Linux

All about Linux including various configuration procedures, scripts and tips

- Auto Suspend USB
- LXDE Visual Artifacts when Switching from Desktops with Chrome

- Scripts
  - Script - Backup Script for Home Directories and MySQL Databases
  - Script - MySQL Dump Databases Separated by DB Name
  - Script - Move Infected Emails to Quarantine and Notify Users
  - Delete Old Emails and Notify User

- Server Software
  - Apache Option FollowSymLinks not allowed here Error
  - Migrating Self-Signed SSL Certificate to LetsEncrypt Certificate
  - LAMP Stack Upgrade Issues
  - Standard Installation Procedures for LAMP Stack on CentOS 7
  - Slow Loading on Ownloud 8
  - Postfix and Dovecot Configuration
  - Install RethinkDB on CentOS 7
  - Turtl API Server and Client Installation CentOS 7

- Software Development
  - Creating War File in Linux
  - Standard Procedures for CakePHP Application Deployment
  - Installing Clozure CL and QuickLisp on CentOS 7

- Sound
  - No Sound over Wine
  - E: [pulseaudio] module.c: Failed to load module "module-equalizer-sink" (argument: ""): initialization failed.

- Storage
  - LVM Extending from New Physical Volume

- System
  - ArchLinux Upgrade Issues
  - CentOS Installation Issues

    - Changing Default S2RAM to USWSUSP Suspend Module
    - Fixing Incorrect Lid State by Hacking DSDT
    - JournalD Administration
    - Linux on Macbook Administration
    - SELinux - Services Blocked by SELinux
    - Standard CentOS Workstation Setup

- Ansible
    - Playbook - Clearing Users' Data Files in a Group of Windows Machines
    - Playbook - Update Windows Machine (Windows Update Disabled)
    - Playbook - Initiate Clamscan on Machines with ClamWin Installed
    - Playbook - Disable Windows Updates

General

Anything that are related to Linux but does not fit into the category of networking, storage, database or Desktop Environments

General

Batch Image Resize

Keeping Aspect Ratio

```
mogrify -path [Full path to store the resized images] -resize [width]x[height] -quality [quality
```

No Aspect Ratio

```
mogrify -path [Full path to store the resized images] -resize [width]x[height]! -quality [qualit
```

General

Cheking Printer Ink Level

It can be frustrating sometimes that Linux users aren't able to check the ink levels on our printers like Windows users could, but luckily there are packages that will resolve this problem for major printer manufacturers:

1. Install libieee1284-devel
2. Install libinklevel
3. Install ink
4. Use command `ink -p usb` to check

General

Convert PNG to ICO using ImageMagick

```
convert logo.png -define icon:auto-resize=64,48,32,16 logo.ico
```

General

How to do Mac/iOS Stuff in Linux

Converting Apple Developer Certificate to .p12 with OpenSSL

1. Convert the developer certificate file you receive from Apple into a PEM certificate file. Run the following command-line statement from the OpenSSL bin directory: `openssl x509 -in developer_identity.cer -inform DER -out developer_identity.pem -outform PEM`
2. If you are using the private key from the keychain on a Mac computer, convert it into a PEM key: `openssl pkcs12 -nocerts -in mykey.p12 -out mykey.pem`
3. You can now generate a valid P12 file, based on the key and the PEM version of the iPhone developer certificate: `openssl pkcs12 -export -inkey mykey.key -in developer_identity.pem -out iphone_dev.p12`

General

Sendmail Sample Usage

mail.txt:

```
MIME-Version: 1.0
Content-Type: text/html
From: newsletter@shopbah.com
Subject: TESTING 123 hehehe

<html><head><title>TESTING ONLY BAH</title></head>
<body>
<strong>Content line</strong> 1
<strong>Content line</strong> 2
<strong>Content line</strong> 3
</body></html>
```

* `sendmail address@example.com < mail.txt`

General

Windows - Issues

IIS Service Unavailable Error

1. Search for "run"
2. In the run dialog, enter "`iisreset`" and press run

Networking

Linux network troubleshooting and administration

Networking

CentOS 7 - Configuring Cacti

Install Required Dependencies

```
yum -y install mariadb-server php php-cli php-mysql net-snmp-utils rrdtool php-snmp gcc mariadb-
```

Enable Required Services for Cacti

```
chkconfig httpd on
chkconfig mariadb on
chkconfig crond on
```

Download and Extract Cacti

cd /var/www/html
wget http://www.cacti.net/downloads/cacti-0.8.8c.tar.gz
tar -xzvf cacti-0.8.8c.tar.gz

Setting Up Cacti for Apache

Add Cacti User & Enable Cron Jobs

```
adduser cacti
echo "*/5 * * * * cacti php /var/www/html/cacti/poller.php &>/dev/null" >> /etc/cron.d/cacti
```

Fix Cacti Directory Permission

```
cd /var/www/html/cacti
chown -R cacti.apache rra log
```

```
chmod 775 rra log
```

Set Up Cacti Database

```
mysql -p cacti < /var/www/html/cacti/cacti.sql
GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'MyV3ryStr0ngPassword';
flush privileges;
exit
cd /var/www/html/cacti/include/
vi config.php (and change $database_* configuration and $url_path)
```

Open Firewall Ports to HTTP and HTTPS

```
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --reload
```

Login to cacti using admin:admin and go to “Console -> System Utilities” and click on “Rebuild Poller Cache” after the first login!

Networking

IPTables - Forwarding Between LAN and WLAN

Add the following to `/etc/udev/rules.d/10-network.rules`, substitute `LAN_MAC_ADDR` and `WLAN_MAC_ADDR` with your Ethernet device and WLAN device MAC addresses for persistent network names:

```
SUBSYSTEM=="net", ACTION=="add", ATTR{address}=="LAN_MAC_ADDR", NAME="ether0"
SUBSYSTEM=="net", ACTION=="add", ATTR{address}=="WLAN_MAC_ADDR", NAME="wifi0"
```

Add the following to `/etc/sysctl.d/30-ip_forward.conf`:

```
net.ipv4.ip_forward=1
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.all.forwarding=1
Add the following to /etc/iptables/iptables.rules:
*nat
:PREROUTING ACCEPT [783:65928]
:INPUT ACCEPT [73:9660]
:OUTPUT ACCEPT [6180:382480]
:POSTROUTING ACCEPT [18:1260]
-A POSTROUTING -o wifi0 -j MASQUERADE
COMMIT

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [176:192839]
-A INPUT -i lo -m comment --comment "Inbound from loopback (lo)" -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -j NFLOG --nflog-group 1
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -i wifi0 -j ACCEPT
-A FORWARD -i wifi0 -o ether0 -m comment --comment "ether0 <\- wifi0" -j ACCEPT
-A FORWARD -i ether0 -o wifi0 -m comment --comment "wifi0 -> ether0" -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Networking

Connecting to OpenVPN Using NetworkManager

Install the required packages

```
sudo apt-get install network-manager network-manager-openvpn network-manager-openvpn-gnome
```

Creating individual files from client.ovpn file

These files must be kept safe and private at all times

1. Make a directory called openvpn in your home directory
2. Copy the client.ovpn file into dir openvpn
3. Optional: Keep an original copy of the file – call it client.ovpn.orig
4. Next we will create 4 files under the openvpn directory. Open the client.ovpn file in a text editor
5. Create a file called ca.crt – copy the text between and from client.ovpn into this file
6. Create a file called client.crt – copy the text between and from client.ovpn into this file
7. Create a file called client.key – copy the text between and from client.ovpn into this file
8. Create a file called ta.key – copy the text between and from client.ovpn into this file
9. At this point i have a total of 6 files under my openvpn directory

Modify the client.ovpn file

Just before the ## —–BEGIN RSA SIGNATURE—– line add the below lines and save:

```
ca ca.crt
cert client.crt
```

```
key client.key
tls-auth ta.key
```

Setting up the Network Manager

1. Click on Ubuntu network icon on the top right
2. Select VPN Connections -> Configure VPN (the Network Connections window will open)
3. Click on the VPN tab and click Import
4. Select the client.ovpn file we just modified and it should automatically import some things into the next screen
5. Connection Name will be = client – change this to something meaningful (i set it to companyVPN)
6. Gateway must be imported already
7. Type is : Password with Certificates (TLS) – this was also set for me
8. Provide the username and password for VPN
9. User certificate will be client.crt
10. CA certificate will be ca.crt
11. Private Key will be client.key
12. Click on Advanced -> TLS Authentication Tab
13. Key file will be ta.key
14. Key Direction must be set based on the key direction in your client.ovpn file
15. Open the client.ovpn file and search for “key-direction” and note the number after that (mine is key-direction 1)
16. Put this number in the Key Direction field in the TLS Authentication Tab
17. Click save on all windows and close all windows.

Time to test connection

1. Click on network icon on the top right
2. Select VPN Connections and you should see your connection there – click it
3. If successfully connected, you will see a message and then you can verify your IP address with ifconfig
4. There is a Disconnect VPN under VPN Connection for obvious reasons

Networking

OpenVPN - Firewall Configuration

FirewallD

Use the following commands to open all ports required by OpenVPN:

```
firewall-cmd --list-services
firewall-cmd --permanent --add-service openvpn
firewall-cmd --permanent --add-masquerade
firewall-cmd --query-masquerade
firewall-cmd --reload
```

IPTables

My IPTables configuration `/etc/iptables/iptables.rules` for OpenVPN:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [32:2712]
:LOGGING - [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p icmp -m icmp --icmp-type 0 -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo0 -m comment --comment "Allow loopback lo0" -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT
-A INPUT -j LOGGING
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -i tun+ -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A LOGGING -j LOG --log-prefix "DROPPED: " \--log-level 7
-A LOGGING -j DROP
COMMIT
```

```
# Completed on Mon Jun 30 06:48:44 2014
# Generated by iptables-save v1.4.7 on Mon Jun 30 06:48:44 2014
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [2:165]
:OUTPUT ACCEPT [2:165]
-A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
COMMIT
```

Networking

RHEL VLAN and Bonding Configuration

Check list:

- Check whether the 8021q module has been loaded.
- lsmod | grep 8021q
- If the 8021q module is not loaded, run the following command to load it: modprobe 8021q

Configuration

Add the following lines to /etc/modprobe.conf :

```
alias bond0 bonding

options bonding max_bonds=1

Edit /etc/sysconfig/network-scripts/ifcfg-eth0 it should look something like this:
DEVICE=eth0
USERCTL=no
ONBOOT=yes
MASTER=bond0
SLAVE=yes
BOOTPROTO=none
HWADDR=

Edit /etc/sysconfig/network-scripts/ifcfg-eth1 it should look something like this:
DEVICE=eth1
USERCTL=no
ONBOOT=yes
MASTER=bond0
SLAVE=yes
BOOTPROTO=none
HWADDR=
```

Now create the Bond0 interface:

NOTE: No IP address will be assigned to the bond0 device.

Create a new file `/etc/sysconfig/network-scripts/ifcfg-bond0` it should look like this:

```
DEVICE=bond0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet

BONDING_OPTS="mode=1 miimon=100"
```

NOTE: mode could be different, these are the mode options, but if Blade server is using Virtual Connect user should use mode=1.

mode=0 (balance-rr) Round-robin
mode=1 (active-backup) Active-backup
mode=2 (balance-xor) XOR
mode=3 (broadcast) Broadcast
mode=4 (802.3ad) IEEE 802.3ad Dynamic link aggregation
mode=5 (balance-tlb) Adaptive transmit load balancing
mode=6 (balance-alb) Adaptive load balancing

The first four modes are the most commonly used:

VLAN tag setup

This will be a virtual interface with a VLAN tag of 48. User's VLAN set-up is most likely different so just replace 48 with the VLAN tag of user's network. i.e. bond1.50 would be the bonded interface for VLAN 50.

Create a new file `/etc/sysconfig/network-scripts/ifcfg-bond0.48` it should look like this:

```
DEVICE=bond0.48
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
VLAN=yes
NETMASK=255.255.255.0
NETWORK=192.168.48.0
IPADDR=192.168.48.100
```

Ensure that the default gateway in this configuration is recorded in the /etc/sysconfig/network file otherwise it may not work properly. Once done, it should look something like:

```
NETWORKING=yes
HOSTNAME=
GATEWAY=192.168.48.1
```

User has now setup bonding and VLAN tagging. User needs to restart networking to make the changes active.

```
service network restart
```

Testing

Verify bonding interface is up and running

```
ifconfig -a
```

Verify configuration (RHEL 5 is using `sysfs` , so check out `/sys/class/net/`)

Networking

Setup SFTP to Public Directory (/var/www)

Configuring SSH for SFTP

1. `vim /etc/ssh/sshd_config`
2. Comment the following line:
    1. `Subsystem sftp /usr/local/libexec/sftp-server`
3. Add the following lines:
    1. `Subsystem sftp internal-sftp`
    2. `Match Group <sftp group>`
    3. `ChrootDirectory %h`
    4. `ForceCommand internal-sftp`
    5. `X11Forwarding no`
    6. `AllowTcpForwarding no`
4. Save and close
5. Reload ssh `sudo systemctl restart sshd`

Add SFTP User and Set Permission

1. `sudo groupadd <user> -g <sftp group> -s /bin/false -d /var/www/html`
2. `sudo passwd <user>`
3. `sudo chown root /var/www/html`
4. `sudo chmod 755 /var/www/html`
5. `sudo mkdir /var/www/html/<dir>`
6. `sudo chmod 775 /var/www/html/<dir>`
7. `sudo chown apache: apache /var/www/html/<dir>`
8. `sudo chmod g+s /var/www/html/<dir>`

Selinux

1. `sudo setsebool -P ssh_chroot_rw_homedirs on`
2. `sudo setsebool -P httpd_unified 1`
3. `sudo setfacl -d -m g: apache: rw /var/www/html/<dir>`

References

1. Spiceworks Article
2. CentOS Docs

Networking

FirewallD - Opening a Port

Use this command to find your active zone(s):

```
firewall-cmd --get-active-zones
```

It will say either public, dmz, or something else. You should only apply to the zones required.

In the case of dmz try:

```
firewall-cmd --zone=dmz --add-port=<port>/tcp --permanent
```

Otherwise, substitute dmz for your zone, for example, if your zone is public:

```
firewall-cmd --zone=public --add-port=<port>/tcp --permanent
```

Then remember to reload the firewall for changes to take effect.

```
firewall-cmd --reload
```

Networking

Using LetsEncrypt for OpenVPN WebSSL

Using letsencrypt for OpenVPN Access Server is nothing more than symlinking the files to letsencrypt keys and certs:

1. `sudo -s`
2. `cd /usr/local/openvpn_as/etc/`
3. `mv web-ssl web-ssl.bak`
4. `mkdir web-ssl`
5. `ln -s /etc/letsencrypt/live/<letsencrypt domain dir>/privkey.pem web-ssl/server.key`
6. `ln -s /etc/letsencrypt/live/<letsencrypt domain dir>/cert.pem web-ssl/server.crt`
7. `ln -s /etc/letsencrypt/live/<letsencrypt domain dir>/fullchain.pem web-ssl/ca.crt`
8. `systemctl restart openvpnas`

Networking

Monitor Mode on Broadcom-wl Driver

Enable monitor mode:

```
$ echo 1 > /proc/brcm_monitor0
```

Enabling monitor mode will create a `prism0` network interface. Wireshark and other network tools can use this new `prism0` interface.

