Linux on z/VM Systems Management

Rob van der Heij
IBM Netherlands

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

BookManager*	IBM*	Parallel Sysplex*	VM/ESA*
DB2*	IBM logo*	PR/SM	VSE/ESA
DFSMS/MVS*	Language Environment*	QMF	VTAM*
DFSMS/VM*	Multiprise*	RACF*	z/Architecture
e-business logo*	MVS	RAMAC*	z/OS
Enterprise Storage Server	NetRexx	S/390*	z/VM
ESCON*	OpenEdition*	S/390 Parallel Enterprise Server	zSeries
FICON	OpenExtensions	VisualAge*	
GDDM*	OS/390*	VisualGen*	

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation; LINUX is a registered trademark of Linus Torvalds; Penguin (Tux) compliments of Larry Ewing; Tivoli is a trademark of Tivoli Systems Inc.; Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries; UNIX is a registered trademark of The Open Group in the United States and other countries; Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation; SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC. * All other products may be trademarks or registered trademarks of their respective companies.

Notes: Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions. This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Contents

Things you need to run a lot of Linux virtual machines on z/VM

- Linux Installation
- Automated Installs and Cloning
- Software Management
- Systems Programmer Management
  - SSH - Secure Shell
  - Using sudo

Enterprise (Systems Management)

versus

(Enterprise Systems) Management

SuSE QuickStart Disk

Introduction

- Linux for S/390 is normally installed over the network
  - IPL from virtual reader
  - Load packages from FTP or NFS server
- Network install is relatively expensive
  - Uses resources in virtual routers
  - Consumes bandwidth
  - Requires network access to an FTP or NFS server
  - Often it takes too long to wait for
- QuickStart Disk is like a virtual CD
  - Linked R/O by the virtual machine
  - Can be IPLed to get a ramdisk system
  - Holds a copy of the RPM binaries packages

Not for SLES 8

SuSE QuickStart Disk

Logging on the virtual machine

- Read Only link to virtual CD in the directory
- Override IPL statement from directory during first logon
- More virtual storage for ramdisk IPL

```
L GWA8083F IPL 1CD STORAGE 96M
ENTER PASSWORD  (IT WILL NOT APPEAR WHEN TYPED):

z/VM Version 4 Release 2.0, Service Level 0000 (64-bit),
built on IBM Virtualization Technology
There is no logmsg data
FILES: 0002 RDR,   NO PRT,   NO PUN
LOGON AT 09:52:49 DST SUNDAY 06/02/02
hwc low level driver: can write messages
hwc low level driver: can not read state change notifications
hwc low level driver: can read commands
hwc low level driver: can read priority commands
Linux version 2.4.7-SuSE-SMP (root@s390vm11) (gcc version 2.95.3 20010315 (SuSE)
) #1 SMP Tue Oct 30 23:24:09 GMT 2001
```

SuSE QuickStart Disk

Load the dasd driver

```
SuSE Instsys linux390:/root # insmod dasd dasd=200-207,1cd
Using /lib/modules/2.4.7-SuSE-SMP/kernel/drivers/s390/block/dasd.o

SuSE Instsys linux390:/root # cat /proc/dasd/devices
0200(FBA ) at ( 94:  0) is dasda:active at blocksize: 512, 50000 blocks, 24 MB
0201(ECKD) at ( 94:  4) is dasdb:active at blocksize: 4096, 72000 blocks, 281 MB
0202(ECKD) at ( 94:  8) is dasdc:active at blocksize: 4096, 180000 blocks, 703 MB
0203(ECKD) at ( 94: 12) is dasdd:active at blocksize: 4096, 180000 blocks, 703 MB
0204(none) at ( 94: 16) is dasde:unknown
0205(none) at ( 94: 20) is dasdf:unknown
0206(none) at ( 94: 24) is dasdg:unknown
0207(none) at ( 94: 28) is dasdh:unknown
01cd(ECKD) at ( 94: 32) is dasdi:active at blocksize: 4096, 450000 blocks, 1757 MB

SuSE Instsys linux390:/root # cat /proc/partitions
major minor  #blocks  name

....
  94    12     720000 dasdd
  94    13     719904 dasdd1
  94    32    1800000 dasdi
  94    33    1728000 dasdi1
  94    34      71904 dasdi2
```

