LinuxFest Northwest

2017

Secure Cloud: Linode With Full Disk Encryption

Roberto C. Sánchez

Spoiler: The Solution Is, "Full Disk Encryption"

About the Presenter

- I am a software engineer and consultant

- I have been programming since 1990

- I have been active in FOSS since 2002

- I teach Computer Science/Engineering at Wright State University (Dayton, OH)

- Find me here:
  http://www.linkedin.com/in/robertocsanchez/

Outline

- Linux virtual server encryption options
- Threats mitigated by each encryption option
- Pros/cons of a Linux virtual server with FDE
- Types of protection FDE does/does not provide
- HOWTO: Deploy a Linode with FDE
- Unique issues associated with managing a Linux virtual server with FDE

Encryption Options

- **File-based encryption**

  - Encrypt specific files (when not in use)

- **Encrypted volumes**

  - / and /boot remain unencrypted

  - Key volumes (e.g., /home, /var/lib/postgresql, /var/spool/postfix, etc.) get encrypted

- **Full disk encryption (encrypt everything)**

  - Only /boot remains unencrypted (can't boot encrypted kernel)

  - / and all other filesystems are encrypted

Common Issues

- More encryption == less convenience
- Managing encryption keys
- Providing passphrases when needed

File-Based Encryption

- Protects only specific files

- Files must be decrypted somewhere in order to be used

- Requires you to pick and choose which files to protect

- Less likely to impede the boot process

Encrypted Volumes

- Protects all files under the encrypted mount point/directory (when offline)

- Encrypted filesystem/volume cannot be mounted without providing passphrase/key

- Depending on which mount points/directories are encrypted, boot process may be affected

- Launching of certain services may have to be delayed until encrypted volumes are decrypted

Full Disk Encryption

- Protects all files on the system (when off)

- System cannot be booted without providing key/passphrase

Virtual Server FDE Pros/Cons

- Pros
  - Provides excellent protection against many physical attacks (especially if the server is off)
  - Practically eliminates "leakage" through temporary files and swap (they are encrypted as well)
- Cons
  - Deployment requires non-standard steps which may not be well supported
  - Deployment could be more difficult to automate
  - Boot process stops until passphrase is entered

Types of Protection From FDE

- Protected against:
  - Bad actor physically removing disk drive(s)
  - Bad actor taking a filesystem image
  - Physical relocation of server
- Probably not protected against:
  - Compromise through a vulnerable running process (e.g., httpd, sshd, etc.)
  - Malicious user in control of physical host (e.g., super user, intruder, etc.) while virtual server is on
  - Inspection of memory areas from hypervisor environment (see previous item)
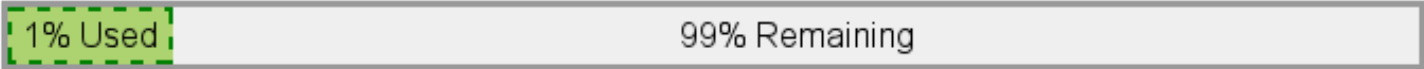
HOWTO: Linode With FDE

Linodes

Linode	Status	Plan	IP	Location	Backups	Options
node01	Running	Linode 4096		Newark, NJ, USA	**No** - Enable	**Dashboard** | Remove
node02	Running	Linode 4096		Dallas, TX, USA	**No** - Enable	**Dashboard** | Remove

Manage Images | Manage StackScripts | Add a Linode

This Month's Network Transfer Pool

1% Used	99% Remaining

1GB Used, 5999GB Remaining, 6000GB Quota

Select an instance type

Standard Instances

Linode 1024	Linode 2048	Linode 4096	Linode 8192	Linode 12288
20GB Storage	30GB Storage	48GB Storage	96GB Storage	192GB Storage
1 CPU Core	1 CPU Core	2 CPU Cores	4 CPU Cores	6 CPU Cores
1TB XFER	2TB XFER	3TB XFER	4TB XFER	8TB XFER
$5/mo or (.0075/hr)	$10/mo or (.015/hr)	$20/mo or (.03/hr)	$40/mo or (.06/hr)	$80/mo or (.12/hr)

