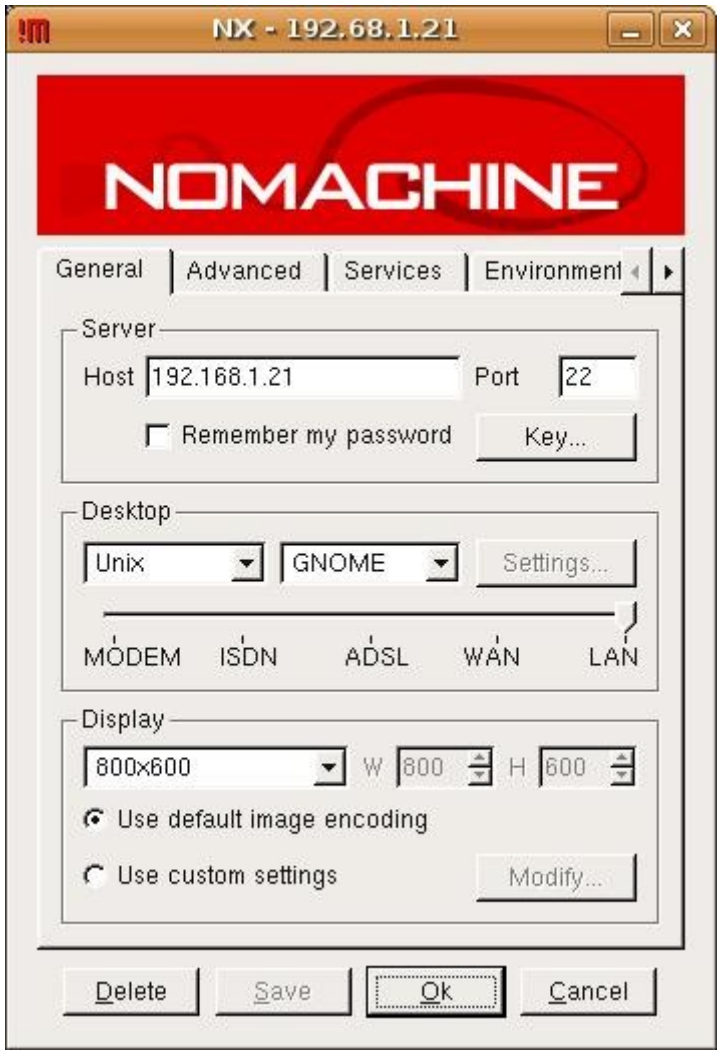
Autor: Sergi Tur Badenas

NoMachine. FreeNX

Connexió:

1)

2)



3)

Autor: Sergi Tur Badenas

NoMachine. FreeNX

Autor: Sergi Tur Badenas

Gestió Remota

Còpies de seguretat.
rdiff, rdiff-backup, rsync, keep...

Autor: Sergi Tur Badenas

RSync

- **Es pot utilitzar per fer còpies de seguretat remotes.**
  - Diferents escenaris exemple:
    - Sincronitzar homes d'usuari entre diverses màquines.
    - Sincronitzar fitxers de còpia de seguretat en màquines remotes.
  - Ben fet pot permetre fins i tot fer còpies incrementals a l'estil de rdiff.
  - L'inconvenient és que la restauració de còpies de seguretat es delega a l'usuari.
- **RSync a la wiki**

Autor: Sergi Tur Badenas

RSync

- **Sincronització de la home d'un usuari entre dues màquines**

```
$ cat /home/usuari/FesVenirFitxers
 #! /bin/sh
 rsync -e ssh -avuz --delete --exclude '.*' --exclude 'Fes*Fitxers' \
usuari@192.168.0.10:/home/usuari /home
```

```
 $ more /home/usuari/Desktop/FesMarxarFitxers
 #! /bin/sh
 rsync -e ssh -avuz --exclude '.*' --exclude 'Fes*Fitxers' /home/usuari \
usuari@192.168.0.10:/home
```

- **Còpies incrementals**
  - Es pot automatitzar per tal de fer còpies incrementals diàries amb cron.

```
rm -rf backup.3
mv backup.2 backup.3
mv backup.1 backup.2
cp -al backup.0 backup.1
rsync -a --delete source_directory/
backup.0/
```


Autor: Sergi Tur Badenas

Rdiff i Rdiff-backup

- **Instal·lació:**

```
$ sudo apt-get install rdiff-backup
```

- **Còpies de seguretat:**
  - Locals

```
$ sudo rdiff-backup carpeta copia
```

  - Remotes

```
$ sudo rdiff-backup local-dir  hostname.net::/remote-dir
```

  - A diferència de Rsync té opcions per automatitzar la restauració.
  - Conjuntament amb SSH (sistema de claus públiques) i cron podem automatitzar les còpies de seguretat en màquines remotes.
  - En aquesta web podeu trobar el pas a pas.

Autor: Sergi Tur Badenas

Keep

- **Eina gràfica basada en rdiff-backup**
  - Permet fer còpies de seguretat incrementals de diferents carpetes (podem tenir “fotos” del nostre sistema en diferents moments).


```
$ sudo apt-get install keep
```

- Permet restaurar per dates les còpies de seguretat.
- Si s'utilitza conjuntament amb particions especials per a les còpies, discs durs o recursos remots pot ser una eina bàsica de còpia de seguretat.

Autor: Sergi Tur Badenas

Keep

Autor: Sergi Tur Badenas

slbackup

- **Sistema de còpies de seguretat d'SkoleLinux**
  - Basat en rdiff-backup.
  - Permet fer còpies incrementals, fotos del sistema, escollir clients i servidors de còpies de seguretat, etc.
  - Disposa d'un modul Webmin.


```
sudo apt-get install slbackup webmin-slbackup
```


Autor: Sergi Tur Badenas

slbackup

- **Fitxer XML de configuració**
  - **/etc/slbackup/slbackup.conf**
- **Integrat a SkoleLinux a través de Webmin**
  - Amb claus SSH podem fer còpies de seguretat de la xarxa SkoleLinux.

```
<client>
    <10.0.2.2>
        address   10.0.2.2
        keep   185
        location   /etc
        location   /var/backups
        location   /root
         location   /boot
        location   /tftpboot
        location   /opt/ltsp/i386/etc
        type   extern
        user   root
    </10.0.2.2>
    <localhost>
        address   localhost
        keep   185
        location   /etc
        location   /home
        location   /var/backups
        location   /boot
        location   /srv/www
        location   /root
        type   local
        user   root
    </localhost>
</client>
server_address   localhost
server_destdir   /var/backup
server_type   local
server_user   root
```


Autor: Sergi Tur Badenas

Llicència Creative Commons

creative commons

COMMONS DEED

Reconeixement-CompartirIgual 2.5

Sou lliure de:

- copiar, distribuir i comunicar públicament l'obra
- fer-ne obres derivades
- fer un ús comercial de l'obra

Amb les condicions següents:

Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador.

Compartir amb la mateixa llicència. Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.

- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.

Els drets derivats d'usos legítims o altres limitacions reconegudes per llei no queden afectats per l'anterior

Això és un resum fàcilment llegible del text legal (la llicència completa).

Advertiment

http://creativecommons.org/licenses/by-sa/2.5/es

Autor: Sergi Tur Badenas