two partitions

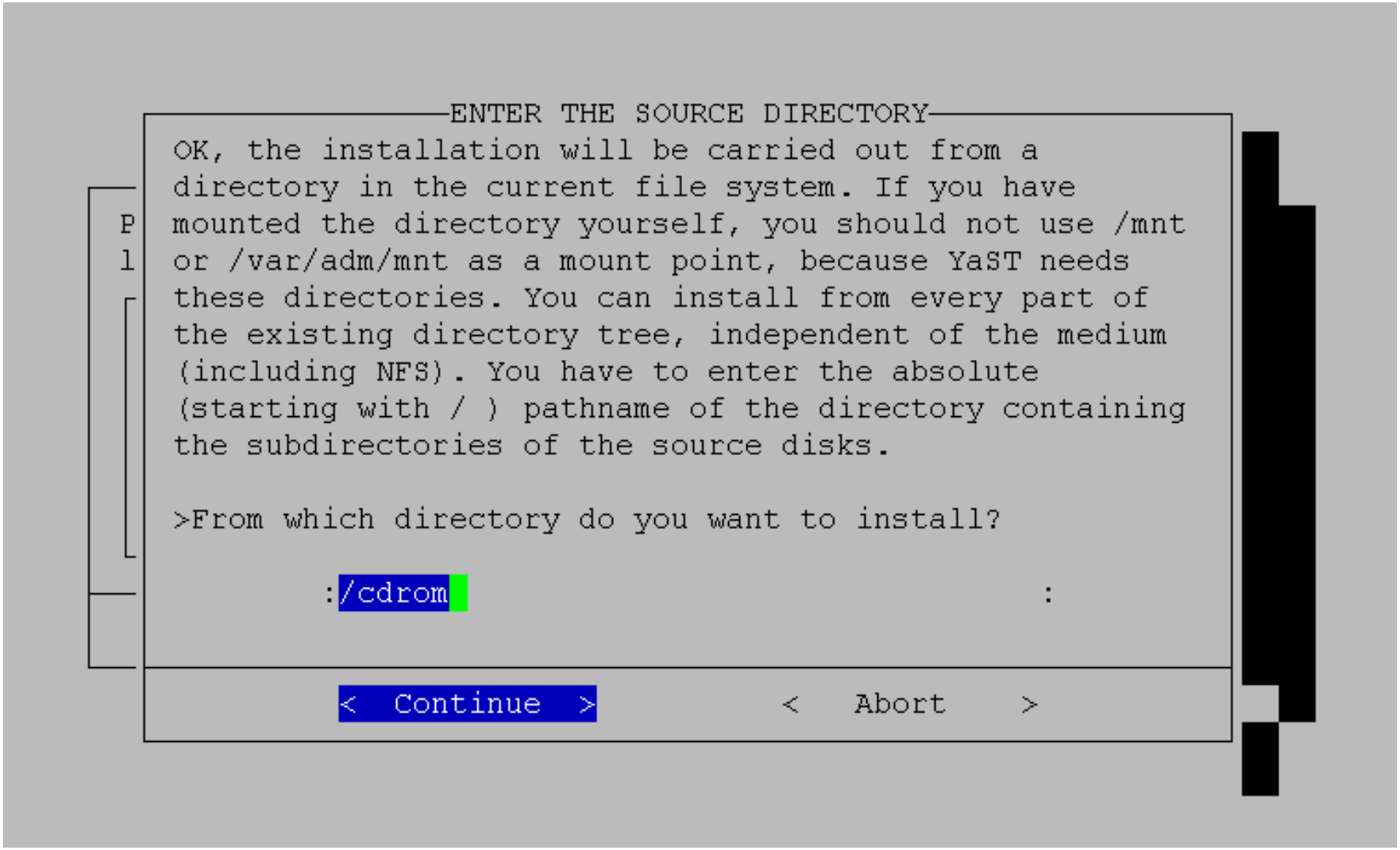
SuSE QuickStart Disk

Access the virtual CD

```
SuSE Instsys linux390:/root # ln /dev/dasdi1 /dev/cdrom
SuSE Instsys linux390:/root # ls -l /dev/cdrom
brw-rw-r--    2 root     disk      94,   33 Oct 30  2001 /dev/cdrom
SuSE Instsys linux390:/root # ls -l /dev/dasdi1
brw-rw-r--    2 root     disk      94,   33 Oct 30  2001 /dev/dasdi1

SuSE Instsys linux390:/root # mkdir /cdrom
SuSE Instsys linux390:/root # cat /etc/fstab
/dev/cdrom      /cdrom          ext2    ro,noauto       0 0
SuSE Instsys linux390:/root # mount /cdrom
SuSE Instsys linux390:/root # df
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/root                26294     23309      1664  94% /
/dev/cdrom             1700792   1577116     37276  98% /cdrom
```