To disable monitor mode:

```
$ echo 0 > /proc/brcm_monitor0
```

Networking

SSH Tunneling

`ssh -p <port> <username>@<remote host> -L <local listening port>:<remote's host ip>:<remote's host port> -N`

Note:
Remote's host and port can be any host and port accessible by the remote host, e.g. to access the router web interface on 192.168.1.1 (remote) use <local listening port>:192.168.1.1:80

Networking

Syncing Files with FTP

I came across a problem when doing migration last time, the server grew too big that I cannot just simply compress the files and move it to another server, it was more than 20GB files. So, I came across an FTP client called LFTP that will synchronize files and folders over FTP. The script below is the script I used to sync the files, let's call it sync.sh:

```
#! /bin/bash
HOST='<ftp host>'
USER='<ftp user>'
PASS='<password>'
RCD='<remote directory to sync>'
lftp -e "
open $HOST
user $USER $PASS
mirror --verbose --continue $RCD
bye
"
```

To sync only certain folders, use the following sciprts:

```
#! /bin/bash
HOST='<ftp host>'
USER='<ftp user>'
PASS='<password>'
RCD='<remote directory to sync>'
lftp -e "
open $HOST
user $USER $PASS
mirror --verbose --continue --exclude '.*' --exclude '.*/' --include '<folder1>' --
include '<folder2>' $RCD
bye
"
```

To have sync overnight even when logged out, use the command `nohup bash sync.sh > sync.log`.

Networking

ArchLinux - Setting Up Fortinet SSL VPN

1. Install ppp, openfortivpn and networkmanager's fortinet plugin package: `sudo pacman -Syu ppp openfortivpn networkmanager-fortisslvpn`
2. Get certificate digest by running: `sudo openfortivpn <IP Address>:<Port> --username=<username>`
3. Enable kernel module: `modprobe ppp_generic`
4. Reconnect with openfortivpn: `sudo openfortivpn <IP Address>:<Port> --username=<username> --trusted-cert <certificate digest>`
5. Now you can connect to the VPN by creating a new Fortinet SSLVPN (fortisslvpn) connection:
   - Enter the `Gateway` in the format `<IP Address>:<Port>`
   - Your username and password
   - Finally click "Advanced" and enter the certificate digest into `Trusted certificate` field

References

- ArchLinux PPP
- Openfortivpn

Desktop Environments

Everthing to do about Desktop Environments, including LXDE, XFCE, KDE and Gnome

Getting Cursor Pointer Theme for LXDE

1. Installing the package `xcursor-themes`
2. Then go to `Preferences` > `Customize Look and Feel`
3. Select your cursor pointer theme under `Mouse Cursor` tab

Desktop Environments

LXDE Volume Keybinding

Add the following lines to `~/.config/openbox/lxde-rc.xml`:

```
<keybind key="XF86AudioMute">
  <action name="Execute">
    <command>amixer sset Master toggle</command>
  </action>
</keybind>
<keybind key="XF86AudioRaiseVolume">
  <action name="Execute">
    <command>amixer sset Master 5%+</command>
  </action>
</keybind>
<keybind key="XF86AudioLowerVolume">
  <action name="Execute">
    <command>amixer sset Master 5%-</command>
  </action>
</keybind>
```

Issue command => `openbox --restart`

LXDE Blueproximity Settings

Locking Command: `xscreensaver-command -activate`
Unlock Command: `pkill xscreensaver`
Proximity Command: `xscreensaver-command -time || daemonize /usr/bin/xscreensaver -no-splash`
Daemonize Utility: To stop blueproximity from hanging when using the proximity command, it requires the daemonize command (http://software.clapper.org/daemonize/). Using "xscreensaver -no-splash &" or "xscreensaver -no-splash" will cause blueproximity to hang.

Auto Suspend USB

There are 2 settings that needs to changed:

1. Add `usbcore.autosuspend=0 usbcore.autosuspend_delay_ms=-1` to `/boot/grub/grub.cfg` kernel param
2. Disable monitor power manager control in `xfce4-power-manager` settings
3. Install `acpid`
4. Add the following udev rules to `/etc/udev/rules.d/99-usb-autosuspend.rules`:

```
ACTION=="add", SUBSYSTEM=="usb", TEST=="power/control",
ATTR{power/control}="on"
ACTION=="add", SUBSYSTEM=="usb", TEST=="power/autosuspend",
ATTR{power/autosuspend}="0"
ACTION=="add", SUBSYSTEM=="usb", TEST=="power/autosuspend_delay_ms",
ATTR{power/autosuspend_delay_ms}="-1"
```

Desktop Environments

LXDE Visual Artifacts when Switching from Desktops with Chrome

LXDE Visual Artifacts when Switching Desktops. Install a composite manager will remove the artifacts, below is a list of composite managers:

- xcompmgr - a minimal alternative to Compiz
- Compton - A bug-fixed fork of dcompmgr, which is a fork of xcompmgr
- Cairo Compmgr (Cairo Composite Manager) - a compositing add-on for existing window managers. It uses Cairo), a vector graphics library also used in GTK+.
- Unagi Compositing Manager - a compositing manager which can be used along with an existing window manager. It uses the XCB library. I used Compton for my composite manager:

Install `compton` package Add `@compton -b` to the end of `/etc/xdg/lxsession/LXDE/autostart`

References:

1. https://wiki.archlinux.org/index.php/Compton

Scripts

Contains all the script I used for my administration

Scripts

Script - Backup Script for Home Directories and MySQL Databases

```
#!/bin/sh

# Home directory to backup must be absolute path, with trailing slash
home_dir='/home/'
# Target backup directory, must be absolute path, with trailing slash
backup_dir='/backups/'

# Database user
db_user='root'
# Database Password
db_pwd=''

cd "$home_dir"
# Get list of users based on home dir
users=`find . -maxdepth 1 -type d \( -iname "*" ! -iname "backups" ! -iname "lost+found" \) -
exec echo {} \; | sed "s#./##" | grep -v '^/home$'`
for user in $users; do
    # Skip if user string is empty
    if [ $user == "" -o $user == ".." -o $user == "." ]; then
        continue
    fi
    # Archive all files in directory
    archive="$backup_dir`date +%Y%m%d`.$user.tar.gz"
    tar czf "$archive" "$user"
done

# Database backup script
if [ ! -z "$db_pwd" ]; then
```

```
    databases=`mysql -u$db_user -p$db_pwd -e "SHOW DATABASES;" | tr -d "| " | grep -v
Database`
else
    databases=`mysql -u$db_user -e "SHOW DATABASES;" | tr -d "| " | grep -v Database`
fi
cd $backup_dir
for db in $databases; do
    if [[ "$db" != "information_schema" ]] && [[ "$db" != "performance_schema" ]] && [[ "$db"
!= "mysql" ]] && [[ "$db" != _* ]] ; then
        sql="`date +%Y%m%d`.$db.sql"
        echo "Dumping database: $db"
        if [ -z "$db_pwd" ]; then
            mysqldump -u$db_user $db > $sql
        else
            mysqldump -u$db_user -p$db_pwd $db > $sql
        fi
        tar -czf "`date +%Y%m%d`.$db.sql.tar.gz" $sql
        rm $sql
    fi
done
```

NOTE: Add this to `cronjob` to delete backups older than 90 days: `find . -type d -mtime +90 -exec rm {}\;`

Scripts

Script - MySQL Dump Databases Separated by DB Name

```
#! /bin/bash

DUMP_EXEC="mysqldump" #path to mysqldump
MYSQL_EXEC="mysql" #path to mysql

MYSQL_USER="root" #db user
MYSQL_PASSWORD="" #db password

databases="$MYSQL_EXEC -u$MYSQL_USER"
if [ "$MYSQL_PASSWORD" ]; then
    databases="$databases -p$MYSQL_PASSWORD"
fi

eval "$databases -e 'show databases'" | while read dbname
do
    if [ "$dbname" ]; then
        echo "Dumping database: $dbname"
        dumpScript="$DUMP_EXEC --max_allowed_packet=1G -u$MYSQL_USER"
        if [ "$MYSQL_PASSWORD" ]; then
            dumpScript="$dumpScript -p$MYSQL_PASSWORD"
        fi
        eval "$dumpScript --complete-insert '$dbname' > '$dbname.sql'"
    fi
done
```

