Being Alan Westhagen

This document explains routine tasks that Alan Westhagen performed the RFPK Software Team Leader.

The information in this document is targeted primarily towards the RFPK Software Team and associates and is specific to the computer systems and network installed in the RFPK Laboratory of the Department of Bioengineering of the University of Washington. RFPK is the Resource for Population Kinetics. Its work is supported, in part, by grant P41 EB-001975 of the National Institutes of Health (NIH) of the U.S. Department of Health and Human Services.

Table of Contents

Passwords

Administering machines and software packages requires one to know a lot of passwords. Here is the method that Alan used at RFPK.

The File

All usernames and passwords are kept in a single text file, which is always encrypted. An unencrypted file is never allowed to remain on disk, except during the short time that it is being edited. The file has the pathname `/root/pass.gpg` and is encrypted with a conventional assymmetric cypher, using the command **gpg -c**.

Reading the File

If you want to look for a password in the file, you can read it without having to place an unencrypted copy of the file on disk, by using the following commands:

```
su -
gpg -d pass.gpg | less
```

Finding a Password

Suppose you want to find a password for whitechuck or for an application installed on whitechuck. Here's an easy way to do that, with out placing an unencrypted copy of the file on disk:

```
su -
gpg -d pass.gpg | grep whitechuck
```

Changing the file

If you need to make changes to the file, you will have to create one or more unencrypted copies on disk, depending on which editor you use. *Remove all unencrypted copies as soon as you have reencrypted the file.*

To get a plain text file, edit it with emacs, make a backup copy of the file, reencrypt it and remove the plain text, do the following:

```
su -
gpg pass.gpg
cp pass.gpg pass.gpg.bak
emacs pass
gpg -c pass
rm pass pass~
```

Purchase RHN Subscriptions

Each Linux machine must have a subscription to the RedHat Network (RHN) update service. It does not matter whether the machine is used as a developer workstation or as a server. RFPK uses *RedHat Enterprise Linux Academic Server Edition* for all Linux machines.

When adding a new Linux computer the the set already in use at RFPK, it is much easier if the subscription for it is purchased before Linux is installed. RedHat has designed its installation process so that the first time the system is booted after all the software has been loaded, additional configuration information is requested, including the account name for the RHN subscription.

RedHat provides academic pricing, which costs much less than the standard pricing. The RedHat academic products [1] website is unclear about whether or not computers owned by the university, as opposed to those owned by students, faculty or staff, are eligible for this favorable pricing. Ben Freeman, the RedHat sales representative assigned to the educational industry group, affirm, however, that RFPK owned machines are eligible.

To get academic pricing on a new subscription, and to have that subscription added to the account that we already have, is a bit tricky. If you carefully do the following, it should work.

1. Go to the RedHat Academic Products [2] website.

   You will find that several products are listed. You want RedHat Enterprise Linux Academic *Server* Edition. Click the **Buy Individual Subscription** link.

2. At the *Individual Subscription* page, click the **Subscribe Now** link under RedHat Enterprise Linux Academic *Server* Edition.
3. On the *Buy RedHat Enterprise Linux Academic Server Edition* page, you should be asked to log in. *If you are not asked to log in*, click the **Log in to Your Account** link at the bottom of the page.

   Log in using RFPK's RHN administrative login, *alanwesthagen*. This is very important; otherwise the subscriptions that you buy may not be associated with the pool of entitlements that RFPK already owns.

4. A page should appear, with most of the information already filled in. You must provide the name of institution (University of Washington), the last four digits of your employee number (look on your Husky card), and must attest that you are over 18 years of age.

   Verify that the *email* field contains your email address. If not, change to, so that verification of the order and other RHN administrative mail will come to you.

   After you have entered the information, click the **Submit** button.