SuSE QuickStart Disk



SuSE QuickStart Disk

- Installation continues like any other installation
  - Typically much faster than with FTP or NFS installs
  - No resources used by virtual routers etc
- Some repair work needed after reboot of Linux
  - Include the virtual CD in the kernel command line again
  - Add the /cdrom entry to /etc/fstab
- YaST will use the installation medium for extra packages
- Manual steps can be automated by changes in the initrd
- All Linux images have access to the virtual CD
  - Very easy access to packages that were not yet installed
  - Not possible to update the virtual CD afterwards

Automated Installs and Cloning

- Manual installation is not attractive for a large number of Linux images
  - time consuming and waste of resources
  - error prone
- There is a need for automated installs

Typical Linux for S/390 installation:

- IPL with ramdisk system and get network connection
- Format the disks and create filesystems etc
- Install selected packages with RPM
- Modify some of the configuration files for this system

Automated Installs and Cloning

Red Hat - Kickstart

- Automated install for Red Hat Linux
- Configuration file with all answers to install questions
- Creates a unique boot floppy (or boot via network)
- Mainly aimed at Intel installations
- For S/390 installs the loader program takes answers from the parm file
- Could punch the files and then autolog the guest
- The installer needs a lot of work to use the virtual CD

`http://www.redhat.com/docs/manuals/linux/RHL-7.2-Manual/custom-guide/`

Automated Installs and Cloning

SuSE - ALICE

- Automated Linux Installation and Configuration Environment
- On request of T-Online and made available in Open Source
- Very specific for Intel installations
- Duplicates most of the function in YaST
- Unique boot floppy, loading packages via network
- Unique boot CD, including the packages
- Lacks most of the zSeries specific things

Automated Installs and Cloning

Installing systems through "third party" install

- Linux 2.4.7 can dynamically link and detach minidisks
- A Linux virtual machine can prepare the disks for the new image
  - prepare filesystem
  - link to target minidisk in R/W
  - mount the device
  - install packages (using rpm --root)
  - apply configuration changes
  - detach the minidisk
  - have someone autolog the new Linux image

Automated Installs and Cloning

Applying the Configuration Changes

- Process described in the ISP/ASP Redbook
- When systems are similar enough you can compare them
  - Often you can help make the systems very similar
- Perform a manual install of two systems
- Do not reboot, but mount filesystems in another image
  - Run md5sum against files in both systems and compare
  - Study the list of files and take out the 'wrong' files
    - backup files from YaST
    - work files from RPM and YaST

Automated Installs and Cloning

- Run `diff` to compare the versions of the file

```
--- disk2/etc/rc.config Mon Apr 29 08:12:55 2002
+++ disk3/etc/rc.config Fri May 10 00:11:55 2002
@@ -152,7 +152,7 @@
 #
 # IP Adresses
 #
-IPADDR_0="192.168.8.2"
+IPADDR_0="192.168.8.3"
 IPADDR_1=""
 IPADDR_2=""
 IPADDR_3=""
@@ -171,7 +171,7 @@
 # Sample entry for ethernet:
 # IFCONFIG_0="192.168.81.38 broadcast 192.168.81.63 netmask 255.255.255.224"
 #
-IFCONFIG_0="192.168.8.2 pointopoint 192.168.8.1 mtu 1500 up"
+IFCONFIG_0="192.168.8.3 pointopoint 192.168.8.1 mtu 1500 up"
 IFCONFIG_1=""
 IFCONFIG_2=""
 IFCONFIG_3=""
```

Automated Installs and Cloning

- Make the differences between files generic

```
--- disk2/etc/rc.config Mon Apr 29 08:12:55 2002
+++ disk3/etc/rc.config Fri May 10 00:11:55 2002
@@ -152,7 +152,7 @@
 #
 # IP Adresses
 #
-IPADDR_0="192.168.8.2"
+IPADDR_0=":ipaddr:"
 IPADDR_1=""
 IPADDR_2=""
 IPADDR_3=""
@@ -171,7 +171,7 @@
 # Sample entry for ethernet:
 # IFCONFIG_0="192.168.81.38 broadcast 192.168.81.63 netmask 255.255.255.224"
 #
-IFCONFIG_0="192.168.8.2 pointopoint 192.168.8.1 mtu 1500 up"
+IFCONFIG_0=":ipaddr: pointopoint :gateway: mtu 1500 up"
 IFCONFIG_1=""
 IFCONFIG_2=""
 IFCONFIG_3=""
```

