All;

For documentation purposes and whatever else may come…

The latest version of ClamAV is 0.99.4 and consists of 4 packages for Ubuntu 14.04:

clamav-base

clamav-freshclam

clamav

clamav-daemon

installed in that order.

Once all have been installed you’ll need to run freshclam –v, to get the latest updates.

I have downloaded the packages from:  <https://packages.ubuntu.com/trusty/utils/>:

clamav-base\_0.99.4+addedllvm-0ubuntu0.14.04.1\_all.deb

clamav-freshclam\_0.99.4+addedllvm-0ubuntu0.14.04.1\_amd64.deb

clamav\_0.99.4+addedllvm-0ubuntu0.14.04.1\_amd64.deb

clamav-daemon\_0.99.4+addedllvm-0ubuntu0.14.04.1\_amd64.deb

To install these packages use the dpkg –I command.

i.e., dpkg –I ./clamav-base\_0.99.4+addedllvm-0ubuntu0.14.04.1\_all.deb

I modified the /etc/clamav/freshclam.conf file:

Checks **2;  changed from 24.** This tells freshclam to only check for updates twice a day as opposed to 24 times.

I thought that was a little excessive, especially for a Linux system.

I modified the /etc/clamav/clamd.conf file:

LogSyslog **true;** This tells clamav to write all of its info into the syslog file.

As stated above once all of the packages have been installed you’ll need to run

freshclam –v to get the latest updates.

To have the system scanned every Sunday at 0647 create a small script in the /etc/cron.weekly folder.

cd /etc/cron.weekly

vi weekly-system-scan

#!/bin/bash

SCAN\_DIR = “/”

LOG\_FILE=”/var/log/clamav/Weekly\_scan.log

echo “ “

echo “Weekly scan of / started on: $(date)” >> $LOG\_FILE

echo “ “

/usr/bin/clamscan –i –r $SCAN\_DIR >> $LOG\_FILE

echo “ “

echo “Weekly scan of / finished on: $(date)” >> $LOG\_FILE

echo “ “

Be sure to change the permissions on the cron script.

chmod +x /etc/cron.weekly/weekly-system-scan

To stop or start clamav use the following commands:

/etc/init.d/clamav-daemon stop

/etc/init.d/clamav-daemon start

I have verified the script above by placing it in first the /etc/cron.hourly folder

then in the cron.daily folder and reviewing the logs that the scans create to verify

that the scans ran when and as expected.  As an FYI the full system scan to approximately

30 minutes to run.

That should get us complaint with A/V software on the ETC….

All;

I just wanted to let you all know that I was successful in getting the warning banner to display on both the processor and the ETC

last Friday.  BTW, I was also able to open the gate!!!

For the Processor:

Added a line to the /etc/gdm/custom.conf file, under the [greeter] line that reads:

InfoMsgFile=/etc/issue

It’s not pretty as there’s a formatting issue with the spaces but at least all of the required test is there!!!

For the ETC:

This was a bit more complicated.

I created a file in /usr/bin called warning-banner.sh.

the file consist of:

#!/bin/bash

zenity --question --title="NASA WARNING BANNER" --width=800 --height=200 --text="

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*                                                                               \*

\*  You are accessing a U.S. Government information system, which includes:      \*

\*  (1) this computer;                                                           \*

\*  (2) this computer network;                                                   \*

\*  (3) all computers conected to this network including end user systems;       \*

\*  (4) all devices and storage media attached to this network or                \*

\*      to any computer on this network;                                         \*

\*  (5) cloud and remote information services.                                   \*

\*                                                                               \*

\* This information system is provided for U.S. Government-authorized use only.  \*

\* You have no reasonable expectation of privacy regarding any communication     \*

\*   transmitted through or data stored on this information system. At any time, \*

\*   and for any lawful purpose, the U.S. Government may monitor, intercept,     \*

\*   search, and seize any communication or data transiting, stored on, or       \*

\*   traveling to or from this information system.                               \*

\*                                                                               \*

\* You are NOT authorized to store or process classified information on this     \*

\*   information system.                                                         \*

\*                                                                               \*

\* Unauthorized or improper use of this system may result in suspension or       \*

\*   loss of access privileges, disciplinary action, and civil and/or            \*

\*   criminal penalties.                                                         \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

until [[ $? = '0' ]]; do

   zenity --question --title="NASA WARNING BANNER" --width=800 --height=200 --text="

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*                                                                               \*

\*  You are accessing a U.S. Government information system, which includes:      \*

\*  (1) this computer;                                                           \*

\*  (2) this computer network;                                                   \*

\*  (3) all computers conected to this network including end user systems;       \*

\*  (4) all devices and storage media attached to this network or                \*

\*      to any computer on this network;                                         \*

\*  (5) cloud and remote information services.                                   \*

\*                                                                               \*

\* This information system is provided for U.S. Government-authorized use only.  \*

\* You have no reasonable expectation of privacy regarding any communication     \*

\*   transmitted through or data stored on this information system. At any time, \*

\*   and for any lawful purpose, the U.S. Government may monitor, intercept,     \*

\*   search, and seize any communication or data transiting, stored on, or       \*

\*   traveling to or from this information system.                               \*

\*                                                                               \*

\* You are NOT authorized to store or process classified information on this     \*

\*   information system.                                                         \*

\*                                                                               \*

\* Unauthorized or improper use of this system may result in suspension or       \*

\*   loss of access privileges, disciplinary action, and civil and/or            \*

\*   criminal penalties.                                                         \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

done

Once completed I change the perms of it to 755. (chmod 755 /usr/bin/warning-banner.sh)

Next you need to modify the /etc/lightdm/lightdm.conf file.

