1 System admin philosophies

2 5+2=7

3 Prototype Architectures
# A naïve HP-UX to Linux Comparison

<table>
<thead>
<tr>
<th><strong>HP-UX</strong></th>
<th><strong>Linux</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>More expensive</td>
<td>Cheaper to acquire</td>
</tr>
<tr>
<td>Specific hardware</td>
<td>Commodity hardware</td>
</tr>
<tr>
<td>Niche/specialised</td>
<td>Generic, many roles</td>
</tr>
<tr>
<td>Controlled deployment</td>
<td>Proliferation</td>
</tr>
</tbody>
</table>
How and what to administer
For example...

<table>
<thead>
<tr>
<th></th>
<th>Upgrade</th>
<th>Downgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX</td>
<td>swinstall ...</td>
<td>swremove ...</td>
</tr>
<tr>
<td>RedHat</td>
<td>rpm -u ...</td>
<td>rpm -i --force ??? ...</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>apt-get install ...</td>
<td>apt-get install --force- ??? ...</td>
</tr>
</tbody>
</table>
The first decision to make

How will changes be made?

What kind of redundancy?

Needs scalability?

Operating system

Virtualisation VMWare/Xen

Single System Image Cluster

Exclusive application?

Application level

Re-imaging

In place

No

Yes

MC/ServiceGuard-style cluster

Multi-node application

LVS

Parallel

No

Yes
5 “serious” prototype architectures

- **LVS**  Load-balanced
- **Multi-node**  Oracle, DNS, Proxies, Caches
- **ServiceGuard**  Fail-over cluster
- **SSI**  Single system image
- **Virtualised**  VMware, Xen, KVM, (K/)Qemu
...and 2 “not-so-serious” prototype architectures

LVS  Load-balanced
Multi-node  Oracle, DNS, Proxies, Caches
ServiceGuard  Fail-over cluster
SSI  Single system image
Virtualised  VMware, Xen, KVM, (K/)Qemu
LTSP  Thin clients
Standalone  Desktops and unimportant servers
- A layer 4 switch.
- Receives connect requests from clients and then chooses one of the available backend servers.
- Backend server can offer any TCP or UDP service
- Backend servers can be added and removed without client smarts
- NAT, tunnel and direct return options supported.
The application handles the clustering and coherency. Common examples are:

- Oracle 10g
- Web application farms
ServiceGuard (T2798AA)

Before failover  Virtual IP addr and name refers to System A
After failover   Virtual IP addr and name refers to System B
ServiceGuard on Linux information

- cluster lock disks aren’t supported – use a quorum server instead
- raidtools gets confused – use LVM2 instead
- cluster filesystems are supported
- multi-node packages are supported
- otherwise, identical to HP-UX ServiceGuard
OpenSSI is being developed by HP staff and others. Current “wow” features:

- clusterwide PIDs
- process migration
- Load leveling at `exec()` time and during process execution
- Still early in development (2.0pre1 released Nov 2007)
### Virtualised

<table>
<thead>
<tr>
<th></th>
<th><strong>substrate</strong></th>
<th><strong>superstrate</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boot</strong></td>
<td>Local</td>
<td>File or dev on SAN</td>
</tr>
<tr>
<td><strong>OS image</strong></td>
<td>All identical</td>
<td>Mostly different</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>DHCP (usually)</td>
<td>Fixed</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>Lots</td>
<td>Restricted</td>
</tr>
<tr>
<td><strong>Hardware paths</strong></td>
<td>Redundant</td>
<td>Non-redundant</td>
</tr>
<tr>
<td><strong>Backed up</strong></td>
<td>No (usually)</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Install method</strong></td>
<td>PXE or CD-ROM</td>
<td>Disk copy or mount and chroot by substrate</td>
</tr>
</tbody>
</table>
Virtualisation options

**VMware**  Well-known, supports MS-Windows well

**Xen**  In standard Linux kernel, only free live migration system, low performance impact

**KVM**  In standard kernel, will be basis for others in the future.

**User Mode Linux**  Most flexible, can work on very old Linux versions

**K/Qemu**  Full system emulator – can run x86 Linux binaries on Itanium, for example
Very Quick Xen

2. Edit `/etc/xen-tools/xen-tools.conf`
3. Run `xen-create-image --hostname hostname`
4. `xm create -c /path/to/config` to start a virtual machine
5. `xm shutdown name` to stop
6. `xm console name` to access console
7. `xm migrate --live name desthost` to move to new hardware without interruption
LTSP – Linux Terminal Server Project

- Network booting
- Thin clients for desktops (LTSP)
Warewulf clusters

- Network booting
- Thin clients for desktops (LTSP)
- Or overnight reboot of existing desktops for computation (Warewulf)
Standalone

When ...

