Linux System Swiss Army Tools for Administrators

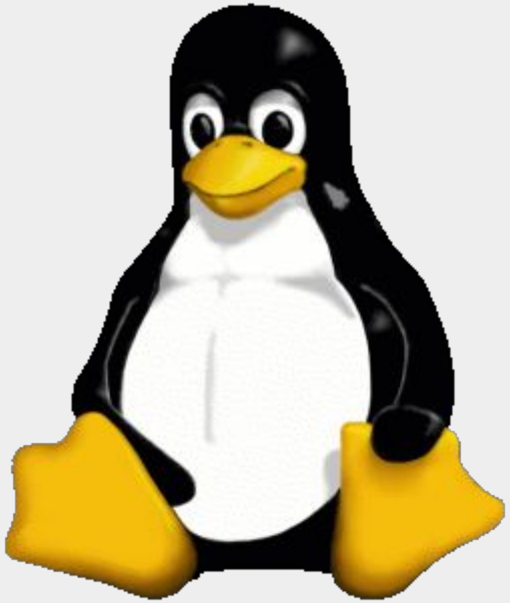
webpros™
SUMMIT2019

Presented by:
Kevin A. McGrail
kmcgrail@InfraShield.com

INFRASHIELD

Introduction

Tux, the Linux mascot



About the Speaker

MAPLE LEAF
READY TO EAT · PRÊT À MANGER
KAM
LUNCHEON MEAT / PAIN DE VIANDE
455
TENEUR ÉLEVÉE EN PROTÉINES
340 g

Kevin A. McGrail
Director, Business Growth

Member of the Apache Software Foundation
& Release Manager for Apache SpamAssassin

cpanelloop@pccc.com

Google Developers Experts 2019
G Suite Product GDE

https://www.linkedin.com/in/kmcgrail

INFRASHIELD

GUI vs CLI

Graphical User Interface

aka a windows interface

Command Line Interface

aka a Terminal

NOTE: Most of what I will cover today is for the CLI but you can open a terminal window in a GUI on your Linux Box

QUIZ #1:

Q: What is WYSIWYG?

A: You are old (like me).

What Distro?

Lots of Flavors!

https://www.centos.org
https://www.redhat.com

https://debian.org & Raspbian

OS X

https://ubuntu.org

Mint/Slackware/SUSE/Fedora/Slack /Gentoo....

The Top Two

#1 Man aka RTFM

In Linux, the command ‘man’ followed by a program name will give you the manual for the program.

- <space> for next page, <enter> for the next line
  - IMPORTANT: **DO NOT USE <return>!**
- p for previous page
- /<search term>

#2 Streams aka Pipes

In Linux, the '|' is a pipe. It streams output from one program or file to another.

Examples will look like this:

```
tail -f /var/log/maillog | grep -i -e msn.com -e outlook.com \
-e hotmail.com -e live.com | grep -i DSN
```

#2 Streams aka Pipes (Continued)

Q: Is there a limit on pipes?

A: The limit is usually based on the number of open files you can have.

ADVANCE: see bash command 'ulimit -a'

"I once saw a junior admin run `'cat access_log | grep blah'` and run a box out of memory" Adam Wien

Connecting to the Terminal

Locally, with a graphical environment, you’ll launch terminal, xterm or a similar tool to get a local command prompt.

Advanced: look at using tmux, I hear the kids love it!

Remotely, use an SSH client!

Putty (https://www.chiark.greenend.org.uk/~sgtatham/putty/) - Windows & Unix

VanDyke SecureCRT (https://www.vandyke.com/products/securecrt/) - PC & Mac

Unix Mantra: Every tool is small & does one job very well

File Transfers

IMPORTANT: Don’t use FTP!

sftp

scp

ADVANCED:

Zmodem over SSH (https://www.extraputty.com/features/zmodem.html)
SecureCRT supports this!

```
yum install lrzsz
sz <filename>
```

Text Editors and Religious Wars

vi (or vim with color syntax)

emacs

nano

pico

What Did I Run?

history

!<#>

Some Basic File Commands

cd - change directory

ls - list files - NOTE: ls -abcdefghijklmnopqrstuvwxyz

```
    ls -al
    ls -1s
```

pwd - path to the current working directory

~ - An alias for your home directory - `cd ~` is the same as `cd`

clear - clears the screen

Searching Streams & Files

grep

What is it? A way to search for lines matching a pattern

Working with Compressed Files? Use these commands:

zgrep for .z files
bzgrep for .bz2 files
zipgrep for .zip files

Advanced: Use a stream! `bzip2 -cdfq | grep [search term]`

QUIZ #2:

Q: What does grep stand for?