[SeatDefaults]

autologin-guest=false

allow-guest=false

autologin-user=

autologin-user-timeout=0

autologin-session=lightdm-autologin

greeter-show-manual-login=true

greeter-hide-users=true

greeter-setup-script=/usr/bin/warning-banner.sh

These entries will fix a multitude of sins!!  The last one is what will bring up the warning banner.

A reboot is required before the warning banner will work.

I verified everything worked with Paul before I left.

One other thing I noticed was that the ETC once again could NOT “get outside”.  Turns out the default route wasn’t there again??!!

The only thing I can think of is that someone changed the connection of the Ethernet cable to the “other” port on the ETC system

because the network was now on Eth0. and when I went to /etc/NetworkManager/system-connections and looked at

Ethernet connection 1, the dreaded never-default=true.  I removed that line at POOF, everything worked…

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Create the /etc/dconf/profile/gdm file with the following contents:

user-db:user  
system-db:gdm  
file-db:/usr/share/gdm/greeter-dconf-defaults

Create or edit the banner-message-enable and banner-message-text options in /etc/dconf/db/gdm.d/01-banner-message:

[org/gnome/login-screen]  
banner-message-enable=true

disable-user-list=true  
banner-message-text=’ AGENCY APPROVED WARNING BANNER TEXT'

If you need to add <CRLF> use a \n.

Run the following command to update the system databases:

# dconf update

Ensure that /etc/dconf/db/gdm & /etc/dconf/profile/gdm are set to 644.

Restart gdm by running systemctl restart gdm

Hi team,

As discussed last week, we’d like to refine the charging guidance a little. This helps us know better for cost reporting whether folks are working on Ops Center stuff or station stuff, but all the money comes from the same place, so don’t go nuts trying to keep track.

Some of you are used to using more than one SLR charge number already and might be familiar with separating out your different tasks, but in case you aren’t, this is what I’m expecting.

When in doubt, use your primary charge number. If you know that you are working on a project that falls in another category, take your best guess at how much time you spend working on it. When in doubt, ask. For meetings where we discuss a bunch of stuff, default to your primary charge number.

Here are the categories:

SLR Operations Center:  J2712.2.022.X.XXX.A.XXX.CXXXXX (display name: 22 - 3.0 SLR Data Operati)

               Software or hardware work for Pharaoh532, NuLambda, FileServer, etc

               Data operations:  quality checks, predictions, schedules, data flow

SLR Station Engineering:  J2712.2.022.X.XXX.A.XXX.DXXXXX (display name: 22 - 4.0 Engineering and)

               Software or hardware work for station processor, controller, event timer computer

               Station hardware, e.g. laser, MPACS, radar, MET4

               Activities prompted by a station problem report

Could you add PTO for tomorrow? You should be able to find the charge number if you click "new" and then "search" and look under INDIRECT/FRINGE, it's listed as ENPT (exempt/non-exempt PTO).

SLROC Virtualization:  J2712.2.022.X.XXX.A.XXX.JXXXXX (display name: 22 - SLR Data Operations)

               Preparation of files/software to import into the SPOCC

               Writing scripts to interact with the SPOCC

               Changes to OC software to accommodate interaction with the SPOCC

               Analyzing things that come out of the virtualized OC (predictions, schedules, hourlies)

If you have questions, please ask Chris or me.

Emmanuel,

When filling out your timecard, if you think of it, could you add this charge number and use it for any processor work you are doing?

J2712.2.022.X.XXX.A.XXX.DXXXXX

This is the charge number for station engineering. The one you have currently is for the data operations center. For record keeping purposes, I'm starting to ask folks to differentiate between Ops Center and Station work.

The processor, controller, and ETC are station work. The fileserver, Pharaoh, NuLambda, Lambda532, Mantis, and SVN can all count as Ops Center work.

If you have any questions, please let me know.

Kate

**chmod u+s /lib64/dbus-1/dbus-daemon-launch-helper**  
#disable power button   
**sudo -u gdm**/usr/bin/gconftool-2 --type bool --set /apps/gdm/simple-greeter/disable\_restart\_buttons true   
#disable showing local user list   
**sudo -u gdm**/usr/bin/gconftool-2 --type bool --set /apps/gdm/simple-greeter/disable\_user\_list true   
#enable the banner and display /etc/issue   
**sudo -u gdm**/usr/bin/gconftool-2 --type bool --set /apps/gdm/simple-greeter/banner\_message\_enable true   
**sudo -u gdm**/usr/bin/gconftool-2 --type string --set /apps/gdm/simple-greeter/banner\_message\_text "$(cat /etc/issue)"

To create a GUI login banner on an Ubuntu 14 system create/modify the

/etc/lightdm/lightdm.conf file as follows.