- time-to-recover doesn’t matter
- data loss is acceptable
- up-front cost is an issue

→ some superstrates
  → desktops
  → testing and learning
  → prototypes
Standalone

When . . .

- time-to-recover doesn’t matter
- data loss is acceptable
- up-front cost is an issue

→ some superstrates
  → desktops
  → testing and learning
  → prototypes

Lots of systems are built like this
Distributed Filesystems

4. Coherency

5. Replication options

6. Multi-mount filesystems

7. Distributed storage options
Mount a filesystem from two servers

```bash
hostA> mount label="afaf324edce2c4" /mnt
hostA> ssh hostB mount label="afaf324edce2c4" /mnt
```

- Read-only for ext3, ext4, reiserfs, xfs etc.
Mount a filesystem from two servers

hostA> some_replicationd hostB
hostA> ssh hostB some_replicationd hostA
hostA> echo hello > /mnt/greeting.txt
hostA> ssh hostB cat /mnt/greeting.txt
hello

- Read-only for ext3, ext4, reiserfs, xfs etc.
- ...unless you replicate
Mount a filesystem from two servers

```bash
hostA> echo hello > /mnt/greeting.txt
hostA> ssh hostB cat /mnt/greeting.txt
hello
```

- ...unless you replicate
- Or use a clustered filesystem...
- Read-write possible for OCFS2, GFS, Lustre
The second question: Data coherency
Real-time responsive replication

- `inotify` to signal changes
- `incrond` to respond
- `scp $# hostB:$#` to propagate

**best for:** numerous tiny files
Semi-responsive

- `rsync from cron`
  
  **best for:** smaller numbers of big files
Manually controlled

- Store data in subversion repository
- Schedule `svn up` and `svn commit` from `cron`

**best for:** configuration files
High-integrity

- CD burned and placed in each server
- New CD burned with each change

best for: un-hackable locked-down environments
OCFS2

- Oracle-sponsored open source project
- No guarantees that timestamp updates or inode changes make sense
- Supports context-dependant symbolic links
- Choice of lock managers

best for: Oracle
Lustre

- Designed for high-performance compute environments
- Scalable to petabytes of storage
- Zero single points of failure
- High-bandwidth access to SAN storage (35GB/s from HP Scalable File Share)

**best for:** i/o bandwidth bottlenecked applications
Sistina (now RedHat) GFS

- In the default Linux kernel
- Uses SAN or network block devices
- Part of RedHat Cluster Suite
- Interacts badly with HP blades using iLO power management

best for: general purpose
Network Block Devices

What if each computer could make its storage visible to other computers as a block device?

- Mirror to a disk on another computer
- Layer a global filesystem using standalone computers
- Migrate virtual machines without SAN storage
What network block devices are there?

- **nbd** the original; point-to-point, authentication by IP address
- **enbd** enhanced; signature-based verification of the server
- **gnbd** part of GFS, but can operate without it. Not part of Linux kernel, but included in most vendor’s kernels. Integrated with fencing.
- **drbd** “distributed replicated block device” – provides RAID1 devices spread across two nodes. Not part of Linux kernel, but included in most vendor’s kernels.
What network block device should I use?

**nbd/enbd**  Testing

**gnbd**  As part of GFS, and for RAID across multiple machines.

**drbd**  Failover clusters
Backup and Recovery

What
Who
How
When
Which
How and what to backup

- Typical Linux
- Typical HP-UX
- Typical Test / Dev
- Typical cache
Infrastructure Components