5. You will be presented with another page which, in essence, tells you that your are qualified to purchase up to 40 copies. Click the **Buy Now** button.
6. You will then see an order contract. You can fill in the number of copies that you want and check the box that shows that you have read the license agreement. The click the **Checkout** button.
7. Yet another page will appear. Click the **Proceed to Secure Checkout** button.
8. On this page, you provide credit card information. If you have a University of Washington ProCard, use it. Otherwise, use a personal credit card. You can get reimbursed via the petty-cash reimbursement system in place in the Bioengineering Department office.
9. Complete checkout.
10. You will receive an invoice by email. Be sure to print this twice. You will need one copy for reimbursement and the other for your records.

Renew RHN Subscriptions

A month or two in advance of the expiration of an RHN subscription, you will receive email from RHN encouraging you to renew. The message contains a link to the renewal web site. It is best to renew immediately, especially if the subscription is for the workstation (WS) edition. The academic price of WS is $25, but it is not offered anymore, except for renewals. If you allow the subscription to expire, you will have to purchase an academic server (AS) subscription for $50. Even when you renew several months in advance of expiration, your credit card will not be charged until the old subscription expires and the new subscription goes into effect.

Using the University of Washington's RedHat Site Licences

The University of Washington now maintains a satellite RedHat Network Server on campus, and has purchased a site-license for all University of Washington students, faculty and staff. Configuring your computer to work with the satellite server will enable updates to be performed using the up2date command on either the workstation (WS) or advanced server (AS) editions of RedHat Enterprise Linux versions 3

and 4. The benefit of using this system is primarily the savings of $25/subscription through RedHat.

One consequence of using the University of Washingon's RedHat Linux site license is that RedHat will no longer provide customer support for your installation of the software, and you are essentially on your own. This should not be used unless you are very familiar with the Linux operating system, or you have a system administrator who is able to support your installation.

You may configure your computer to use the RHN Satellite server by following the instructions as provided by the Computing & Communication documentation [3] on the subject.

Install Linux on Additional Machines

All of the workstations and servers in the RFPK Linux network run the same version of RedHat Enterprise Linux. There are two different variants of this, however, one for each of the two processor architectures in use. The Sun V20z, which acts as the cspkserver, has the AMD-64 architecture. All the others have the standard architecture. This section outlines the process for installing the software whenever another machine is added to the collection.

1. Make sure that RFPK has a subscription (also called an entitlement) to the Redhat Network (RHN) update service, that is not currently used for another machine. To see the current subscriptions, go the entitlements [4] web page and log in using the RFPK administrative login, *alanwesthagen*. You will see a list of systems currently subscribed. At the bottom of the page you will see a line which reports the number of subscriptions and the number of systems subscribed. If the number of subscriptions does not exceed the number of systems subscribed, you will need to purchase an additional subscription before performing the installation.
2. Select the set of installation CDROMs appropriate for the version of Linux being used and for the processor architecture of the machine that will be the recipient of the software. If the required CDROMs cannot be located in the lab, you may have to download new images and burn them onto blank CD-Rs.

   To find the appropriate images to download, go again to the entitlements [5], and click on the **Channels** button in the bar near the top of the page. You will be transferred to a page which lists a lot of version/architecture pairs. Select the one that is correct for your target machine, and click that link. After that, follow the instructions in our Downloading and Burning ISOs [6] document.

3. Place disk-1 of the set in the CD drive of the target machine and boot. If the machine does not boot from the CD, you will have to go into the BIOS and change the booting order.
4. Once the bootstrap has loaded from the CD, you will be asked whether or not you would like to test the readability of your CDROMs. You should definitely do this, unless you have recently used these disks and know them to be sound.
5. Proceed with the installation. Refer to the document Operating System Version Migration [7] when trying to decide on options for packages, time base, etc.
6. After the installation is complete, the machine will reboot. You will then be asked a series of questions, including those about registering with RHN. When asked whether to use and existing account, provide our username, *alanwesthagen*.
7. The next time that the machine is booted, the installation will be complete.