Automated Installs and Cloning

- Run **patch** to apply the changes
- Patch can be applied to pure copies of first image
  - Copy from installed system instead of format
- When copies are made in advance, creation of a new Linux images takes a few seconds
- Will get more complicated when systems are less equal

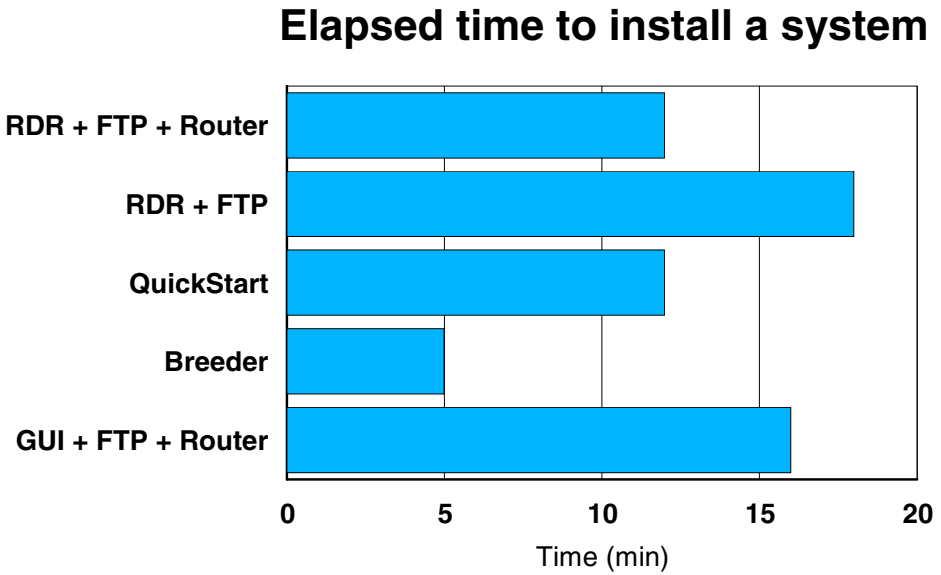
```
cat /mnt/one.patch | \
   sed "s/:hostname:/$uid/g" | \
   sed "s/:ipaddr:/$ipa/g" | \
   sed "s/:gateway:/194.255.207.1/g" | \
   sed "s/:tunnel:/$tun/g" | \
   (cd /mnt/disknew ; patch -p1)
```

Automated Installs and Cloning

- Automated installation can be done much quicker
- Measurements shown are for a minimal install

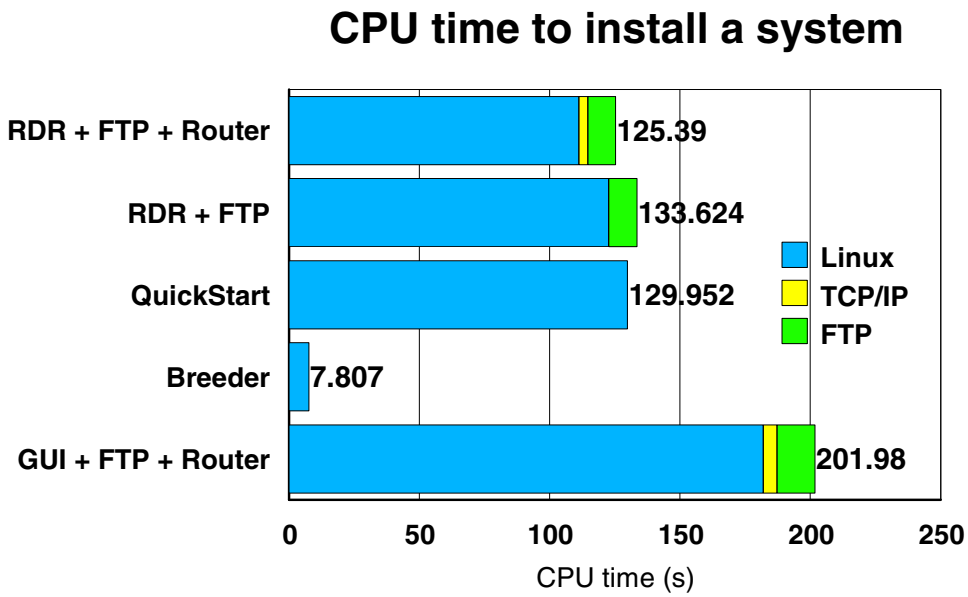
- Breeder is a home grown "cloning" approach
  - copy a pre-installed system
  - apply configuration changes