**imager**  Computer which re-installs other computers over the network

**local satellite**  Server holding ISO images, RPMs, DEBs accessible via HTTP / FTP / NFS

**substrate**  Standardised, simplified operating system install image used in virtualised solutions
### What to backup

<table>
<thead>
<tr>
<th></th>
<th>/etc</th>
<th>/ remainder</th>
<th>data</th>
<th>imager</th>
</tr>
</thead>
<tbody>
<tr>
<td>LVS</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Multi-node</td>
<td>svn</td>
<td>?</td>
<td>Once</td>
<td>√</td>
</tr>
<tr>
<td>ServiceGuard</td>
<td>svn</td>
<td>?</td>
<td>√</td>
<td>?</td>
</tr>
<tr>
<td>SSI</td>
<td>svn</td>
<td>√</td>
<td>√</td>
<td>N/A</td>
</tr>
<tr>
<td>Virtualised</td>
<td>superstrate only</td>
<td>superstrate only</td>
<td>√</td>
<td>N/A</td>
</tr>
<tr>
<td>LTSP</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Standalone</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
How to backup

Of course there are other alternatives for backing up your systems... but DataProtector™ and mkcdrec... are all you need.

Now can I get my sales commission?
How to backup

Of course there are other alternatives for backing up your systems . . .
How to backup

Of course there are other alternatives for backing up your systems ... but
How to backup

Of course there are other alternatives for backing up your systems ... but DataProtector™ and mkcdrec ...
How to backup

Of course there are other alternatives for backing up your systems ... but DataProtector™ and mkcdrec ... are all you need.
Of course there are other alternatives for backing up your systems ... but DataProtector\textsuperscript{TM} and mkcdrec ... are all you need.

Now can I get my sales commission?
DataProtector on Linux

**Pricing**  The same as MS-Windows (i.e. cheap) not like Unix pricing (i.e. expensive)

**Cell Manager**  Supported on 64-bit x86. A post-exec from an internal database backup to restore the internal database to a directory on another DR-ready machine will work correctly.

**Cell Console**  Command-line only (no GUI for Linux), but GUls for other client platforms (e.g. Windows, Solaris, HP-UX) work fine.

**Media Agent**  Fully supported, including SCSI and external control robotics, on 32-bit and 64-bit platforms (which makes do-it-yourself Virtual Tape Libraries possible).

**Disk Agent**  Supported. Some manual fiddling for exotic file systems

**Integrations**  Very wide support.
mkcdrec

- Makes a bootable CD-ROM / DVD / ISO image which restores the system (like make_recovery)
- Can store backup data on tape, DataProtector backup CD-ROM/DVD, NFS server – encrypted or not
- Supports one-button disaster recovery, PXE booting.
- Can use remote tape drives for backup and restore.
- x86 32-bit, x86 64-bit, Itanium (somewhat)
Using mkcdrec

- Install `mkcdrec (http://mkcdrec.ota.be/)`
- Edit `/etc/mkcdrec.conf`
- Schedule `make in cron`
Disaster recovery options

- mkcdrec boot from burned CD-ROM.
- mkcdrec booted via PXE
- mkcdrec boot from one-button-DR tape drive
- SAN hosted boot recovery with DataProtector
- Traditional: re-install, then DataProtector restore
SAN Hosted boot recovery

1. The boot LUN is attached to another Data Protector client...
2. The LUN is partitioned and formatted.
3. The Data Protector GUI is used to restore to the LUN.
4. The LUN is installed to the failed client.
5. The failed client is booted from the LUN.
## Wrap-up

<table>
<thead>
<tr>
<th></th>
<th>DR Recovery</th>
<th>Data Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>LVS</td>
<td>Auto-install</td>
<td>DataProtector</td>
</tr>
<tr>
<td>Multi-node</td>
<td>?</td>
<td>DataProtector</td>
</tr>
<tr>
<td>ServiceGuard</td>
<td>?</td>
<td>DataProtector</td>
</tr>
<tr>
<td>SSI</td>
<td>mkcdrec</td>
<td>DataProtector</td>
</tr>
<tr>
<td>Virtualised</td>
<td>substrate</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Auto-install</td>
<td>N/A</td>
</tr>
<tr>
<td>Virtualised</td>
<td>superstrate</td>
<td>DataProtector</td>
</tr>
<tr>
<td></td>
<td>mkcdrec</td>
<td>DataProtector</td>
</tr>
<tr>
<td></td>
<td>or DP DiskDelivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or snapshot revert</td>
<td></td>
</tr>
<tr>
<td>LTSP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Standalone</td>
<td>mkcdrec</td>
<td>DataProtector</td>
</tr>
</tbody>
</table>
Performance and capacity planning