Check Cron and Logwatch Output

Once a day, the email that root receives on whitechuck should be checked. If any of the programs that **cron** runs automatically during the night has an error, email will be sent to the root user. Once each night a program called **logwatch** filters the system log for what appear to be security breaches and sends the output to the the root user.

To examine this output

```
ssh whitechuck
su -
pine
```

then examine the mail in the inbox.

1. *Cron:* the system is backed up to tape Sunday morning by a program called **bru**. At completion of the backup run, an email summary is sent to root. Normally the report will simply say that there were no errors. If more than a handful of errors are reported, the backup should be run again.
2. LogWatch: the report has several sections of interest:
    a. *pam-unix:* pam is the authentication agent. This section of the report summarizes authentication failures.
    b. *SSHD:* because the gateway/firewall forwards **ssh** request to whitechuck, most attempts by outsiders to log into `spk.rfpk.washington.edu` will be handled by the ssh daemon. All attempts are listed. Note: there is overlap between these attempts and those listed in the pam-unix section.

Keep Systems Up-To-Date

Keeping all of the Linux systems up-to-date is important for reliability and security. RHN provides a web-accessible utility for making this easy. Go to the RHN site which reports on Systems [8] and check the status of your systems at least once a week. If the status shows that any of the systems have errata available, click the names of these systems to see what the errata pertain to. If there are no errata for the Linux kernel, everything can be updated automatically from the web. Simply check-mark each of the systems that have errata outstanding, click the **Manage** button, and then schedule the updates to occur as soon as possible.

On any machine which has errata that pertain to the Linux kernel, the update cannot be done from the web. Instead, the command **up2date** must be run by root on each of the machines, and then the machines rebooted. In the case of the development workstations, each developer should do this himself or herself. Send email, requesting this. You will need to update the servers individually. The easiest way to handle this is to log in as an ordinary user, using **ssh**, use **su** to become root, and then to run **up2date**.

Maintain Network Security

For security and reliability, all of RFPK's Linux workstations and servers are only accessible from the public internet via a gateway server which serves as a firewall.

Network Architecture

A gateway/firewall is implemented with IpCop, which is a special version of Linux, and the following physical components:

1. The gateway server, which is the old HP Vectra PC, located in the back corner of the server area in our lab in AERL. The latches for the case cover of this machine are broken. To open the case, just slide the top and sides, which are formed by a single piece of folded sheet metal, forward. This machine has three separate ethernet network interface cards (NICs).
2. LinkSys 8-port ethernet switch for the DMZ network. It is connected by *orange* CAT-5 patch cables to the gateway server and to the web server.
3. Two Compex DSR2216 16-port ethernet switches, one located in a cubicle on the east side of the lab in AERL and the other in a cubicle on the west side. Together, these serve the LAN network. Using *green* CAT-5 patch cables, the west side switch is connected to the gateway server and to all of the west side workstations and servers. It is connected to the east side switch with a blue CAT-5 patch cable with green ends, that differs from the other cables in the lab in that it is rated for service in an overhead plenum space. The east side switch is connected to the east side workstations with green CAT-5 patch cables.
4. As already mentioned, CAT-5 patch cables:
    a. A red CAT-5 patch cable between one of the NICs in the gateway server and a wall socket. The color red is symbolic of the fact that the public internet, also known as the red network, is dangerous.
    b. Orange CAT-5 patch cables between one of the NICs in the gateway server and the LinkSys switch and between the switch and the web server. The color orange is symbolic of the fact that the machines on the DMZ network, also known as the orange network, are partially accessible to the public internet and, hence, partially in danger.
    c. Green CAT-5 patch cables, between one of the NICs in the gateway server and the west side Compex switch, and between both Compex switches and all workstations and servers on the LAN. The color green is symbolic of the safety of the LAN compared to the public internet.
    d. A blue plenum-rated CAT-5 patch cable, with green ends, which connects the two Compex switches together, so that they act, in essence, as one. Because this is part of the green network, it would have been preferable for the cable to be green, but all that was available was a blue cable with green ends.