- CLONEDISK support in DirMaint - VM63122



Automated Installs and Cloning

- Savings in CPU time are considerable
- Resources used for install can not be used to run the business
- Third party install allows systems to be configured to run the application rather than the installer
  - Virtual machine size
  - Network connectivity
  - Allocated capacity
  - Installed packages



Automated Installs and Cloning

- Process works when systems are similar enough
  - It can be used to get a common base system
- Biggest savings are by not installing software
  - Resources for installation
  - Disk space (and backup)
  - Need for maintenance
  - Security and System Administration
- PC approach with dedicated hardware: install everything

Automated Installs and Cloning

- Installing additional packages must be easy
- Additional packages can be installed from R/O linked minidisk
  - Can not be updated afterwards so hard to stay current
- Need for hierarchy in the RPM repository
  - Provide different sets of packages for various customers
  - Different levels of stability (e.g. test versions)
  - Service Levels may be different
- YaST is rather restrictive, so manual RPM installs needed
  - Uses control files in proprietary format
- Additional installs often require a lot of extra packages
  - Sometimes hard to find the missing packages (rpmfind.net)
  - Pre-required packages cause incompatibility

APT - Advanced Packaging Tool

- APT is the package manager for Debian distributions
- Debian uses .deb packages rather than rpm
- Conectiva made the apt-rpm port to work with rpm's

Features provided by apt-rpm:

- automatically resolve dependencies
- hierarchy in the respository
- concept of local and remote repositories
- upgrade process

`https://moin.conectiva.com.br/AptRpm`

APT-RPM

Server Side Installation

- Rebuild and install apt port from Conectiva
- An apt-rpm repository can be made out of symlinks to the binary rpm's in a copy of SuSE or Red Hat distribution
- Generate dependency index for the repository
  - The apt index can be stored on the virtual CD as well
- Multiple repositories can be used to keep different categories
  - Different type of access to repositories (e.g. CD, FTP, NFS)
  - Useful to separate add-on's from original distribution
  - No need to update the virtual CD to provide upgraded packages
- Clients can use multiple repositories
  - Use local (partial) replica repositories
  - Include repositories with early versions or specific customization
- During installation of a package apt will pick the 'best' version

APT-RPM

Client Side Installation

- Install apt and libapt packages
- Prepare sources.list

```
linux008:~ # cat /etc/apt/sources.list
# See sources.list(5) for more information, especialy
# Remember that you can only use http, ftp or file URIs
# CDROMs are managed through the apt-cdrom tool.

rpm     file:/cdrom/apt/SuSE-7.2 suse os
rpm     ftp://emealinux.ehone.ibm.com/apt/SuSE-7.2 suse t4vm
```

base set of packages from virtual CD

additional packages via anonymous ftp

APT-RPM

Client Side Installation

- Run **`apt-get update`** to build a cache of the index

```
linux008:~ # cp sources.list /etc/apt/sources.list
linux008:~ # apt-get update
Ign file: suse release.os
Get:1 ftp://emealinux.ehone.ibm.com suse/base/pkglist.t4vm [8640B]
Get:2 ftp://emealinux.ehone.ibm.com suse release.t4vm
Ign ftp://emealinux.ehone.ibm.com suse release.t4vm
Fetched 8640B in 12s (697B/s)
Processing File Dependencies... Done
Reading Package Lists... Done
Building Dependency Tree... Done
file:/cdrom/apt/SuSE-7.2/ will not be authenticated.
ftp://emealinux.ehone.ibm.com/apt/SuSE-7.2/ will not be authenticated.
```