13  Numerical comparisons

14  Rules of thumb

15  Memory management quiz

16  Performance tricks everyone should know
## SpecInt2000 Performance Comparisons

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>SpecInt2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>N4000</td>
<td>PA8600 (552MhZ)</td>
<td>367/379</td>
</tr>
<tr>
<td>rx5670</td>
<td>1.5GhZ Itanium 2</td>
<td>1312/1312</td>
</tr>
<tr>
<td>bl465c</td>
<td>AMD2220 2-core</td>
<td>1829/1991</td>
</tr>
<tr>
<td>bl480c</td>
<td>Xeon 5160 2-core</td>
<td>3028/3039</td>
</tr>
</tbody>
</table>

- synth. 3GhZ 2-core PA ~ 4000
- synth. 3GhZ 2-core IA ~ 5200
## SpecFp2000 Performance Comparisons

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>SpecFp2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>N4000</td>
<td>PA8600 (552MhZ)</td>
<td>338/369</td>
</tr>
<tr>
<td>rx5670</td>
<td>1.5GhZ Itanium 2</td>
<td>2108/2108</td>
</tr>
<tr>
<td>bl465c</td>
<td>AMD2220 2-core</td>
<td>1833/2023</td>
</tr>
<tr>
<td>bl480c</td>
<td>Xeon 5160 2-core</td>
<td>2739/2756</td>
</tr>
<tr>
<td>synth. 3GhZ 2-core PA</td>
<td>~ 3600</td>
<td></td>
</tr>
<tr>
<td>synth. 3GhZ 2-core IA</td>
<td>~ 8400</td>
<td></td>
</tr>
</tbody>
</table>
### Java Performance Comparison – Pseudo-JBB2000

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>JBB2000 per cpu</th>
</tr>
</thead>
<tbody>
<tr>
<td>N4000</td>
<td>PA8600 (552MhZ)</td>
<td>5024</td>
</tr>
<tr>
<td>rx5670</td>
<td>1.5GhZ Itanium 2</td>
<td>29117</td>
</tr>
<tr>
<td>DL560</td>
<td>Xeon 2.8GhZ</td>
<td>19893</td>
</tr>
<tr>
<td></td>
<td>synth. 3GhZ PA</td>
<td>~ 27000</td>
</tr>
<tr>
<td></td>
<td>synth. 3GhZ IA</td>
<td>~ 58000</td>
</tr>
</tbody>
</table>
## Pseudo-TPC-C Performance Comparison

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>Pseudo-TPC-C</th>
</tr>
</thead>
<tbody>
<tr>
<td>N4000</td>
<td>PA8600 (552Mhz)</td>
<td>7,545</td>
</tr>
<tr>
<td>rx5670</td>
<td>1.5Ghz Itanium 2</td>
<td>34,000</td>
</tr>
<tr>
<td>bl480c</td>
<td>Xeon 5160 2-core</td>
<td>73,600</td>
</tr>
<tr>
<td>synth.</td>
<td>3Ghz PA</td>
<td>~ 41,000</td>
</tr>
<tr>
<td>synth.</td>
<td>3Ghz IA</td>
<td>~ 68,000</td>
</tr>
</tbody>
</table>
If you want to match a PA-RISC or Itanium CPU with x86 CPUs based on clock speed... 

- **integer** add 30% - 60% extra
- **floating point** add 20% (versus PA-RISC) or 200% (versus Itanium)
- **java** add 50% extra (versus PA-RISC) or 200% (versus Itanium)
- **database** subtract 3% - 20%
Memory management quiz – question 1

You are an operating system. A big program calls fork(). What do you do?
You are an operating system. A big program calls `fork()`. What do you do?

1. Check there is enough swap space free to swap the new process out entirely.
You are an operating system. A big program calls \texttt{fork()}. What do you do?

1. Check there is enough swap space free to swap the new process out entirely. \texttt{HP-UX, swapmem off}
Memory management quiz – question 1

You are an operating system. A big program calls `fork()`. What do you do?

1. Check there is enough swap space free to swap the new process out entirely. **HP-UX, swapmem off**
2. Check there is enough memory + swap space to page the process out.
Memory management quiz – question 1

You are an operating system. A big program calls `fork()`. What do you do?