       This cable passes from one side of the lab to the other, above the ceiling tiles, in what is known as the heating and ventilating plenum. If there were a fire and ordinary cables were used, it is possible that the heat would cause the insulation on the cables to release dangerous fumes into the ventilation system. The insulation on plenum-rated cable has the property that it does not emit such fumes.

Security Standards

The following standards must be maintained:

1. There must be *no Microsoft Windows* behind the firewall, due to the manner in which the University of Washington network is administered and the ongo-

ing vulnerability of Windows to viruses and spyware. Whenever administrators in the University of Washington Computing and Communications (C&C) department observe network traffic that indicates that a subnetwork contains an infected computer, they shut the entire subnetwork down, and only then attempt to determine exactly which machine was misbehaving. The subnetwork, which may contain many healthy machines as well as the infected one, can be down for days, completely disrupting the work of the "innocent" bystanders. This happened to RFPK. Only one Windows machine was infected, but all of the Linux machines were placed off-line for days. Our current gateway architecture was implemented as a result of that experience. This is now even more important, because we need to keep our servers up at all times, to serve external users.

The gateway is connected to the university network at only one place. To C&C, all of the workstations and servers behind the gateway appear as a single host. The IP address of that host is the IP address of the gateway. Its domain name is `spk.rfpk.washington.edu`. It is the sole computer on its subnetwork, from the point of view of C&C.

2. All external access must be via the gateway. Never bypass the gateway by connecting a workstation or server directly to the university network.
3. All logins, with the exception of logins from an attached keyboard and monitor, must be made via **ssh**. No telnet, rsh, or ftp, for example.
4. All file transfers must be made via **scp**. No rcp or ftp, for example.
5. External **ssh** connections are forwarded by the gateway to whitechuck. This is the only means that is allowed for logging in from the red network.
6. The root user must not be permitted to log into whitechuck from another computer. Because all external logins are forwarded to whitechuck, this means that to gain root access to the network an attacker must first guess the username and password of an ordinary user, and then must guess the root password.

   This restriction is established by the following line in the file `/etc/ssh/sshd_config`

   ```
   PermitRootLogin no
   ```

7. Public key authentication is configured so that the root user on whitechuck can transfer files via **scp** to cspkserver and webserver without providing a password. Details concerning this type of configuration can be found here [9].

Maintain the IpCop Configuration

IpCop is the software that enables the gateway computer to act as a physical three-interface firewall. It, in fact, a specialized version of Linux. The computer, which resides in the far southwest corner of the lab, can be accessed via a keyboard and monitor which are shared, by means of a kvm switch, with whitechuck and webserver. It cannot be accessed using **ssh** because it is set up to forward any **ssh** connection to whitechuck. By logging into the computer from the keyboard, you can perform Linux system administration. This is almost never needed.

The firewall features of IpCop are maintained via a set of administrative screens provided by a graphical user interface. This GUI is not accessible from the keyboard and monitor because, due to a mismatch between the graphics card in the gateway and

that in whitechuck, a graphical desktop cannot be run on the gateway. This is not a problem, however, because the IpCop configuration can be maintained via a web interface [10] from any workstation behind the firewall. The administrative screens are protected by a username (*admin*) and a password.

The administrative web pages that are most frequently accessed are *Services* and *System*.

Services

Within *Services*, the pages that have been used by RFPK for configuration are *dhcp*, *port forwarding*, *external service access*, and *dmz pinholes*.

Dhcp

IpCop provides a dhcp server for the green network. When first added to the network, a host receives its IP address and certain other network configuration parameters from the dhcp server. This simplifies system administration.

One side-effect of using a dhcp server is that the IP address can change if a host is removed from the network and then later reconnected, because the IP address may be reassigned to a different machine in the meantime. Processes in place at RFPK expect IP addresses not to change, however. For example, the deployment script, **deploy_candidate.pl**, copies files from aspkserver to cspkserver. If the IP address of cspkserver were to change, the script would "break".