History of Grep

g/re/p

Global Regular Expression Print

Q: Why was grep invented?

A: https://www.youtube.com/watch?v=NTfOnGZUZDk

Parsing Lists of Data

uniq (short for unique)

  Key parameter: --count

sort

  Key parameter: -n for number

Examples:

```
ls -1s | sort -n
lastb -i | awk '{print $3;}' | sort | uniq --count | sort -n
```

Bash

aliases & functions in bash
NOTE: store in .bashrc, logout and log back in. chsh to confirm shell

Examples:

```
function slowmaildq { sendmail -OQueueSortOrder=random \
-O QueueDirectory=/var/spool/slow-mqueue/ -qR$1; }
```

```
alias rm='rm -i'
alias checklogs='locate -r ^/htdocs | grep -v old |grep -r \
access_log$ | grep -v backups | xargs ls -1s | sort -n'
```

Counting Lists

wc

What is it? Short for word count

Key Parameter:

-l for lines

Example:

```
lsof -f | wc -l
```

Accessing Files as Streams - Cat

cat

What is it? A way of outputting a file as a stream.

Example:

```
cat /etc/redhat-rele*
```

Accessing Files as Streams - Head/Tail

head/tail

A way of viewing the top or bottom of a file.

Key Parameters:

-f with the tail command we’ll “follow” changes to the file

-n for the number of lines to show - Usually defaults to 3-5

Example:

```
tail /var/log/maillog -n 50
```

Accessing Files as Streams - More/Less

more/less

What is it? Less is more. A modern replacement for more that paginates output. HINT: You already were using it with man!

```
more /var/log/messages
```

<space> for next page, <enter> for the next line

p for previous page

/<search term>

Bash For, If/Else & While

Bash is a programming language. You can do logic like For, Ifs & While.

Example: Use the following bash for loop to delete all messages for example.com:

```
#QIDS="qid1 qid2 qidN"
QIDS="$(mailq | grep -B1 'example.com' | grep '^[a-z]'  | awk  '{print
$1}' \
| sed  's/\*$//')"
for q in $QIDS
do
  qtool.pl -C /etc/mail/sendmail.cf -d /var/spool/mqueue/$q
done
```

Bash For, Ifs & While

#Check all your maillogs for pop3 logins:

```
for f in maillog*; do echo $(grep 'dovecot: pop3(' $f | wc
-l ) $f; done
```

#Pedantic

```
for f in maillog*; do echo $(grep -c 'dovecot: pop3(' $f )
$f; done
```

HINT: man grep will give you a lot of interesting parameters. **-c, -l -i, -v, -e**

QUIZ #3:

Q: Who Invented Champagne?

Level 20 Monks & Clerics

Benedictine Monk, Dom Perignon.

“Come quickly! I am drinking the stars!”

What is Cleric Bayes most famous for? Hint: "An Essay Toward Solving a Problem in the Doctrine of Chances"

https://en.wikipedia.org/wiki/Thomas_Bayes

Mutt

mutt

- What is it? CLI-based Mail User Agent or MUA

Key Commands:

- t for tag
- T for search for tagging
- ; to run a batch command on tagged emails
- v to view the email structure

Mail

mail

What is it? A not as user friendly CLI MUA

Key Points:

good for testing and scripts that email small notes

```
echo "test message" | mail -s"Test Subject" \
kmcgrail+swisstest@infrashield.com

whois infrashield.com 2>&1 | /bin/mail -s 'domain check' \
kmcgrail+swisstest@infrashield.com
```