Linode 24576	Linode 49152	Linode 65536	Linode 81920	
384GB Storage	768GB Storage	1152GB Storage	1536GB Storage	
8 CPU Cores	12 CPU Cores	16 CPU Cores	20 CPU Cores	
16TB XFER	20TB XFER	20TB XFER	20TB XFER	
$160/mo or (.24/hr)	$320/mo or (.48/hr)	$480/mo or (.72/hr)	$640/mo or (.96/hr)	

High Memory Instances

Linode 16384	Linode 32768	Linode 61440	Linode 102400	Linode 204800
20GB Storage	40GB Storage	90GB Storage	200GB Storage	340GB Storage

5TB XFER	6TB XFER	7TB XFER	8TB XFER	9TB XFER
$60/mo or (.09/hr)	$120/mo or (.18/hr)	$240/mo or (.36/hr)	$480/mo or (.72/hr)	$960/mo or (1.44/hr)

Location

Fremont, CA

Add this Linode!

Linodes

| Linode	Status	Plan	IP	Location	Backups	Options
linode3073559	Being Created	Linode 1024	192.81.130.199	Fremont, CA, USA	**No** - Enable	**Dashboard** | Remove
node01	Running	Linode 4096		Newark, NJ, USA	**No** - Enable	**Dashboard** | Remove
node02	Running	Linode 4096		Dallas, TX, USA	**No** - Enable	**Dashboard** | Remove

Manage Images | Manage StackScripts | Add a Linode

This Month's Network Transfer Pool

1% Used	99% Remaining
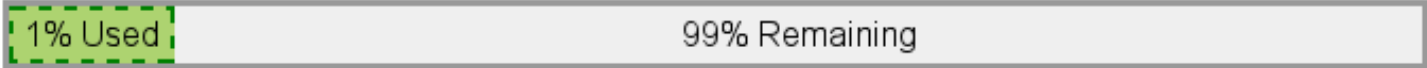
1GB Used, 6863GB Remaining, 6864GB Quota

Your transfer is prorated and will reset next month

Linodes » **linode3073559**

Dashboard

Select	Configuration Profiles	Options

Rebuild | Deploy an Image | Create a new Configuration Profile

Disks

Create a new Disk

Host Job Queue (more)

Success   **Linode Initial Configuration**
Entered: 3 minutes 43 seconds ago - Took: 0 seconds

Graphs

Server Status

Your Linode is currently

Brand New

Network

- Transfer/mo: 1000 GB
- Incoming: 0 bytes
- Outgoing: 0 bytes
- Total: 0 bytes

You have used

0%

of your monthly transfer

Storage

- Total: 20480 MB
- Used: 0 MB
- Free: 20480 MB

Linodes » linode3073559 » **Edit Disk**

Edit Disk

Label   boot

Type   ext4

Size   256   MB   Enter a size between 1 and 20480

Save Changes

Storage Stats

0 MB	20480 MB	20480 MB
Allocated	Free	Total

Dashboard   Remote Access   Rebuild   Rescue   Resize   Clone   Graphs   Backups   Settings

Linodes » linode3073559 » **Edit Disk**

Edit Disk

Label   swap

Type   swap

Size   2048   MB   Enter a size between 1 and 20224

Save Changes

Storage Stats

256 MB	20224 MB	20480 MB
Allocated	Free	Total

Linodes » linode3073559 » **Edit Disk**

Edit Disk

Label	root
Type	ext4
Size	18176 MB

Enter a size between 1 and 18176

Save Changes

Storage Stats

2304 MB	**18176 MB**	**20480 MB**
Allocated	Free	Total

Dashboard

Select	Configuration Profiles	Options

Rebuild | Deploy an Image | Create a new Configuration Profile

Disks

boot (256 MB, ext4)   Edit | Remove

swap (2048 MB, swap)   Edit | Remove

root (18176 MB, ext4)   Edit | Remove

Create a new Disk

Host Job Queue (more)

Success   **Create Filesystem** - root
Entered: 11 seconds ago - Took: 1 second

Dashboard

Select	Configuration Profiles	Options
		Rebuild | Deploy an Image | Create a new Configuration Profile

Disks

boot (256 MB, ext4)	Edit | Remove
swap (2048 MB, swap)	Edit | Remove
root (18176 MB, ext4)	Edit | Remove
	Create a new Disk

Host Job Queue (more)

Success   **Create Filesystem** - root
Entered: 11 seconds ago - Took: 1 second

Linodes » linode3073559 » **Edit Configuration Profile**

Configuration Profile

Label and Notes

Label   Debian Jessie w/ FDE   ←

Notes

Virtual Machine Mode

VM Mode   ⦿ Paravirtualization   ←   Controls if devices inside your virtual machine are paravirtualized or fully virtualized.
               ○ Full-virtualization   Paravirt is what you want, unless you're doing weird things.