1. Check there is enough swap space free to swap the new process out entirely. **HP-UX, swapmem off**

2. Check there is enough memory + swap space to page the process out. **HP-UX, swapmem on**

3. Hope that the child process calls `exec()` soon.
You are an operating system. A big program calls `fork()`. What do you do?

1. Check there is enough swap space free to swap the new process out entirely. **HP-UX, swapmem off**
2. Check there is enough memory + swap space to page the process out. **HP-UX, swapmem on**
3. Hope that the child process calls `exec()` soon. **Linux default**
A process asks for more memory. You have already used up all real memory and all on-disk swap space. What do you do?
A process asks for more memory. You have already used up all real memory and all on-disk swap space. What do you do?

1. Stretch the truth – OK the request if it’s small and hope some memory comes free later.
Real + virtual + imaginary memory

A process asks for more memory. You have already used up all real memory and all on-disk swap space. What do you do?

1. Stretch the truth – OK the request if it’s small and hope some memory comes free later. Linux default
2. Tell a whopper – OK the request no matter what size it is and hope some memory gets comes free later.
Real + virtual + imaginary memory

A process asks for more memory. You have already used up all real memory and all on-disk swap space. What do you do?

1. Stretch the truth – OK the request if it’s small and hope some memory comes free later. **Linux default**
2. Tell a whopper – OK the request no matter what size it is and hope some memory gets comes free later. `echo 1 > /proc/sys/vm/overcommit_memory`
3. Refuse the request
A process asks for more memory. You have already used up all real memory and all on-disk swap space. What do you do?

1. Stretch the truth – OK the request if it’s small and hope some memory comes free later. Linux default

2. Tell a whopper – OK the request no matter what size it is and hope some memory gets comes free later. `echo 1 > /proc/sys/vm/overcommit_memory`

3. Refuse the request HP-UX
A process asks for more memory. You have already used up all real memory and all on-disk swap space. What do you do?

1. Stretch the truth – OK the request if it’s small and hope some memory comes free later. **Linux default**

2. Tell a whopper – OK the request no matter what size it is and hope some memory gets comes free later. **echo 1 > /proc/sys/vm/overcommit_memory**

3. Refuse the request **HP-UX or echo 2 > /proc/sys/vm/overcommit_memory**
Memory management quiz – question III

Your promises catch up with you. A process is trying to write a page of memory which you promised, but you have nowhere to save it.
Your promises catch up with you. A process is trying to write a page of memory which you promised, but you have nowhere to save it.

1. Send a special signal to all processes to say “free memory if you can”.

Memory management quiz – question III

Your promises catch up with you. A process is trying to write a page of memory which you promised, but you have nowhere to save it.

1. Send a special signal to all processes to say “free memory if you can”. AIX

2. Freeze that process until memory is available.
Memory management quiz – question III

Your promises catch up with you. A process is trying to write a page of memory which you promised, but you have nowhere to save it.

1. Send a special signal to all processes to say “free memory if you can”. **AIX**
2. Freeze that process until memory is available.
3. Randomly kill something big.
Your promises catch up with you. A process is trying to write a page of memory which you promised, but you have nowhere to save it.

1. Send a special signal to all processes to say “free memory if you can”. **AIX**
2. Freeze that process until memory is available.
3. Randomly kill something big. **Linux default**
Memory management quiz – question IV

Which of these can be used for swap? Raw device, logical volume, a file, a directory, a RAM block device, NFS files
Memory management quiz – question IV

- Which of these can be used for swap? Raw device √, logical volume √, a file √, a directory ×, a RAM block device ×, NFS files √

- Do you need swap space?
Memory management quiz – question IV

- Which of these can be used for swap? Raw device √, logical volume √, a file √, a directory ×, a RAM block device ×, NFS files √

- Do you need swap space? **No**

- After a kernel panic, does memory get dumped to the swap device?
Memory management quiz – question IV

- Which of these can be used for swap? Raw device √, logical volume √, a file √, a directory ×, a RAM block device ×, NFS files √
- Do you need swap space? No
- After a kernel panic, does memory get dumped to the swap device? No – Linux doesn’t normally dump-on-crash
- What is the equivalent of the HP-UX kernel variables maxssiz, maxtsiz, maxdsiz, max_dbc_pct??
Memory management quiz – question IV