Regular ~~Hell~~ Expressions

regular expressions are a way to do very complex pattern matching

Example: `s/^\/\/www.infrashield.com\/.*/www.InfraShield.com/ig`

man perlre

“The sour patch kids of the programming language.” -KAM

AWK, Sed & Cut

awk

AWK is a programming language. Useful for changing data into a columnar format and extracting a specific column

sed

sed is a stream editor

cut

cut is a way to remove data from a line

Perl One-Liners

perl one-liners

Example:

```
grep "Org HAS NO CAPACITY"
/var/log/proserver/com_backup42_app.log.* | perl -e \
'while (<>) { s/.*orgName=(.*?),.*/$1/; print}' \
| sort | uniq)
```

The Book of Adam does sayeth, Verse 12 “Anything that takes multiple awk or sed statements in a single command line, you should switch to using perl.”

Run Commands from Files / Streams

Source

source <file with a list of commands>

echo

```
echo "echo test" | sh
```

“Anything you have to do more than twice should be scripted.” - Adam Wien

“Hire a lazy SysAdmin” - Confucius

Doing things based on Streams

xargs

find

Examples: (note the -0 versus the -l1)

```
find -name '*.php' -print0 | xargs -0 grep -l base64_decode
```

```
grep "error state" /var/log/maillog | awk -F ']: ' \
'{print $2}'  | awk -F':' '{print $1}' | xargs -l1 -i \
grep {} /var/log/maillog | grep "error state" -A8 -B8 | more
```

Running Commands in the Background

ctrl-z

pauses the foreground app

jobs

lists jobs running (-l gives the process id)

%1, %2, …

Switch to a the job number (fg switches to the current job)

bg (HINT: you can also add & to a command to do this)

Move the current job into the background

Running Commands One after the Other

command 1; command 2

Run command 1 and then run command 2

command 1 && command 2

Run command 1, then if it succeeds, run command 2

command 1 || command 2

Run command 1, then if it fails, run command 2

Screen

screen - What is it? A CLI Terminal Manager

ctrl-a - The master screen escape

ctrl-a ? - gives you screen help

ctrl-a 0/1/2/3/… - switches to another screen
ctrl-a " - will give you a screenlist

ctrl-a c - for a new screen

ctrl-a d - detach screen
screen -r - reattach

Manual Port Tests

ports

```
more /etc/services
```

nmap

```
nmap [name or ip]
```

telnet

Great for manual testing. Demonstrate Manual SMTP Test.

Manual SMTP Test

More at: https://raptor.pccc.com/raptor.cgim?template=email_spam_compendium

```
telnet <server name> 25
helo <your server name>
mail from: <your email>
data
rcpt to: <a valid e-mail address you are allowed to email on the server>
Subject:<the subject of your message>

<the body of your message>
.
quit
```

Basic DNS Tools

nslookup/dig/host

```
dig -t any mcgrail.com

nslookup 38.124.232.10

host mcgrail.com
```

Shell File Expansion

“*” versus * = Shell Expansion

use “--” to say, “no more command parameters”

#Find and prune Dovecot caches in sub-directories.

```
find home/ -name .imap -exec rm -ri {} \;
```

Time & Date

time

What is it? Not what you think it is! How long a program takes to run!

```
[kmcgrail@talon2 ~]$ time
real    0m0.000s
user    0m0.000s
sys     0m0.000s
```