Boot Settings

Kernel   GRUB 2   ←

Run Level   ⦿ Default Run Level   ←
                 ○ Single user mode
                 ○ init=/bin/bash

Memory Limit   ○ Limit to [0] MB
                    ⦿ Maximum (1024 MB)   ←

Block Device Assignment

Block Device Assignment

/dev/sda	boot ⬅
/dev/sdb	swap ⬅
/dev/sdc	root ⬅
/dev/sdd	--
/dev/sde	--
/dev/sdf	--
/dev/sdg	--
/dev/sdh	--
initrd	-- No initrd --

root / boot device
- ● Standard: /dev/sda ⬅
- ○ Custom: [   ]

Filesystem/Boot Helpers

Distro Helper	○ Yes ● No ⬅	Helps maintain correct inittab/upstart console device
Disable updatedb	○ Yes ● No ⬅	Disables updatedb cron job to avoid disk thrashing
modules.dep Helper	○ Yes ● No ⬅	Creates a modules dependency file for the kernel you run
Automount devtmpfs	○ Yes ● No ⬅	Controls if pv_ops kernels automount devtmpfs at boot
Auto-configure Networking	○ Yes ● No ⬅	Automatically configure static networking (more info)

[Save Changes] ⬅

Linodes » **linode3073559**

Dashboard

Select	Configuration Profiles	Options
⊙	**Debian Jessie w/ FDE** (GRUB 2)	Edit | Remove
Boot		Rebuild | Deploy an Image | Create a new Configuration Profile

Disks

📀	**boot** (256 MB, ext4)	Edit | Remove
📀	**swap** (2048 MB, swap)	Edit | Remove
📀	**root** (18176 MB, ext4)	Edit | Remove
		Create a new Disk

Host Job Queue (more)

Success	**Create Filesystem** - root
	Entered: 12 minutes 34 seconds ago - Took: 1 second

Linodes » linode3073559 » **Rescue**

Rescue Mode

Boots your Linode into Rescue Mode. Access it via the console.

/dev/sda	boot
/dev/sdb	swap
/dev/sdc	root
/dev/sdh	Finnix Media

Reboot into Rescue Mode

Dashboard

Select	Configuration Profiles	Options
⊙	Debian Jessie w/ FDE (GRUB 2)	Edit | Remove

Reboot   Rebuild | Deploy an Image | Create a new Configuration Profile

Disks

💾	boot (256 MB, ext4)	Edit | Remove
💾	swap (2048 MB, swap)	Edit | Remove
💾	root (18176 MB, ext4)	Edit | Remove

Create a new Disk

Host Job Queue (more)

Success	**System Boot** - Rescue Mode
	Entered: 26 seconds ago - Took: 4 seconds
Success	**System Shutdown**
	Entered: 26 seconds ago - Took: 0 seconds
Success	**Create Filesystem** - root
	Entered: 16 minutes 1 second ago - Took: 1 second

Server Status

Your Linode is currently

Running

Shut down

1 day uptime

Network

- Transfer/mo: 1000 GB
- Incoming: 0 bytes
- Outgoing: 0 bytes
- Total: 0 bytes

You have used

0%

of your monthly transfer

Storage

- Total: 20480 MB
- Used: 20480 MB
- Free: 0 MB

You have allocated

100%

towards disk images

Utilizing lish and Finnix

- You need to ssh into the lish console at the data center where you created your Linode

- The lish console is really GNU screen

- If you are not familiar with GNU screen, then press 'Control-A' followed by '?' for help

File   Edit   View   Search   Terminal   Help

```
roberto@miami:~$ ssh         @lish-fremont.linode.com
Linux lish-fremont.linode.com 4.8.3-x86_64-linode76 #1 SMP Thu Oct 20 19:05:39 E
DT 2016 x86_64
Linodes located in this data center:
linode3073559          Fremont, CA

Linodes located in other data centers:
node02                 Dallas, TX
node01                 Newark, NJ
[connexer@lish-fremont.linode.com]# linode3073559
```