Script - Move Infected Emails to Quarantine and Notify Users

The following script will do the following:

1. Parse email headers from ClamScan Results
2. Move infected email to `$QUARANTINE` folder
3. Construct email messages
4. Email the users who has any infected emails in their mailbox

```
#! /bin/bash

ADMIN="admin@domain.com" # Admin email
QUARANTINE="/quarantine/directory/" # Quarantine folder with trailing slash
HEADER="The emails listed has been moved to quarantine and will be deleted after 30 days. If you have any concerns, please contact the server administrator"
FOOTER="This is an automated email through ClamScan results, please find the script details at 'https://wiki.twcloud.tech/books/linux/page/script---move-infected-emails-to-quarantine-and-notify-users'"

# Getting email information
[ -z "$1" ] && echo "File parameter missing" && exit 1
[ ! -f "$1" ] && echo "File not found / not a regular file" && exit 1
declare -A emails
while read i; do
    file=`echo "$i" | sed -e 's/\: \ .*FOUND//'`
    if [ ! -f "$file" ]; then
        continue
    fi
    infection=`echo "$i" | sed -n 's/\: \ .*FOUND//'`
    to=`cat "$file" | grep -m 1 "^Envelope-to\: \s\+" | sed 's/Envelope-to\: \ //' | grep -EiEio '\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b'`
```

```
    # Try find To: header if Envelope-to: not found
    [[ -z "$to" ]] && to=`cat "$file" | grep -m 1 "^To\:\s\+" | sed 's/To\:\ //' | grep -EiEio
'\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b'`
    from=`cat "$file" | grep -m 1 "^From\:\s\+" | sed 's/From\:\ //'`
    d=`cat "$file" | grep -m 1 "^Delivery-date\:\s\+" | sed 's/Delivery-date\:\ //'`
    subject=`cat "$file" | grep -m 1 "^Subject\:\s\+" | sed 's/Subject\:\ //'`

    # Send empty "$to" to admin
    [[ -z "$to" ]] && to="$ADMIN"

    # Construct email message
    [[ -z "${emails[$to]}" ]] && emails[$to]="$HEADER"
    emails[$to]="${emails[$to]}\n\nFrom: $from\nDate: $d\nSubject: $subject"

    # Move emails to quarantine
    mv "$file" "$QUARANTINE"
done < "$1"

# Notify email users that the emails are sent to quarantine
for k in "${!emails[@]}"; do
    echo -e "${emails[$k]}\n----------\n$FOOTER" | mail -s "Infected emails quarantined" -c
"$ADMIN" $k
done
```

Scripts

Delete Old Emails and Notify User

```
ADMIN="admin@domain.com" # Admin email
DOMAIN="domain.com" # Domain name
HEADER="The emails listed has been moved to trash, and will be deleted on the 31st December every year"
FOOTER="This is an automated email generated through a script, please find the script details at 'https://wiki.twcloud.tech/books/linux/page/delete-old-emails-and-notify-user'"
REMOVE_FILE_AGE=60 # File age to remove in days
USER="user" # Username used to login to the hosting account
TRASH_FOLDER="/home/$USER/trashed_emails/" # Trash folder with trailing slash

# Getting email information
[ -z "$1" ] && echo "Email user parameter missing" && exit 1
[ ! -d "/home/$USER/mail/$DOMAIN/$1/cur" ] && echo "Email not found" && exit 1
# Declarations
declare -A emails

for file in $(find "/home/$USER/mail/$DOMAIN/$1/cur" -type f -mtime +${REMOVE_FILE_AGE} -print); do
    if [ ! -f "$file" ]; then
        continue
    fi
    to="$1@$DOMAIN"
    from=`cat "$file" | grep -m 1 "^From\:\s\+" | sed 's/From\:\ //'`
    d=`cat "$file" | grep -m 1 "^Delivery-date\:\s\+" | sed 's/Delivery-date\:\ //'`
    subject=`cat "$file" | grep -m 1 "^Subject\:\s\+" | sed 's/Subject\:\ //'`

    # Send empty "$to" to admin
    [[ -z "$to" ]] && to="$ADMIN"

    # Construct email message
    [[ -z "${emails[$to]}" ]] && emails[$to]="$HEADER"
```

```
    emails[$to]="${emails[$to]}\n\nFrom: $from\nDate: $d\nSubject: $subject"

    # Move emails to trash
    mv "$file" "$TRASH_FOLDER"
done

# Notify email users that the emails are sent to trash
for k in "${!emails[@]}"; do
    echo -e "${emails[$k]}\n----------\n$FOOTER" | mail -s "Inbox Cleared" -c "$ADMIN" $k
done
```

Server Software

Server software configuration and installation procedures such as Apache, and Postfix

Server Software

Apache Option FollowSymLinks not allowed here Error

Apache htaccess `Option FollowSymLinks not allowed here` error:

```
find /home -name ".htaccess" -type f -exec sed -i '/FollowSymLinks/SymLinksIfOwnerMatch/g' {} ";"
```

Server Software

Migrating Self-Signed SSL Certificate to LetsEncrypt Certificate

Download Let's Encrypt Client

1. `sudo -s`
2. `git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt`

Update Apache Configuration

Let's Encrypt does not detect multiple virtual host in a single file, so if you have multiple virtual hosts in a single file, you need to separate it and update the configuration for SSL only. Then redirect all plain-text traffic to SSL using a single virtual host.

Create a new virtual host in `/etc/httpd/conf.d/redirect_ssl.conf` to redirect plain-text traffic to SSL, replace all `<domain>` to your TLD, such as `example.com`:

1. `<VirtualHost *:80>`
2. `ServerName <domain>`
3. `ServerAlias *.<domain>`
4. `RewriteEngine on`
5. `RewriteRule ^/(.*) https://%{HTTP_HOST}/$1 [NC,R=301,L]`
6. `</VirtualHost>`

Setup SSL Certificates

1. `cd /opt/letsencrypt`
2. `./letsencrypt-auto --apache -d <domain> -d www.<domain> -d <subdomain>.<domain>`

Replacing `<domain>` with your domain, subsequent subdomains can be specified with `-d` option.

Restart Apache and Test

1. `systemctl restart httpd`

(Optional) Renewing SSL Certificates

Let's Encrypt issue **90 days** validity certificates, but you can however, renew it earlier in case errors occurred.

To renew the certificates, simply use the following command:

1. `/opt/letsencrypt/letsencrypt-auto renew`

If you have just created a new certificate, Let's Encrypt will never issue you a new one, it will only issue a new certificate for your domains if the validity period is **less than 30 days**, so, you can create a cronjob to try and renew the certificate every day, week or month, in case anything goes wrong with your certificate.

To setup cronjob to automatically renew certificate, enter command `crontab -e` to create a new cronjob and add the following line:

1. `0 3 * * 1 /opt/letsencrypt/letsencrypt-auto renew >> /var/log/le-renew.log`

The cronjob above will run on **every monday** at **3 A.M.**, it will append any output from `/opt/letsencrypt/letsencrypt-auto` to `/var/log/le-renew.log`. Please refer to the reference for more info on Linux cronjobs.