- Which of these can be used for swap? Raw device √, logical volume √, a file √, a directory ×, a RAM block device ×, NFS files √
- Do you need swap space? No
- After a kernel panic, does memory get dumped to the swap device? No – Linux doesn’t normally dump-on-crash
- What is the equivalent of the HP-UX kernel variables maxssiz, maxtsiz, maxdsiz, max_dbc_pct?? Linux doesn’t have these limits
Performance tricks everyone should know

- Mount all filesystems with `-o relatime` – `atime` only updated if the previous `atime` was earlier than the `ctime` or `mtime`.
- Reduce graphics memory (in BIOS) for servers
- `hdparm` is very conservative – IDE disk access can often be sped up considerably
- Reduce swapiness – `sysctl -w vm.swappiness=10`
Authenticating MS-Windows users logging into Linux

- Do you have a domain or AD tree?
  - YES: Install pGina; authenticate Windows against Linux LDAP
  - NO: SSH keypairs in the user's home directory
- Do you need 2-factor authentication?
  - YES: SSH keypairs stored in a USB key disk with a passphrase
  - NO: Do you want passwords?
    - YES: Authenticate against LDAP tree
    - NO: I DON'T WANT TO
- IT STINKS

Windows-based LDAP server from AD
Linux-based LDAP server for usernames, groups, etc.
What if I have no users?

- **LVS** LDAP for system accounts and machine info
- **Multi-node** Often require LDAP
- **ServiceGuard** LDAP avoids “forgot to add it to the other node” problem
- **SSI** LDAP common
- **Virtualised** LDAP for administrator accounts in substrate, reduces admin load for superstrate
- **LTSP** LDAP necessary when > 1 server
- **Standalone** LDAP useful to save user account data, reduces admin load
What can I store in LDAP?

- User accounts (and personal contact information)
- Groups
- Email aliases and forwarding rules
- Filesystems to automount
- Hostnames (but use DNS instead)
- `sudo` access lists
Use LDAP or suffer

Notice the pattern: LDAP, either served by existing MS-Windows, or elsewise. It’s worth the time even if it’s “only” for a few system accounts. Those few accounts will multiply over time.
LDAP and Linux login observations

- Linux can use the MS-Windows schema (with `pam_winbind.so`), but some other Unixes (and most devices in general) cannot. You might end up with user account information in two places anyway.
- Depending on flakey MS-Windows infrastructure makes Linux flakey too.
- Using `smbmount` to automount home directories from MS-Windows servers isn’t worth the pain. Create Unix-style home directories instead and have them shared by Samba to MS-Windows servers.
- Consider LTSP first before deploying hundreds of standalone Linux desktops.
- Watch out for databases not understanding your schema
Single sign-on without Kerberos

1. Give each MS-Windows user a USB key, a copy of Putty and perhaps Xming.
2. Create a private key on the USB key disk, and an autorun to start up the Paegent with that private key.
3. Put the public key in that user’s ~/.ssh/authorized_keys.
4. Users enter the passphrase once each day and then have access to all Linux systems without further authentication.
5. At the end of the day, the user logs out takes the key disk home.
Single sign-on without Kerberos

1. Give each MS-Windows user a USB key, a copy of Putty and perhaps Xming.
2. Create a private key on the USB key disk, and an autorun to start up the Paegant with that private key.
3. Put the public key in that user’s ~/.ssh/authorized_keys.
4. Users enter the passphrase once each day and then have access to all Linux systems without further authentication.
5. At the end of the day, the user logs out takes the key disk home.

Or, put the private key (unencrypted) in their home directory, and set up their profile to start Paegant automatically.
Single Sign-on with Kerberos

- Most, but not all Linux services are Kerberised. Web apps are often not.
- Time sync matters!
- If using Kerberos + NFS, then user’s cron jobs don’t have access to their home directory
Other exotic authentication options

PAM is configurable and easily extensible.

- **pam_otp_auth** One time passwords
- **pam_pgsq** PostgreSQL database
- **pam_ibutton** Texas Instruments 1-wire iButton
- **pam_imap** Authenticate against an IMAP server
- **pam_usbauth** Uses the unique id of USB devices
- **pam_blue** Login based on Bluetooth device presence
know what your users and systems are doing, make it easy for them to do so,
know when something is wrong and recover quickly and accurately,
know what your users will want in the future and be able to make it happen easily,
know what impact every change will have, and know that what you know is right
Comments? Corrections?