APT-RPM

Client Side Installation

- Run **`apt-get -f install`** to fix any unresolved dependencies

```
linux000:~ # apt-get -f install
Reading Package Lists... Done
Building Dependency Tree... Done
Correcting dependencies... Done
The following packages will be REMOVED:
  yast2 yast2-config-cups yast2-config-environment yast2-config-hwinfo
  yast2-config-inet yast2-config-lvm_config yast2-config-network
  yast2-config-online-update yast2-config-package-manager yast2-config-printer
  yast2-config-rcconfig yast2-config-security yast2-config-update
  yast2-config-users yast2-db-printer yast2-lib-printer yast2-menu
  yast2-module-support yast2-trans-cups yast2-trans-hwinfo
  yast2-trans-libprinter yast2-trans-network yast2-trans-online-update
  yast2-trans-package-manager yast2-trans-printer yast2-trans-security
0 packages upgraded, 0 newly installed, 26 to remove and 3 not upgraded.
Need to get 0B of archives. After unpacking 11.6MB will be freed.
Do you want to continue? [Y/n]
```

APT-RPM

Client Side Installation

- Run **`apt-get -f upgrade`** to pick up new versions

```
linux000:~ # apt-get upgrade
Reading Package Lists... Done
Building Dependency Tree... Done
3 packages upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 2111kB of archives. After unpacking 3022kB will be freed.
Do you want to continue? [Y/n] y
Get:1 ftp://emealinux.ehone.ibm.com suse/t4vm aaa_base 2001.10.19-4.t4vm [274kB]
Get:2 ftp://emealinux.ehone.ibm.com suse/t4vm k_deflt 2.4.7-31.t4vm.2 [1753kB]
Get:3 ftp://emealinux.ehone.ibm.com suse/t4vm s390-tools 0.5-45.c [83.5kB]
Fetched 2111kB in 26s (81.0kB/s)
Executing RPM (-Uv)...
aaa_base                    ##################################################
Updating etc/rc.config...
k_deflt                     ##################################################
s390-tools                  ##################################################
linux000:~ #
```

APT-RPM

Sample Package Installation

- Installation via **`apt-get install`**
  - Use the **`-s`** or **`-S`** option to review what will happen
- Dependencies will be resolved automatically

```
linux008:/var/cache/apt # apt-get install vmlinx
Processing File Dependencies... Done
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  cpint
The following NEW packages will be installed:
  cpint vmlinx
0 packages upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 0B/19.1kB of archives. After unpacking 42.4kB will be used.
Do you want to continue? [Y/n]
```

APT-RPM

- An easy way to install additional packages and apply upgrades
- Encourage customers to install only what they need
  - No resources wasted
  - Less exposure through backlevel software
- Options for automated upgrades
  - Manage your own repositories
  - Schedule apt-get upgrade to run off-shift

- Many more options:
  `http://www.rpm.org/software/updaters/`

IP Configuration - the easy way

- DHCP - Dynamic Host Configuration Protocol
  - Normally used to configure (mobile) IP clients
  - Pass client a free address from the pool (less IP addresses needed)
- Can also be used to configure servers
  - IP address taken from a table rather than random
  - Can use a long lease for DHCP
- Uses Broadcast capability of Guest LAN
- MAC address defined in CP directory

```
USER LINUX31 XXXXXXXX 64M 512M G
 INCLUDE RMHTUX
 NICDEF 0410 TYPE QDIO LAN SYSTEM LAN1 MACID 00201f
 MDISK 201 3390 1001  125 LX3L03  MR READ    WRITE
*
USER LINUX32 XXXXXXXX 64M 512M G
 INCLUDE RMHTUX
 NICDEF 0410 TYPE QDIO LAN SYSTEM LAN1 MACID 002020
 MDISK 201 3390 1251  125 LX3L03  MR READ    WRITE
```

IP Configuration - the easy way

- MAC address linked to IP address through dhcpd.conf
- DNS to map host name to IP address

dhcpd.conf

```
host linux30 { hardware ethernet 02:00:00:00:20:1e; fixed-address linux30; }
host linux31 { hardware ethernet 02:00:00:00:20:1f; fixed-address linux31; }
host linux32 { hardware ethernet 02:00:00:00:20:20; fixed-address linux32; }
```