date

```
Wed Sep 18 11:53:22 EDT 2019
```

Calendar

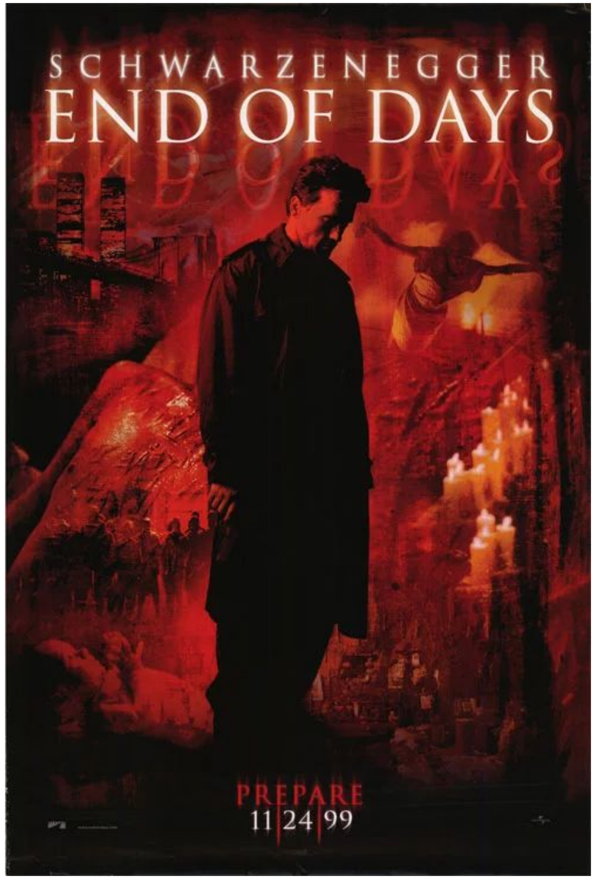
cal

```
[kmcgrail@talon2 ~]$ cal 9 1752
   September 1752
Su Mo Tu We Th Fr Sa
       1  2 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
```

Q: What’s up with this calendar?

Gregorian Reformation

A: The Gregorian Reformation of September 1752



Synchronize Files

rsync

- IMPORTANT: Supports tunneling over SSH!

rclone

- https://rclone.org

Download files from the Web

wget/curl

NOTE: Also supports a few other protocols like FTP

```
wget www.mcgrail.com/downloads/KAM.cf
```

Standard File Descriptors & Redirection

> - Redirect to a file and overwrite

>> - Redirect and append to a file

< - Take input from a file

```
mail -s"Test Subject" \
kmcgrail+swisstest@infrashield.com < /tmp/text-message
```

Advanced File Descriptors & Redirection

“-” - Just the dash is a way of say STDIN or STDOUT. Use /dev/stdin or /dev/stdout instead

STDIN (0), STDOUT (1) & STDERR (2)

2>&1 - Redirect STDERR to STDOUT

[command] > fileA 2>&1 - Redirect errors and output to fileA

[command] > fileA 2> fileB Redirect output to fileA and errors to fileB

NOTE: `command 2>%1 > file` will not work!

Handy “Devices”

yes

```
yes | cp -i /etc/redhat-release /tmp

yes n| cp -i /etc/redhat-release /tmp
```

/dev/zero

/dev/null

```
[command] > /dev/null
cp /dev/null /tmp/emptyfile
```

QUIZ #4: Q: What else will create an empty file?

A: touch [filename]
or cat /dev/null > [filename]
or echo '' > [filename]

Random Devices and Entropy

/dev/random

ADVANCED: haveged / rngd

Line Delimiters

cr/lf & \n\r

\n vs \n\r

https://en.wikipedia.org/wiki/ASCII

NOTE:

- ctrl-c to cancel
- ctrl-v to escape
- ctrl-t for tab
- ctrl-g for bell

Locate & Cron

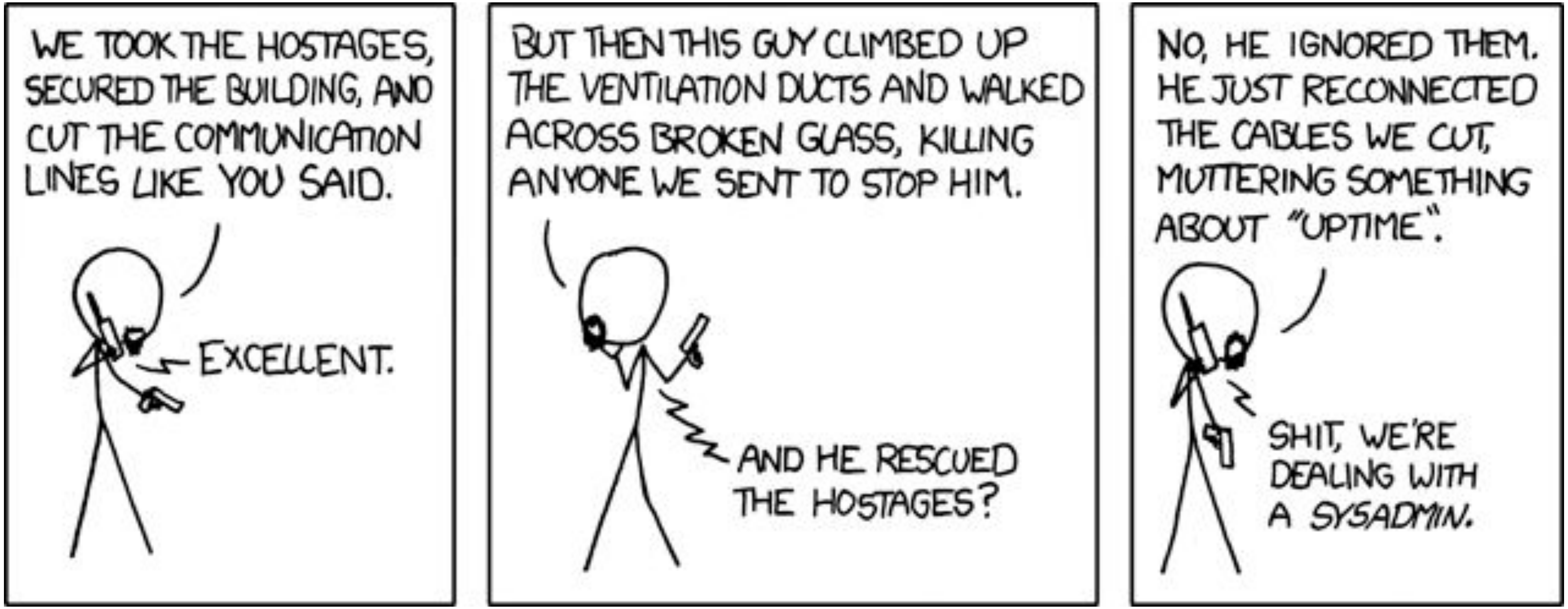
locate

```
   #find -name '*.php' -print0 | xargs -0 grep -l base64_decode

   yum install mlocate

   /etc/cron.daily/mlocate

   locate -0 -r \.php$  | xargs -0 grep -l base64_decode
```

cron

SysAdmin Humor

Xkcd, bofh, lmgtfy, Dilbert & The IT Crowd


WE TOOK THE HOSTAGES, SECURED THE BUILDING, AND CUT THE COMMUNICATION LINES LIKE YOU SAID.
EXCELLENT.
BUT THEN THIS GUY CLIMBED UP THE VENTILATION DUCTS AND WALKED ACROSS BROKEN GLASS, KILLING ANYONE WE SENT TO STOP HIM.
AND HE RESCUED THE HOSTAGES?
NO, HE IGNORED THEM. HE JUST RECONNECTED THE CABLES WE CUT, MUTTERING SOMETHING ABOUT "UPTIME".
SHIT, WE'RE DEALING WITH A SYSADMIN.

Buffering

stdbuf -o0

Buffering with Perl $|++

syslog syncing (“You may prefix each entry with the minus ``-" sign to omit syncing the file after every logging”)

Thanks!

Image Credits:

KAM photo taken by Ted King, used with permission.
Swiss Flag from https://en.wikipedia.org/wiki/Flag_of_Switzerland#/media/File:Flag_of_Switzerland.svg
Tux courtesy of lewing@isc.tamu.edu and The GIMP
https://imgs.xkcd.com/comics/devotion_to_duty.png CC BY-NC 2.5
End of Days poster used under Fair Use

Thanks to:

Adam Wien for his review and input!

Kevin A. McGrail
www.linkedin.com/in/kmcgrail

Thanks!

Have any omissions you think should be added? Here's some I received after my speech and before I uploaded the deck!

w
top
strace
tab completion in the shell