References

1. Digital Ocean Article
2. Let's Encrypt Article
3. Cronjob Format

LAMP Stack Upgrade Issues

"Table Doesn't Exists" After MySQL/MariaDB Upgrade

Paste MySQL data directory to upgraded data directory, containing `ibdata1`, `ib_logfile0` and `ib_logfile1`, in `lampp`, it's `/opt/lampp/var/mysql`:

1. `sudo cp /opt/lampp_backup/var/mysql /opt/lampp/var/mysql`
2. `sudo chown -R mysql: mysql /opt/lampp/mysql`

Server Software

Standard Installation Procedures for LAMP Stack on CentOS 7

1. System Upgrade

1. `yum -y update`

2. Install Required Software

1. `yum -y install git policycoreutils-python httpd mariadb mariadb-server php-mysql php-gd php-ldap php-odbc php-pear php-xml php-xmlrpc php-mbstring php-snmp php-soap curl curl-devel`

3. Setup MySQL Server

1. `mysql_secure_installation`

4. Start and Enable All Services

1. `systemctl enable httpd`
2. `systemctl enable mariadb`
3. `systemctl start httpd`
4. `systemctl start mariadb`

5. Open Firewall Ports

1. `firewall-cmd --permanent --zone=public --add-service=http`
2. `firewall-cmd --permanent --zone=public --add-service=https`
3. `firewall-cmd --permanent --zone=public --add-port=<ssh_port>/tcp`
4. `firewall-cmd --reload`

6. Change SSH Port

1. `vim /etc/ssh/sshd_config #and append 'Port <ssh_port>'`
2. `semanage port -a -t ssh_port_t -p tcp <ssh_port>`
3. `systemctl restart sshd`

7. Enable Shutdown Button

Edit `/etc/systemd/logind.conf` and uncomment the following 2 lines:

1. `PowerKeyIgnoreInhibited=no`
2. `HandlePowerKey=poweroff`

8. Reboot System

1. `reboot`

(HP MicroServer Only)

Edit `/etc/default/grub` and append `clocksource=hpet nolapic` to the end of `GRUB_CMDLINE_LINUX` variable.

Server Software

Slow Loading on Ownloud 8

Change `/var/www/html/owncloud/config/config.php` database host to `127.0.0.1` instead of `localhost`

Server Software

Postfix and Dovecot Configuration

Installation

1. `hostnamectl set-hostname mail.<domain>.<tld>`
2. `yum -y install postfix dovecot`

Postfix Configuration

1. Append the following to `/etc/postfix/main.cf`:
    1. `myhostname = mail.<domain>.<tld>`
    2. `mydomain = <domain>.<tld>`
    3. `myorigin = $mydomain`
    4. `home_mailbox = mail/`
    5. `mynetworks = 127.0.0.0/8 <domain IP>`
    6. `inet_interfaces = all`
    7. `mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain`
    8. `smtpd_sasl_type = dovecot`
    9. `smtpd_sasl_path = private/auth`
    10. `smtpd_sasl_local_domain =`
    11. `smtpd_sasl_security_options = noanonymous`
    12. `broken_sasl_auth_clients = yes`
    13. `smtpd_sasl_auth_enable = yes`
    14. `smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks, reject_unauth_destination`
    15. `smtp_tls_security_level = may`
    16. `smtpd_tls_security_level = may`
    17. `smtp_tls_note_starttls_offer = yes`
    18. `smtpd_tls_loglevel = 1`
    19. `smtpd_tls_key_file = /etc/letsencrypt/live/<domain>.<tld>/privkey.pem`
    20. `smtpd_tls_cert_file = /etc/letsencrypt/live/<domain>.<tld>/fullchain.pem`
    21. `smtpd_tls_received_header = yes`
    22. `smtpd_tls_session_cache_timeout = 3600s`

23. `smtpd_use_tls=yes`
24. `tls_random_source = dev:/dev/urandom`
25. `virtual_alias_domains = <domain>.<tld>`
26. `virtual_alias_maps = hash:/etc/postfix/virtual`

2. Find and uncomment the following lines in `/etc/postfix/main.cf`:
    1. `#inet_interfaces = localhost`
    2. `#mydestination = $myhostname, localhost.$mydomain, localhost`
3. Append the following lines to `/etc/postfix/master.cf`:
    1. `submission inet n - n - - smtpd`
    2. `-o syslog_name=postfix/submission`
    3. `-o smtpd_sasl_auth_enable=yes`
    4. `-o smtpd_recipient_restrictions=permit_sasl_authenticated,reject_unauth_destination`
    5. `-o milter_macro_daemon_name=ORIGINATING`
    6. `smtps inet n - n - - smtpd`
    7. `-o syslog_name=postfix/smtps`
    8. `-o smtpd_sasl_auth_enable=yes`
    9. `-o smtpd_recipient_restrictions=permit_sasl_authenticated,reject_unauth_destination`
    10. `-o milter_macro_daemon_name=ORIGINATING`
4. Make sure that the following is present in `/etc/postfix/main.cf`:
    1. `alias_maps = hash:/etc/aliases`
5. Edit and add the desired email address to `/etc/postfix/virtual` such as the following:
    1. `info@<domain>.<tld> admin`
    2. `webmaster@<domain>.<tld> admin`
6. Create a map database: `postmap /etc/postfix/virtual`

Dovecot Configuration

1. Find and modify the following lines in `/etc/dovecot/conf.d/10-master.conf`:
    1. `# Postfix smtp-auth`
    2. `unix_listener /var/spool/postfix/private/auth {`
    3. `mode = 0660`
    4. `user = postfix`
    5. `group = postfix`
    6. `}`
2. Find and modify the following lines in `/etc/dovecot/conf.d/10-auth.conf`:
    1. `auth_mechanisms = plain login`
3. Find and modify the following lines in `/etc/dovecot/conf.d/10-mail.conf`:
    1. `mail_location = maildir:~/mail`
4. Find and modify the following lines in `/etc/dovecot/conf.d/20-pop3.conf`:
    1. `pop3_uidl_format = %08Xu%08Xv`
5. Find and modify the following lines in `/etc/dovecot/conf.d/10-ssl.conf`:
    1. `ssl_cert = </etc/letsencrypt/live/<domain>.<tld>/fullchain.pem`
    2. `ssl_key = </etc/letsencrypt/live/<domain>.<tld>/privkey.pem`

Restart and Enable Services

1. `systemctl restart postfix`
2. `systemctl enable postfix`
3. `systemctl restart dovecot`
4. `systemctl enable dovecot`

Open Firewall Ports

1. `firewall-cmd --permanent --add-service=smtp`
2. `firewall-cmd --permanent --add-port=587/tcp`
3. `firewall-cmd --permanent --add-port=465/tcp`
4. `firewall-cmd --permanent --add-port=110/tcp`
5. `firewall-cmd --permanent --add-service=pop3s`
6. `firewall-cmd --permanent --add-port=143/tcp`
7. `firewall-cmd --permanent --add-service=imaps`
8. `firewall-cmd --reload`

Configure DNS

1. Add an `A` record for the mail server:
    1. `name = mail.<domain>.<tld>`
    2. `IP = <mail server IP>`
2. Add an `MX` record:
    1. `Hostname = mail.<domain>.<tld>`
    2. `Priority = 5`
3. Add the following `TXT` records:
    1. `Name = @`
    2. `Text = "v=spf1 ip4:<domain IP> ~all"`
    3. `Name = _dmarc.<domain>.<tld>`
    4. `Text = v=DMARC1; p=none`
4. Add `PTR` record for `<domain>.<tld>`
5. Finally, test your email at `https://www.mail-tester.com/`

Notes on Using Let's Encrypt for SSL

Make sure that `Encryption` is set to `STARTTLS` when configuring mail clients

References

1. Krizna Article
2. Ubuntu Postfix Alias Configuration

Server Software

Install RethinkDB on CentOS 7

Installing RethinkDB

```
sudo wget http://download.rethinkdb.com/centos/7/`uname -m`/rethinkdb.repo -O
/etc/yum.repos.d/rethinkdb.repo
sudo yum install rethinkdb
```