Loading compiled-in X.509 certificates
registered taskstats version 1
kAFS: Red Hat AFS client v0.1 registering.
Btrfs loaded
Key type encrypted registered
console [netcon0] enabled
netconsole: network logging started
hctosys: unable to open rtc device (rtc0)
Freeing unused kernel memory: 1472K (ffffffff8234b000 - ffffffff824bb000)
Write protecting the kernel read-only data: 18432k
Freeing unused kernel memory: 1736K (ffff880001a4e000 - ffff880001c00000)
Freeing unused kernel memory: 1744K (ffff88000204c000 - ffff880002200000)

Welcome to Finnix!

[*] Total memory: **990MiB**, shared ramdisk: **738MiB**
[*] Loading probed module: sysmodules: /lib/modules/4.1.2-finnix/modules.alias:
No such file or directory
[*] Finnix media found at **sdh**
[*] System: **Intel Xeon E5-2680 v2 2.80GHz**
[*] Running Linux kernel **4.1.2-finnix** on **x86_64**
[*] **Finnix 111** ready; **464** packages, **146M** compressed

root@ttyS0:~# []

roberto@manzanillo: /home/roberto   ✕

File   Edit   View   Search   Terminal   Help

```
Write protecting the kernel read-only data: 18432k
Freeing unused kernel memory: 1736K (ffff880001a4e000 - ffff880001c00000)
Freeing unused kernel memory: 1744K (ffff88000204c000 - ffff880002200000)


Welcome to Finnix!

[*] Total memory: 990MiB, shared ramdisk: 738MiB
[*] Loading probed module: sysmodules: /lib/modules/4.1.2-finnix/modules.alias:
No such file or directory
[*] Finnix media found at sdh
[*] System: Intel Xeon E5-2680 v2 2.80GHz
[*] Running Linux kernel 4.1.2-finnix on x86_64
[*] Finnix 111 ready; 464 packages, 146M compressed


root@ttyS0:~# cryptsetup luksFormat /dev/sdc

WARNING!
========
This will overwrite data on /dev/sdc irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
root@ttyS0:~#
```

File   Edit   View   Search   Terminal   Help

```
Freeing unused kernel memory: 1744K (ffff88000204c000 - ffff880002200000)

Welcome to Finnix!

[*] Total memory: 990MiB, shared ramdisk: 738MiB
[*] Loading probed module: sysmodules: /lib/modules/4.1.2-finnix/modules.alias:
No such file or directory
[*] Finnix media found at sdh
[*] System: Intel Xeon E5-2680 v2 2.80GHz
[*] Running Linux kernel 4.1.2-finnix on x86_64
[*] Finnix 111 ready; 464 packages, 146M compressed

root@ttyS0:~# cryptsetup luksFormat /dev/sdc

WARNING!
========
This will overwrite data on /dev/sdc irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
root@ttyS0:~# cryptsetup luksOpen /dev/sdc root
Enter passphrase for /dev/sdc:
root@ttyS0:~# 
```

```
This will overwrite data on /dev/sdc irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
root@ttyS0:~# cryptsetup luksOpen /dev/sdc root
Enter passphrase for /dev/sdc:
root@ttyS0:~# mkfs.ext4 /dev/sda
mke2fs 1.42.13 (17-May-2015)
/dev/sda contains a ext4 file system
        created on Fri May  5 09:35:26 2017
Proceed anyway? (y,n) y
Discarding device blocks: done
Creating filesystem with 262144 1k blocks and 65536 inodes
Filesystem UUID: cb26babb-b5ea-45c3-b208-408a7776e5df
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729, 204801, 221185

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~#
```

```
Creating filesystem with 262144 1k blocks and 65536 inodes
Filesystem UUID: cb26babb-b5ea-45c3-b208-408a7776e5df
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729, 204801, 221185

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# mkfs.ext4 /dev/mapper/root
mke2fs 1.42.13 (17-May-2015)
Creating filesystem with 4652544 4k blocks and 1163264 inodes
Filesystem UUID: 93ef3f81-5e40-47aa-8d9b-d895e4e057e1
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# 
```