Dhcp has a feature called the *lease* which keeps an IP address from being reassigned immediately. A host has a lease on an address for a fixed period of time: 120 minutes, for example. If the lease time is made very long, the IP address becomes, in effect, fixed

When a host that is configured to use dhcp is connected to the network, it needs to discover what IP address to use. It sends a message to the dhcp server containing a unique code which distinguishes it from every other computer in the universe. The code that is used is the MAC address of the ethernet card that the host is using for the communication. The ethernet standard requires every card to have a unique MAC address.

When the dhcp server receives the MAC address from a host that is trying to discover its IP address, it first looks in a table to determine whether or not that MAC address already has a lease on an IP. If so, it sends the IP address back to the host; otherwise it creates a new, temporary lease relating the MAC address with an IP address that was currently unassigned.

The *dhcp* screen provides a simple means for extending the time period of an existing lease practically to infinity, effectively making it *fixed*. You simply enter the MAC address and IP address of the lease in the fields provided.

Here is the step-by-step procedure for adding a machine to the green network and fixing its IP address:

1. Physically connect the machine with a green CAT-5 patch cable to one of two Compex ethernet switches.
2. The machine should connect immediately to the internet. Check this, pinging a well-known site:

   ```
   ping mit.edu
   ```

   If this does not work, you may have to restart the network

   ```
   su
   /etc/rc.d/init.d/network restart
   ```

3. In a shell window, execute **/sbin/ifconfig** to determine what the MAC address of the ethernet card is and what IP address has been temporarily assigned by the dhcp server. The information is in the entry titled "eth0". The MAC address is referred to as "HWaddr" and the IP address as "inet addr".
4. In your browser, connect to the IpCop web interface [11]. Proceed to the *Services* screen and then to the *dhcp* screen.
5. In the *Add a new fixed lease* section of the web page, cut and paste the "HWaddr" value and the "inet addr" value from the ifconfig output in your shell window into the *MAC address* and *IP Address* fields respectively.
6. Press the **Add** button to complete the fixing of the lease. The new (MAC address, IP address) pair should appear in the *Current fixed leases* list that appears at the bottom of the screen.

Port Forwarding

The gateway has the domain name `spk.rfpk.washington.edu` and the IP address 128.95.35.85. None of the hosts behind the firewall have domain names or IP addresses that are *routable* (i.e. usable) on the internet. Instead, all requests for services are directed to `spk.rfpk.washington.edu` and then routed, using network address translation (NAT), by the gateway to the particular server that provides that service. For example, all requests for ssh or scp, are forwarded to whitechuck.

To add an additional service to `spk.rfpk.washington.edu` do the following:

1. Select a port number which is currently not being used for any service at `spk.rfpk.washington.edu`.

   Consider as an example, the problem of making the annual report application, which runs on whitechuck port 80, accessible via the web. Because `spk.rfpk.washington.edu:80` was already used for spk, port 80 was not available for the annual report. Instead, we decided on the external address of `spk.rfpk.washington.edu:8082`, and configured the gateway to transfer all requests directed to that address into requests to port 80 on whitechuck.

2. Determine the internal IP address of the server. (One way to do this is to look at the `/etc/hosts` file on whitechuck). In our example, the internal IP address was that of whitechuck, which is `192.168.1.2`.
3. Go from the IpCop *Home* page to the *Services* page to the *port forwarding* page.
4. Fill in the *Source port* field, the *Destination IP* field and the *Destination port* field. In our example, these would be 80, 192.168.1.2, and 8080, respectively.
5. If you want everyone on the public internet to be able to access this service, click the check box field labeled *Enabled*. On the other hand, if you intend to limit access, be sure that this field is blank, for the time being.
6. Click the **Add** button. The forwarding rule should appear in the list at the bottom of the page.
7. If you are not intending to restrict access to this service, you are through at this point.
8. To restrict access, find your new rule which should just have been added to the list at the bottom of the page and click the plus sign. The *Add a new rule* portion of the screen should change so that two fields are presented: *Remark* and *Source IP*.
9.