DNS zone

```
linux30          IN A            192.168.36.30
linux31          IN A            192.168.36.31
linux32          IN A            192.168.36.32
```

```
Mar 29 14:25:54 vmlinux3.itso.ibm.com OPERATOR 07:25:54 AUTO LOGON  ***       LINUX31  USERS = 217   BY RVDHEIJ
Mar 29 14:26:17 linuxgw dhcpd: DHCPDISCOVER from 02:00:00:00:20:1f via eth1
Mar 29 14:26:17 linuxgw dhcpd: DHCPOFFER on 192.168.36.31 to 02:00:00:00:20:1f via eth1
Mar 29 14:26:24 linuxgw dhcpd: DHCPREQUEST for 192.168.36.31 (192.168.36.254) from 02:00:00:00:20:1f via eth1
Mar 29 14:26:24 linuxgw dhcpd: DHCPACK on 192.168.36.31 to 02:00:00:00:20:1f via eth1
Mar 29 14:26:24 linuxgw dhcpd: DHCPREQUEST for 192.168.36.31 (192.168.36.254) from 02:00:00:00:20:1f via eth1
Mar 29 14:26:24 linuxgw dhcpd: DHCPACK on 192.168.36.31 to 02:00:00:00:20:1f via eth1
```

SSH - Secure Shell

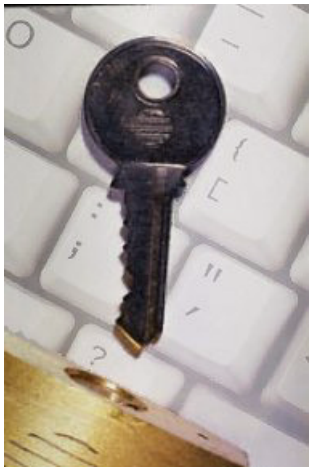
- The standard way for remote logon
- Clients available for many workstation platforms
  - OpenSSH for Linux
  - PuTTY for MS Windows
- Builds encrypted tunnel between host and workstation
  - No password visible for packet sniffers
  - All session data encrypted as well
- SSH can also 'forward' other connections though tunnel
  - Often used for X11 traffic
  - Useful for other applications too (e.g. SMTP)
  - Even possible to run a SLIP - PPP connection over it
- SSH can also do some compression (for dial-up access)

SSH - Secure Shell

Root Password Management

- The Linux root password is needed for serious work
- Customers may need the root password as well
- Root password changes are hard to communicate
- When you need to logon someone will have changed it
- More people than needed will know the password
- Customers may insist in 'fixing' /etc/securetty to reject root logon
  - Make root automatically logon via /etc/inittab
  - Control access to the console via CP or RACF/VM

☛ Use authentication via cryptographic keys instead



SSH - Secure Shell

Beyond Plain Text Passwords

- Authentication via key pairs
- End-user generates a key pair
  - Private key is stored with the client
  - Public key is placed in **`$HOME/.ssh/authorized_keys`**
- Root access controlled per system
- The same key pair can be used for different systems
- No password is needed after authentication via keys
- The private key must be kept secret
  - Should be protected by a 'passphrase'

SSH - Secure Shell

Beyond Plain Text Passwords

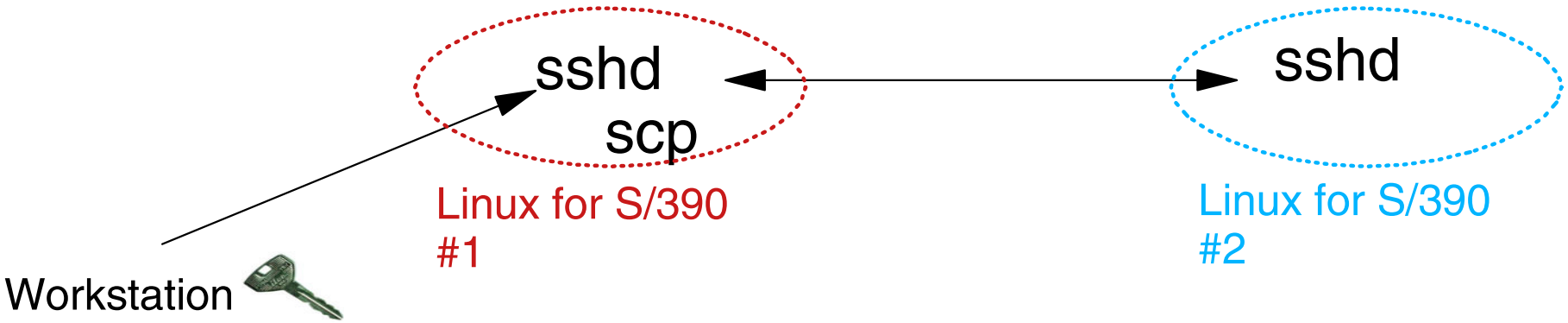
- Authentication is separated from access control
- A single passphrase is used for all systems
- The passphrase is typed only on the trusted workstation
- An ssh-agent on the workstation can hold private keys
  - Putty comes with pageant
- For Linux workstation GUI also starts the ssh-agent
  - Add your private keys with ssh-add
  - Keychain can be useful

```
http://www.ibm.com/developerworks/library/l-keyc.html
http://www.chiark.greenend.org.uk/~sgtatham/putty/
```