File   Edit   View   Search   Terminal   Help

```
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# mkfs.ext4 /dev/mapper/root
mke2fs 1.42.13 (17-May-2015)
Creating filesystem with 4652544 4k blocks and 1163264 inodes
Filesystem UUID: 93ef3f81-5e40-47aa-8d9b-d895e4e057e1
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# cryptsetup -d /dev/urandom create swap /dev/sdb
root@ttyS0:~# mkswap /dev/mapper/swap
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
no label, UUID=3298bcd6-c7f0-41c2-a300-e327cd633a22
root@ttyS0:~# swapon /dev/mapper/swap
root@ttyS0:~# mount /dev/mapper/root /mnt
root@ttyS0:~#
```

```
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# mkfs.ext4 /dev/mapper/root
mke2fs 1.42.13 (17-May-2015)
Creating filesystem with 4652544 4k blocks and 1163264 inodes
Filesystem UUID: 93ef3f81-5e40-47aa-8d9b-d895e4e057e1
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# cryptsetup -d /dev/urandom create swap /dev/sdb
root@ttyS0:~# mkswap /dev/mapper/swap
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
no label, UUID=3298bcd6-c7f0-41c2-a300-e327cd633a22
root@ttyS0:~# swapon /dev/mapper/swap
root@ttyS0:~# mount /dev/mapper/root /mnt
root@ttyS0:~# debootstrap --arch=amd64  --include=openssh-server,vim,cryptsetup
jessie /mnt/
```

File Edit View Search Terminal Help

```
root@ttyS0:~# mkfs.ext4 /dev/mapper/root
mke2fs 1.42.13 (17-May-2015)
Creating filesystem with 4652544 4k blocks and 1163264 inodes
Filesystem UUID: 93ef3f81-5e40-47aa-8d9b-d895e4e057e1
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# cryptsetup -d /dev/urandom create swap /dev/sdb
root@ttyS0:~# mkswap /dev/mapper/swap
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
no label, UUID=3298bcd6-c7f0-41c2-a300-e327cd633a22
root@ttyS0:~# swapon /dev/mapper/swap
root@ttyS0:~# mount /dev/mapper/root /mnt
root@ttyS0:~# debootstrap --arch=amd64  --include=openssh-server,vim,cryptsetup
jessie /mnt/
I: Retrieving Release
```

File   Edit   View   Search   Terminal   Help

```
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000


Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

root@ttyS0:~# cryptsetup -d /dev/urandom create swap /dev/sdb
root@ttyS0:~# mkswap /dev/mapper/swap
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
no label, UUID=3298bcd6-c7f0-41c2-a300-e327cd633a22
root@ttyS0:~# swapon /dev/mapper/swap
root@ttyS0:~# mount /dev/mapper/root /mnt
root@ttyS0:~# debootstrap --arch=amd64  --include=openssh-server,vim,cryptsetup
jessie /mnt/
I: Retrieving Release
I: Retrieving Release.gpg
I: Checking Release signature
I: Valid Release signature (key id 75DDC3C4A499F1A18CB5F3C8CBF8D6FD518E17E1)
I: Retrieving Packages
I: Validating Packages
I: Resolving dependencies of required packages...
```