Create Service File

Create the service file, `/usr/lib/systemd/system/rethinkdb@.service` with the following content:

```
[Unit]
Description=RethinkDB database server for instance '%i'

[Service]
User=rethinkdb
Group=rethinkdb
ExecStart=/usr/bin/rethinkdb serve --config-file /etc/rethinkdb/instances.d/%i.conf
KillMode=process
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

Make sure that it has a permission of `644`: `chmod 644 /usr/lib/systemd/system/rethinkdb@.service`

Creating a Rethink DB Instance

1. Create the RethinkDB data directory: `rethinkdb create -d /path/to/your/rethinkdb/directory`
2. Set the ownership to RethinkDB user: `sudo chown -R rethinkdb. rethinkdb /path/to/your/rethinkdb/directory`
3. Copy RethinkDB sample config file: `sudo cp /etc/rethinkdb/default. conf. sample /etc/rethinkdb/instances. d/instance1. conf`
4. Edit `/etc/rethinkdb/instances. d/instance1. conf`, the line with `directory=` must be changed to point to your Rethink DB data directory.

Start RethinkDB Instance

in this case would be `instance1`:

```
sudo systemctl enable rethinkdb@<name_instance>
sudo systemctl start rethinkdb@<name_instance>
```

References

RethinkDB Startup Doc

Turtl API Server and Client Installation CentOS 7

Turtl API

Clone and Configure Turtl API

1. Create a user for turtl API: `sudo useradd turtl`
2. Switch user to `turtl`: `sudo su turtl`
3. Change directory to `turtl`'s home: `cd ~`
4. Install Clozure CL
5. Install RethinkDB and create an instance for Turtl API
6. Install `libuv`: `sudo yum install libuv`
7. Clone Turtl repo: `git clone https://github.com/turtl/api.git`
8. Copy Turtl API config: `cp config/config.default.lisp config/lisp`
9. Edit and configure `config/config.lisp`, make sure to update the following parameters:

```
(defvar *local-upload* "<local upload directory>"
(defvar *local-upload-url* "<upload url>"
```

Setup Up Service

Create a service file at `/usr/lib/systemd/system/turtl.service` with the following entry:

```
[Unit]
Description=Turtl API Server

[Service]
User=turtl
Group=turtl
ExecStart=/usr/local/bin/ccl64 --load /home/turtl/api/start.lisp
```

```
KillMode=process

[Install]
WantedBy=multi-user.target
```

Start and enable the service:

```
sudo systemctl start turtl
sudo systemctl enable turtl
```

(OPTIONAL) Configure Reverse Proxy in Apache

Create `httpd` virtual host configuration `/etc/httpd/conf.d/turtl.conf` with the following content, make sure to change `<turtl domain>` to your own domain name:

```
<VirtualHost *:80>
    #Server name configuration
    ServerName <turtl domain>
    ServerAdmin webmaster@<turtl domain>

    #Proxy configuration
    ProxyPreserveHost on
    ProxyRequests off
    ProxyPass / https://wiki.twcloud.tech:8181/
    ProxyPassReverse / https://wiki.twcloud.tech:8181/

    #Logging configuration
    ErrorLog /var/log/httpd/turtl.err
    LogLevel warn
</VirtualHost>
```

(OPTIONAL) Restrict User Registration

Add the following lines in your Turtl API Virtual Hosts configuration:

```
    #Restrict Registration
    <LocationMatch  "^/users[/]?$">
```

```
        AuthType Basic
        AuthName "Restricted"
        AuthUserFile /home/turtl/.htpasswd
        Require valid-user
    </LocationMatch>
```

Then generate a `.htpasswd` password file in `/home/turtl`: `sudo htpasswd -c /etc/apache2/.htpasswd <whatever username>`. Make sure that it's in the right permission and owner: `chmod 640 /home/turtl/.htpasswd && chown turtl:apache /home/turtl/.htpasswd`

Installing JS Client

1. Clone `turtl/js` repo to webserver webroot: `sudo mkdir /var/www/turtl && cd /var/www/turtl && sudo git clone https://github.com/turtl/js.git .`
2. Install NodeJS dependencies: `npm install`
3. Copy default config: `cp config/config.js.default config.js`
4. Edit `config/config.js`
5. Update owner and group: `chown -R apache:apache .`
6. Generate assets: `make`

Software Development

All about software development tricks on Linux

Software Development

Creating War File in Linux

1. CD to war directory in the project folder
2. Execute `jar -cvf .war *`

Software Development

Standard Procedures for CakePHP Application Deployment

1. Clone Source File

1. `git clone <git url>`

2. Setup Database

1. `mysql -uroot -p`
2. `create database <database name>;`
3. `grant all on <database name>.* to '<id>'.'localhost' identified by '<password>';`
4. `cd <path/to/cakephp>/app`
5. `Console/cake schema create`
6. `Console/cake schema update -s <update number found in app/Config/Schema/>`

3. Setup PHP

Edit `/etc/php.ini` and add the following line:

1. `date.timezone = "Asia/Kuala_Lumpur"`

4. Allow Write Access to tmp

1. `chmod -R 777 app/tmp/`

5. Setup Apache

Edit `/etc/httpd/conf/conf.d` and change `AllowOverride None` to `AllowOverride All` in `<Directory "/var/www/html">` tag. Then, restart httpd:

1. `sudo systemctl restart httpd`

(OPTIONAL) SELinux

1. `sudo setsebool -P allow_httpd_anon_write on`
2. `sudo setsebool -P allow_httpd_sys_script_anon_write on`
3. `sudo setsebool -P httpd_unified 0`
4. `sudo chcon -R -t httpd_sys_rw_content_t <path_to_cakephp_app>/app/tmp/`

Software Development

Installing Clozure CL and QuickLisp on CentOS 7

Download Clozure CL

Open up terminal and enter the command: `svn co http://svn.clozure.com/publicsvn/openmcl/release/1.11/linuxx86/ccl` Where `linuxx86` is one of:

- `darwinx86`
- `linuxx86`
- `freebsdx86`
- `solarisx86`
- `windows`
- `linuxarm`

Download and Install QuickLisp

1. Download QuickLisp from https://beta.quicklisp.org/quicklisp.lisp
2. Enter the command: `./ccl/lx86cl64 --load /path/to/quicklisp.lisp`
3. In the CCL prompt enter: `(quicklisp-quickstart:install)(ql:add-to-init-file)`

Creating Scripts to Run CCL

1. Edit `./ccl/scripts/ccl` and `./ccl/scripts/ccl64` to change `CCL_DEFAULT_DIRECTORY=/usr/local/src/ccl` line to `CCL_DEFAULT_DIRECTORY=~/ccl`
2. Copy the scripts to `/usr/local/bin` directory: `sudo cp ./ccl/scripts/ccl* /usr/local/bin/`

References

- Linux Format Article
- Clozure CL Official Download Page

Sound

Linux sound problems, configuration and installation

No Sound over Wine

Install `lib32-alsa-plugins lib32-libpulse lib32-openal`

Sound

E: [pulseaudio] module.c: Failed to load module "module-equalizer-sink" (argument: ""): initialization failed.

Symtoms

Starting pulseaudio will forever `Establishing connection`, `pulseaudio -v` will reveal the following errors:

```
W: [pulseaudio] module-equalizer-sink.c: module-equalizer-sink is currently unsupported, and can sometimes cause PulseAudio crashes, increased latency or audible artifacts.
W: [pulseaudio] module-equalizer-sink.c: If you're facing audio problems, try unloading this module as a potential workaround.
E: [pulseaudio] module-equalizer-sink.c: Master sink not found
E: [pulseaudio] module.c: Failed to load module "module-equalizer-sink" (argument: ""): initialization failed.
E: [pulseaudio] main.c: Module load failed.
E: [pulseaudio] main.c: Failed to initialize daemon.
I: [pulseaudio] main.c: Daemon terminated.
```

Solution

Start pulseaudio using Desktop Manager's autostart script, the following instruction is for LXDE:

1. Create a desktop file on `~/.config/autostart/pulseaudio-equalizer.desktop`
2. Add the following lines:

```
[Desktop Entry]
Type=Application
Exec=bash -c 'pactl load-module module-equalizer-sink; pactl load-module module-dbus-protocol;'
```

References

- PulseAudio Wiki
- Archwiki's PulseAudio Troubleshooting

Storage

Storage administration and tricks, including LVM, SCSi etc.

Storage

LVM Extending from New Physical Volume

Create new physical volume from new partition

1. Use `fdisk` utility to create new partition
2. `pvcreate /dev/<new partition>`
3. `pvs`

Adding physical volume to volume group

1. `vgextend <volume group> /dev/<new partition>`

Extending logical volume

1. `lvextend -L+<size><G or M> /dev/<volume group>/<lv name>`
2. `#For XFS:`
3. `xfs_grow /<mount_point>`
4. `#For EXT4:`
5. `resize2fs /<mount>/<point>`

System

Linux system tools, administration and tips

System

ArchLinux Upgrade Issues

Error: key "ABCDE1282828181" could not be looked up remotely

Upgrade archlinux-keyring: `pacman -S archlinux-keyring`

Unable to get past login window after upgrading

This is caused by Nvidia driver being upgraded

nvidia-dkms: `pacman -S nvidia-libgl`

Failed to start load kernel modules after upgrade:

Possible causes:

- `broadcom-wl` module
- Solved by re-"makepkg" `broadcom-wl` from **AUR**
- Find error message in `systemctl status systemd-modules-load.service`

System

CentOS Installation Issues

HP Microserver Gen 7

Kernel Panic on Boot (Both Live USB and New Installation)

Add the following lines to the kernel boot parameters: `nolapic clocksource=hpet`

Blank Screen on Startup

Append `nomodeset` to kernel param

System

Changing Default S2RAM to USWSUSP Suspend Module

If you have any issues to suspend your laptop e.g. `suspend` command doesn't work on your laptop, try changing the default sleep module to `uswsusp`:

1. Edit `/etc/pm/config.d/module` and add the following line: `SLEEP_MODULE=uswsusp`
2. Edit `/etc/pm/config.d/defaults` and add the following line: `S2RAM_OPTS="-f"`
3. Reboot and try to let her sleep.

References

- OpenSuse Documentation on Suspending
- AskUbuntu Thread

System

Fixing Incorrect Lid State by Hacking DSDT

When I install a Linux distro to my VAIO notebook, I found that there is an annoying bug with the lid switch. It does not get updated whenever I suspend on lid close, it means `cat /proc/acpi/button/lid/LID/state` will output `state: close`. When I close the lid again, it won't suspend, instead, it will change the state to open. So in order for it to suspend again on lid close after the first suspend, I have to close it, reopen the lid and close it again.

I have tried installing Linux Mint, Fedora, Fuduntu and Xubuntu, but it is not fixed in any of the distros. So, I don't think it is distro problems. While researching this issues (which I spent two full days), I found that Linux got an amazing feature that enable users to dynamically loading DSDT at boot time, there is no need to update the BIOS. So here's the instuctions:

1. Install `iasl` using `yum`, `apt-get` or whatever package management you are using.
2. Extract DSDT:

```
$ sudo cat/sys/firmware/acpi/tables/DSDT > dsdt.aml
```

3. Disassemble `dsdt.aml` using the following command, this should create a new file `dsdt.dsl`:

```
$ iasl -d dsdt.aml
```

4. Compile it using:

```
$ iasl -tc dsdt.dsl
```

5. Fix any compiler errors, warnings and remarks. On my machine, the output is:

```
dsdt.dsl  1352:                            And (CTRL, 0x1E)
Warning  1106 -                                    ^ Result is not used, operator has no
effect

dsdt.dsl  1584:                        0x00000000,         // Length
Error    4122 -                                ^ Invalid combination of Length and
Min/Max fixed flags
```

```
dsdt.dsl  2443:                                  Name (_T_0, 0x00)
Remark   5111 -            Use of compiler reserved name ^  (_T_0)


dsdt.dsl  2521:                                  Name (_T_0, 0x00)
Remark   5111 -            Use of compiler reserved name ^  (_T_0)
```

a. The first one is on line 1352 can be fixed simply by changing `And (CTRL, 0x1E)` to `And (CTRL, 0x1E, CTRL)`.
b. The second one is on line 1584, the length should be `Range Maximum` - `Range Minimum` + 1, on my machine, so fire up a hex calculator and start subtracting. On my machine, it's `0xE0000000` (`0xDFFFFFFF` - `0x00000000` + `0x00000001`).
c. The third and fourth line is on line 2443 and 2521, because it uses a reserved name, simply replacing all instances of `_T_0` to `T_0` will stop the complaints. In vim, it is as simple as issuing `:%s/_T_0/T_0/g` in command mode.

6. Once everything is fixed (no errors, warning or remarks), add the following line to `_WAK` method, simply search for `_WAK` in `dsdt.dsl`:

```
If (LNotEqual (0x00, LIDS))
{
Store (0x00, LIDS)
Notify (\_SB.LID, 0x80)
}
```

NOTE 1: You might need to change `\_SB.LID` to match your path to `LID` method or on some machine `LID0`. Method name is preceded by an `_` (underscore), so you can search for `_LID` in `dsdt.dsl`. After you found it, you have to determine the scope, scroll up until you found `Scope` keyword that your `LID` or `LID0` method belongs to, inside the bracket is the scope name. It may be in more than one scope, so, it might be `\_PCI0.SB.LID`. If you specify an incorrect path to `LID` method, you will receive the following error:

```
dsdt.dsl 300:  Notify (LID, 0x80)
Error 4068 - ^ Object is not accessible from this scope (LID_)
```

NOTE 2: What this function does is just to update the lid state once it is resumed from sleep. According to the ACPICA documentation, `_WAK` method is called by `AcpiLeaveSleepState()` function of ACPI. If the lid is open, the `LIDS` variable is `0x00`, or `0x01` otherwise. So these few lines translate to "if lid state is not open (closed), change lid state to open and call `LID` method".

7. Compile it using `iasl -tc dsdt.dsl`.
8. If no errors, warnings or remarks, add the following lines to `/etc/grub.d/01_acpi`:

```
# Uncomment to load custom ACPI table
GRUB_CUSTOM_ACPI="/boot/dsdt.aml"
```

```
# DON'T MODIFY ANYTHING BELOW THIS LINE!

prefix=/usr
exec_prefix=${prefix}
libdir=${exec_prefix}/lib

. /usr/share/grub/grub-mkconfig_lib
#. ${libdir}/grub/grub-mkconfig_lib

# Load custom ACPI table
if [ x${GRUB_CUSTOM_ACPI} != x ] && [ -f ${GRUB_CUSTOM_ACPI} ] \
   && is_path_readable_by_grub ${GRUB_CUSTOM_ACPI}; then
   echo "Found custom ACPI table: ${GRUB_CUSTOM_ACPI}" >&2
   prepare_grub_to_access_device `${grub_probe} --target=device
${GRUB_CUSTOM_ACPI}` | sed -e "s/^/  /"
   cat << EOF
acpi (\$root)`make_system_path_relative_to_its_root
${GRUB_CUSTOM_ACPI}`
EOF
fi
```

9. Add executable bit to it:

```
$ sudo chmod +x /etc/grub.d/01_acpi
```

10. Copy the new `dsdt.aml` to `/boot`:

```
$ sudo cp dsdt.aml /boot
```

11. Regenerate `grub.cfg`:

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

12. Reboot

References

- Archwiki on DSDT
- Redhat's Bug Report
- Ubuntu's Bug Report 1
- Ubuntu's Bug Report 2

- Somebody's blog on fixing DSDT errors, remarks and warnings
- ACPICA Documentation

JournalD Administration

Optimizing JournalD Disk Space Usage

Edit `/etc/systemd/journald.conf` and change the following line:

```
SystemMaxUse=200M
```

To check disk space used by journald: `journalctl --disk-usage`

System

Linux on Macbook Administration

Blessing the Linux Kernel

1. Boot into Mac Recovery
2. Start terminal and enter:
3. `bless --folder /Volumes/ARCH_EFI/EFI/arch/grub/ --file /Volumes/ARCH_EFI/EFI/arch/grub/grub`

Changing Apple keyboards (Macbook or USB) fnmode in Linux

Changing it temporarily, as root:

```
echo 2 > /sys/module/hid_apple/parameters/fnmode
```

Changing it Permanently:

Edit `/etc/modprobe.d/hid_apple.conf` and add the following line:

```
options hid_apple fnmode=2
```

System

SELinux - Services Blocked by SELinux

SELinux Blocked Apache Access to Files

```
setsebool -P httpd_unified 1
sudo /sbin/restorecon -R /var/www/html
```

VSFTPD OOPS Error

Issue the following command: `setsebool -P ftp_home_dir 1`

SSH bind port error permission denied

Issue the following command: `semanage port –a –t ssh_port_t –p tcp 1234`

Permission denied HTTP Error 403

Issue the following command: `chcon -R --reference=/var/www /path/to/webroot`

SELinux Denied HTTPD Access to MYSQLD on 127.0.0.1

1. `grep mysqld /var/log/audit/audit.log | audit2allow -M mysqld`
2. `semodule -i mysqld.pp`

SELinux Denied FTP Access to SMB Share

1. Try to login with ncftp first and you will see the error "`OOPS: cannot change directory: /path/to/samba_share`"
2. Execute command: `su -c "grep ftpd_t /var/log/audit/audit.log | allow2audit -M ftpd_smb && semodule -i ftpd_smb"`
3. Try to login again with ncftp and ls command will return empty list a although it isn't
4. Execute command: `su -c "grep ftpd_t /var/log/audit/audit.log | allow2audit -M ftpd_smb && semodule -i ftpd_smb"`
5. Execute command => `sudo setsebool -P allow_ftpd_full_access on`
6. Execute command => `sudo setsebool -P ftp_home_dir on`

Owncloud Custom Data Directory Denied

Assume owncloud data directory: `/var/data`

```
Install policycoreutils-python
/etc/init.d/restorecond start
chkconfig restorecond on
semanage fcontext -a -t httpd_sys_content_t '/var/data(/.*)?'
restorecon -Rv /var/data
```

System

Standard CentOS Workstation Setup

Install GUI (MATE Desktop)

1. `sudo yum install epel-release`
2. `sudo yum groupinstall 'X Window System'`
3. `sudo yum groupinstall 'MATE Desktop'`
4. `sudo systemctl isolate graphical.target`
5. `sudo systemctl set-default graphical.target`

Install Printer

1. `sudo yum install cups`
2. `sudo yum groupinstall "Development Tools"`
3. `sudo systemctl enable cups`
4. `sudo systemctl start cups`
5. `sudo yum install foomatic`

Install drivers for the printer available at Open Printing

Optional - GUI WiFi Support

1. `sudo yum install NetworkManager-wifi`

Ansible

Contains everything on Ansible IT automation tool, playbooks and tricks

Playbook - Clearing Users' Data Files in a Group of Windows Machines

The playbook below will remove all users' data in a computer that belongs in an inventory group. Below is a list of steps that this playbook will do:

1. Disable and remove the target user
2. Reboot to remove any file locks from the logged in user
3. Remove any files in the user's directory, skipping symbolic links
4. Re-create a public user with the same username and empty password that cannot be changed
5. Enable auto login for the user so that new machine will be configured for auto login as well
6. Reboot computer to enable the configuration

The playbook is as follows, please change the variables encapsulated in `< >` with the desired values:

```
---
- hosts: <inventory group / host>
  tasks:
  - name: remove user account
    win_user:
      name: <username>
      account_disabled: yes
      state: absent
  - name: reboot
    win_reboot:
      msg: "Scheduled reset started, windows will reboot in 90 seconds"
      pre_boot_delay: 90
  - name: remove any files in the folder tree
    ignore_errors: yes
    win_shell: |
```

```
      $Path = "C:\Users\<username>"
      Remove-Item "$Path" -Force -Recurse -ErrorAction SilentlyContinue
      if (Test-Path "$Path" -ErrorAction SilentlyContinue)
      {
          $folders = Get-ChildItem -Path $Path -Directory -Force -ErrorAction SilentlyContinue
          ForEach ($folder in $folders)
          {
              Remove-Tree $folder.FullName -Force -ErrorAction SilentlyContinue
          }

          $files = Get-ChildItem -Path $Path -File -Force
          ForEach ($file in $files)
          {
              Remove-Item $file.FullName -Force -ErrorAction SilentlyContinue
          }

          if (Test-Path "$Path" -ErrorAction SilentlyContinue)
          {
              Remove-Item $Path -Force -ErrorAction SilentlyContinue
          }
      }
  - name: re-add user account
    win_user:
      name: <username>
      state: present
      groups: Users
      user_cannot_change_password: yes
      password_expired: no
      password_never_expire: yes
  - name: enable auto logon
    win_shell: |
      Set-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name
'AutoAdminLogon' -Value '1'
      Set-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name
'DefaultUsername' -Value '<default username>'
      Set-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' -Name
'DefaultPassword' -Value ''
  - name: reboot to apply new settings
    win_reboot:
      msg: "Scheduled reset completed, windows will reboot in 5 seconds"
```

```
    pre_boot_delay: 5
```

References:

- https://luke.geek.nz/win/using-powershell-setup-automatic-logon-windows-servers/
- https://stackoverflow.com/a/31450526
- https://docs.ansible.com/ansible/2.5/modules/list_of_windows_modules.html

Ansible

Playbook - Update Windows Machine (Windows Update Disabled)

This playbook will:

1. Modify windows update service to manual in case the machine is set to disabled
2. Start the windows update service
3. Download and install the updates, reboot if required

The playbook is as follows, please change the encapsulated `< >` values to the desired values:

```
---
- hosts: <inventory group / hosts>
  tasks:
  - name: change windows update service to manual
    win_shell: Set-Service wuauserv -StartupType Manual
  - name: start windows update service
    win_shell: Start-Service wuauserv
  - name: download and install updates
    win_updates:
      reboot: yes
```

Ansible

Playbook - Initiate Clamscan on Machines with ClamWin Installed

This playbook will initiate a full scan on all computers using `Clamscan` that is installed through `ClamWin`:

```
---
- hosts: <inventory group / hosts>
  tasks:
  - name: full computer scan
    win_command: '"C:\Program Files (x86)\ClamWin\bin\clamscan.exe" -rv --
move=C:\ProgramData\.clamwin\quarantine\ --database=C:\ProgramData\.clamwin\db\ --
log=C:\ProgramData\.clamwin\log\ClamScanLog.txt --enable-stats C:\'
```

Playbook - Disable Windows Updates

This playbook will download disable_windows_update.ps1 from a server, reachable by all clients and execute the script to disable windows updates on a group of windows machines. Though it is written to specifically disable windows update, it can be modified to execute other scripts as well. The playbook configuration file is ass follows, replace enclosed `< >` tags with the desired values:

```
---
- hosts: <inventory group / hosts>
  tasks:
  - name: download script to disable windows update
    win_get_url:
      url: http://<url>/disable_windows_update.ps1
      dest: C:\
  - name: execute disable windows update script
    win_shell: C:\disable_windows_update.ps1
  - name: remove script
    win_file:
      path: C:\disable_windows_update.ps1
      state: absent
```