Dmz Pinholes

System

Backup Administration

The backup administrator takes overall responsibility for the backup processes. The Backup [12] howto gives details.

On a weekly basis or, preferably, more frequently, the backup administrator should verify the following:

1. All developer home directories are being backed up to the `/usr/local/backup` directory on whitechuck.
2. Nightly symbolic dumps of the spkdb database are being copied to `/usr/local/backup` on both whitechuck and cspkserver.
3. The weekly tape backup of whitechuck is occurring without errors.

Purchase Technical Books and Computer Hardware using ProCard

Alan Westhagen used a Visa card issued by the University of Washington under a program called ProCard [13] to purchase technical books for the software team, and parts for the lab's computers. These are the practices that he followed:

- Always be sure to get an invoice or receipt that indicates what was bought. When ordering on-line, print the order page as well as any email confirmation. When the goods arrive, look for an invoice in the package or affixed to it. As a lasting record, keep the best of the invoices for a given item, if there is more than one, and discard the others.
- As soon as a purchase appears on the PaymentNet website, verify it, and supply information about the purpose. For example, "CD/RW drive for Mitch's workstation".
- As soon as you have received the goods, make a copy of the best invoice and send the original to the department purchasing specialist (Amanda Matousek, MS-357962).
- Early each month, a statement detailing ProCard activity for the previous month becomes available on the web. Print this report and attach copies of the invoices for all purchases listed in the statement. Keep this as the RFPK record of the month's purchases.

Add New Users to the SPK Service

Information You Will Need

New users must be added to both the spkdb database and to Bugzilla. You will need the following information:

1. *First Name.* The user's given name.
2. *Surname.* The user's family name.
3. *Username.* Invent a user name. Hint: you can often take the first part of the email address.
4. *Password.* Invent a strong password. The user can change this later.
5. *Email.* The user's email address. *This is necessary for access to Bugzilla.*
6. *Company.* The organization with which the user is associated.
7. *Country.* The country where the user resides.
8. *State.* State, county, region, administrative department or blank. Whatever makes sense for the country in question.

Add the User to the SPK Database

Jiaji Du has a GUI tool for adding the above to spkdb.

Add the User to Bugzilla

Log into Bugzilla [14]. To add users, you must have the *Editusers* bit in your Bugzilla user privilege mask. If you do not have this privilege, the administrative user [15] can grant it to you.

Assuming that you have the *Editusers* permission, here are the steps to follow for adding a new user to Bugzilla.

1. Log into Bugzilla.
2. At the bottom of the main query page, there is a list of links to configuration information that you might want to edit. Click the *users* link.
3. Somewhere near the middle of the user maintenance page, click the *Add a new user* link.
4. On the *Add user* page, enter the *email address* (not the username!) in the field labeled *Login name*.
5. In the *Password* field, enter the same password that you entered into spkdb.
6. Fill in the user's real name, then click the **Add** button.

Copyright Notice

Notes

1. http://www.redhat.com/solutions/industries/education/products/
2. http://www.redhat.com/solutions/industries/education/products/
3. https://www.washington.edu/computing/linux/rhnsat.html
4. https://rhn.redhat.com/network/systems/entitlements.pxt
5. https://rhn.redhat.com/network/systems/entitlements.pxt
6. ../burn-iso/burn-iso.html
7. ../OS-migrate/OS-migrate.html
8. https://rhn.redhat.com/network/systems/system_list/visible_to_user.pxt
9. ../ssh/ssh.html#server-conf
10. https://192.168.1.1:445/cgi-bin/index.cgi
11. https://192.168.1.1:445/cgi-bin/index.cgi
12. ../backup/backup.html
13. http://www.washington.edu/admin/procard/index.htm
14. http://192.168.2.2:8081/index.cgi
15. http://192.168.2.2:8080/soft/howto/rhel3/bugzilla/bugzilla.html#usersect
16. http://www.opencontent.org/openpub/