[SeatDefaults]

autologin-guest=false

allow-guest=false

autologin-user=

autologin-user-timeout=0

autologin-session=lightdm-autologin

greeter-show-manual-login=true

greeter-hide-users=true

greeter-setup-script=/usr/bin/warning-banner.sh

Next create the following /usr/bin/warning-banner.sh script and set the

permissions to 755.

#!/bin/bash

zenity --question --title="NASA WARNING BANNER" --width=800 --height=200 --text="

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*                                                                               \*

\*  You are accessing a U.S. Government information system, which includes:      \*

\*  (1) this computer;                                                           \*

\*  (2) this computer network;                                                   \*

\*  (3) all computers conected to this network including end user systems;       \*

\*  (4) all devices and storage media attached to this network or                \*

\*      to any computer on this network;                                         \*

\*  (5) cloud and remote information services.                                   \*

\*                                                                               \*

\* This information system is provided for U.S. Government-authorized use only.  \*

\* You have no reasonable expectation of privacy regarding any communication     \*

\*   transmitted through or data stored on this information system. At any time, \*

\*   and for any lawful purpose, the U.S. Government may monitor, intercept,     \*

\*   search, and seize any communication or data transiting, stored on, or       \*

\*   traveling to or from this information system.                               \*

\*                                                                               \*

\* You are NOT authorized to store or process classified information on this     \*

\*   information system.                                                         \*

\*                                                                               \*

\* Unauthorized or improper use of this system may result in suspension or       \*

\*   loss of access privileges, disciplinary action, and civil and/or            \*

\*   criminal penalties.                                                         \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

until [[ $? = '0' ]]; do

   zenity --question --title="NASA WARNING BANNER" --width=800 --height=200 --text="

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*                                                                               \*

\*  You are accessing a U.S. Government information system, which includes:      \*

\*  (1) this computer;                                                           \*

\*  (2) this computer network;                                                   \*

\*  (3) all computers conected to this network including end user systems;       \*

\*  (4) all devices and storage media attached to this network or                \*

\*      to any computer on this network;                                         \*

\*  (5) cloud and remote information services.                                   \*

\*                                                                               \*

\* This information system is provided for U.S. Government-authorized use only.  \*

\* You have no reasonable expectation of privacy regarding any communication     \*

\*   transmitted through or data stored on this information system. At any time, \*

\*   and for any lawful purpose, the U.S. Government may monitor, intercept,     \*

\*   search, and seize any communication or data transiting, stored on, or       \*

\*   traveling to or from this information system.                               \*

\*                                                                               \*

\* You are NOT authorized to store or process classified information on this     \*

\*   information system.                                                         \*

\*                                                                               \*

\* Unauthorized or improper use of this system may result in suspension or       \*

\*   loss of access privileges, disciplinary action, and civil and/or            \*

\*   criminal penalties.                                                         \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

done

What follows is the script that I proposed adding to the root cron jobs.  Basically what it does is to check each

account for when the password will expire.  The script ignores accounts that have a password life of 99999 (never expires),

60 days (regular local users) and -1, basically the same thing as never expires.

It then calculates how many days until the password expires and, if it less than 30 it will reset the

Last password change field.  Which will act as if the user actually changed the password.  Resulting

in the account having the full password life time reset.

-------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#!/bin/bash

DATE=`date +%y-%m-%d`

currentdate=`date +%s` # in seconds

for user in $(cat /etc/passwd |cut -d: -f1)

        do      maxdays=$(chage -l $user | fgrep 'Maximum number of days between password change')

                expiredate=$(chage -l $user | fgrep 'Password expires' | cut -d: -f2)

                if ( [[ ! $expiredate = \*"never"\* ]] )

                then

                        passexp=`date -d "$expiredate" +%s` # Expire Date in seconds

                        exp=$(($passexp - $currentdate)) # Expire time in seconds

                        expdays=$(($exp / 86400)) # Expire time in days

                        if [ $expdays -le 30 ]

                        then

                                if [ $expdays -ge 0 ] # if it's already expired it most likely not needed so don't reset it

                                then

                                        if ( [[ ! $maxdays = \*"-1"\* ]] && [[ ! $maxdays = \*"60"\* ]] && [[ ! $maxdays = \*"99999"\* ]] )

                                        then

                                                echo "Password for $user expires on :"$expiredate

                                                echo "Password for $user expires in $expdays days"

                                                echo "Updating days between passwords for "$user

                                                chage $user -d $DATE

                                        fi

                                fi

                        fi

                fi

done

For Mantis Backup, you need to replace **the bugtracker in /var/lib/mysql**

Only for Mantis backup procedures. SLR backup procedures should go to J2712.2.022.X.XXX.A.XXX.CXXXXX (SLR)

J2712.2.014.X.XXX.A.XXX.CAXXXX (VLBI)

J2712.2.022.X.XXX.A.XXX.CXXXXX (SLR)