File   Edit   View   Search   Terminal   Help

```
I: Retrieving libacl1 2.2.52-2
I: Validating libacl1 2.2.52-2
I: Retrieving adduser 3.113+nmu3
I: Validating adduser 3.113+nmu3
I: Retrieving apt 1.0.9.8.4
I: Validating apt 1.0.9.8.4
I: Retrieving apt-utils 1.0.9.8.4
I: Validating apt-utils 1.0.9.8.4
I: Retrieving libapt-inst1.5 1.0.9.8.4
I: Validating libapt-inst1.5 1.0.9.8.4
I: Retrieving libapt-pkg4.12 1.0.9.8.4
I: Validating libapt-pkg4.12 1.0.9.8.4
I: Retrieving libattr1 1:2.4.47-2
I: Validating libattr1 1:2.4.47-2
I: Retrieving libaudit-common 1:2.4-1
I: Validating libaudit-common 1:2.4-1
I: Retrieving libaudit1 1:2.4-1+b1
I: Validating libaudit1 1:2.4-1+b1
I: Retrieving base-files 8+deb8u7
I: Validating base-files 8+deb8u7
I: Retrieving base-passwd 3.5.37
I: Validating base-passwd 3.5.37
I: Retrieving bash 4.3-11+deb8u1
```

```
roberto@manzanillo: /home/roberto                    ✕

File  Edit  View  Search  Terminal  Help

I: Configuring wget...
I: Configuring apt...
I: Configuring man-db...
I: Configuring libnetfilter-acct1:amd64...
I: Configuring rsyslog...
I: Configuring libk5crypto3:amd64...
I: Configuring nfacct...
I: Configuring apt-utils...
I: Configuring libirs-export91...
I: Configuring libgnutls-openssl27:amd64...
I: Configuring libkrb5-3:amd64...
I: Configuring iputils-ping...
I: Configuring isc-dhcp-common...
I: Configuring isc-dhcp-client...
I: Configuring libgssapi-krb5-2:amd64...
I: Configuring openssh-client...
I: Configuring openssh-sftp-server...
I: Configuring openssh-server...
I: Configuring tasksel...
I: Configuring tasksel-data...
I: Configuring libc-bin...
I: Configuring systemd...
I: Base system installed successfully.
root@ttyS0:~#
```

```
I: Configuring nfacct...
I: Configuring apt-utils...
I: Configuring libirs-export91...
I: Configuring libgnutls-openssl27:amd64...
I: Configuring libkrb5-3:amd64...
I: Configuring iputils-ping...
I: Configuring isc-dhcp-common...
I: Configuring isc-dhcp-client...
I: Configuring libgssapi-krb5-2:amd64...
I: Configuring openssh-client...
I: Configuring openssh-sftp-server...
I: Configuring openssh-server...
I: Configuring tasksel...
I: Configuring tasksel-data...
I: Configuring libc-bin...
I: Configuring systemd...
I: Base system installed successfully.
root@ttyS0:~# mount /dev/sda /mnt/boot/
root@ttyS0:~# mount -o bind /dev /mnt/dev/
root@ttyS0:~# mount -o bind /dev/pts/ /mnt/dev/pts
root@ttyS0:~# mount -t proc /proc/ /mnt/proc/
root@ttyS0:~# mount -t sysfs /sys/ /mnt/sys/
root@ttyS0:~# chroot /mnt/ /bin/bash
root@finnix:/# vim /etc/crypttab
```

File   Edit   View   Search   Terminal   Help

```
# <target name> <source device>        <key file>        <options>
root            /dev/sdc               none              luks
swap            /dev/sdb               /dev/urandom      swap
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                             3,61         All
```

File   Edit   View   Search   Terminal   Help

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
root@finnix:/# tune2fs -l /dev/sda |grep UUID
Filesystem UUID: cb26babb-b5ea-45c3-b208-408a7776e5df
root@finnix:/# tune2fs -l /dev/mapper/root |grep UUID
Filesystem UUID: 93ef3f81-5e40-47aa-8d9b-d895e4e057e1
root@finnix:/# vim /etc/fstab

```
/dev/mapper/swap    none     swap     sw        0          0
UUID=93ef3f81-5e40-47aa-8d9b-d895e4e057e1         /         ext4      errors=remount-r
o         0         1
UUID=cb26babb-b5ea-45c3-b208-408a7776e5df         /boot     ext4      defaults
0         2
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                                        3,90          All
```

```
o          0          1
UUID=cb26babb-b5ea-45c3-b208-408a7776e5df          /boot     ext4     defaults
0          2
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
root@finnix:/# cat /proc/mounts > /etc/mtab
root@finnix:/# mkdir /boot/grub
root@finnix:/# apt-get install -y grub-pc linux-image-amd64
```