SSH - Secure Shell

Authentication Forwarding

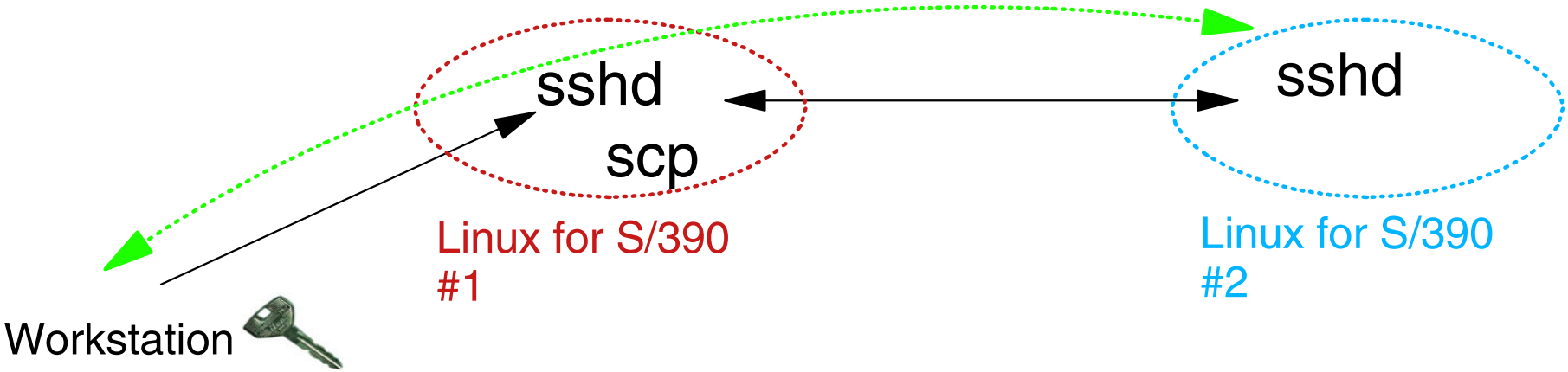
- OpenSSH comes with useful utilities
  - ssh Session to another system
  - scp Secure Copy
  - sftp Secure FTP
- These utilities also need a private key
  - Don't copy the key from your workstation (it is a secret)



SSH - Secure Shell

Authentication Forwarding

- Workstation requests ssh #1 to open an extra socket
- Authentication request from #2 arrives at #1 and is forwarded through the socket to workstation
- Workstation private key and passphrase is used
- The same public key can be used everywhere



Using sudo for Root Access

- Wrapper around setuid
- Grant root access for duration of a single command
- Controlled by /etc/sudoers
  - Lists authorized users
  - Defines commands to be issued
  - Granularity in access is hard to implement
- Provide an audit trail of commands issued as root

```
%maint emealinux = (ALL) NOPASSWD: ALL
```

```
Apr 28 06:01:56 emealinux sudo:  rvdheij : TTY=pts/1 ; PWD=/home/rvdheij ; USER=root ;
        COMMAND=/usr/bin/less /etc/sudoers
Apr 28 06:03:12 emealinux sudo:  rvdheij : TTY=pts/1 ; PWD=/home/rvdheij ; USER=root ;
        COMMAND=/usr/bin/tail /var/log/messages
```

Linux on z/VM - Systems Management

Conclusion

- Linux on z/VM shares a lot of systems management problems with conventional server farms
  - Investigate which existing processes will work for Linux
  - Do not blindly follow suggestions from (PC) Linux experts
- z/VM offers some unique solutions
  - Flexibility through Guest LAN
  - Systems management automation on low level with CMS and CP
- New z/VM function is being added for z/VM
  - Limited cloning function in DirMaint
  - Guest LAN with broadcast for DHCP
- It would be helpful if we had OpenSSH for CMS

rvdheij@nl.ibm.com