File   Edit   View   Search   Terminal   Help

```
Preparing to unpack .../libnuma1_2.0.10-1_amd64.deb ...
Unpacking libnuma1:amd64 (2.0.10-1) ...
Selecting previously unselected package libuuid-perl.
Preparing to unpack .../libuuid-perl_0.05-1+b1_amd64.deb ...
Unpacking libuuid-perl (0.05-1+b1) ...
Selecting previously unselected package linux-base.
Preparing to unpack .../linux-base_3.5_all.deb ...
Unpacking linux-base (3.5) ...
Selecting previously unselected package libklibc.
Preparing to unpack .../libklibc_2.0.4-2_amd64.deb ...
Unpacking libklibc (2.0.4-2) ...
Selecting previously unselected package klibc-utils.
Preparing to unpack .../klibc-utils_2.0.4-2_amd64.deb ...
Unpacking klibc-utils (2.0.4-2) ...
Selecting previously unselected package busybox.
Preparing to unpack .../busybox_1%3a1.22.0-9+deb8u1_amd64.deb ...
Unpacking busybox (1:1.22.0-9+deb8u1) ...
Selecting previously unselected package initramfs-tools.
Preparing to unpack .../initramfs-tools_0.120+deb8u2_all.deb ...
Unpacking initramfs-tools (0.120+deb8u2) ...
Selecting previously unselected package linux-image-3.16.0-4-amd64.
Preparing to unpack .../linux-image-3.16.0-4-amd64_3.16.39-1_amd64.deb ...
Unpacking linux-image-3.16.0-4-amd64 (3.16.39-1) ...
```

Package configuration

Configuring grub-pc

The grub-pc package is being upgraded. This menu allows you to select which devices you'd like grub-install to be automatically run for, if any.

Running grub-install automatically is recommended in most situations, to prevent the installed GRUB core image from getting out of sync with GRUB modules or grub.cfg.

If you're unsure which drive is designated as boot drive by your BIOS, it is often a good idea to install GRUB to all of them.

Note: it is possible to install GRUB to partition boot records as well, and some appropriate partitions are offered here. However, this forces GRUB to use the blocklist mechanism, which makes it less reliable, and therefore is not recommended.

<Ok>

File   Edit   View   Search   Terminal   Help

Package configuration

```
▓▓▓▓▓▓▓J Configuring grub-pc ▓▓▓▓▓▓▓L
▓ GRUB install devices:
▓
▓      [*] /dev/sda (268 MB; ???)
▓      [ ] /dev/sdb (2147 MB; ???)
▓      [ ] /dev/sdc (19058 MB; ???)
▓      [ ] /dev/sdh (167 MB; ???)
▓      [ ] /dev/dm-0 (19056 MB; root)
▓      [ ] /dev/sda (268 MB; ???)
▓
▓
▓                  <Ok>
▓
▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓▓
```

```
Setting up libpod-latex-perl (0.61-1) ...
Setting up libregexp-common-perl (2013031301-1) ...
Setting up libpod-readme-perl (0.11-1) ...
Setting up libtext-template-perl (1.46-1) ...
Setting up libsoftware-license-perl (0.103010-3) ...
Setting up libterm-ui-perl (0.42-1) ...
Setting up libtext-soundex-perl (3.4-1+b2) ...
Setting up linux-image-amd64 (3.16+63) ...
Setting up rename (0.20-3) ...
update-alternatives: using /usr/bin/file-rename to provide /usr/bin/rename (rena
me) in auto mode
Setting up shared-mime-info (1.3-1) ...
Setting up xdg-user-dirs (0.15-2) ...
Setting up xml-core (0.13+nmu2) ...
Setting up irqbalance (1.0.6-3) ...
[ ok ] Starting SMP IRQ Balancer: irqbalance.
Setting up os-prober (1.65) ...
Processing triggers for libc-bin (2.19-18+deb8u7) ...
Processing triggers for initramfs-tools (0.120+deb8u2) ...
update-initramfs: Generating /boot/initrd.img-3.16.0-4-amd64
loadkeys is missing. Please install the 'kbd' package.
Processing triggers for sgml-base (1.26+nmu4) ...
Processing triggers for systemd (215-17+deb8u6) ...
root@finnix:/# vim /etc/default/grub
```

File   Edit   View   Search   Terminal   Help

```
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX=""

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card supports via VBE
# you can see them in real GRUB with the command `vbeinfo'
#GRUB_GFXMODE=640x480
                                                              1,1            Top
```

```
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet cgroup_enable=memory swapaccount=1"
GRUB_CMDLINE_LINUX="console=ttyS0,19200n8"
GRUB_DISABLE_LINUX_UUID=true
GRUB_SERIAL_COMMAND="serial --speed=19200 --unit=0 --word=8 --parity=no --stop=1
"

# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
```

-- INSERT --   12,82   Top

```
# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
"/etc/default/grub" 34L, 1344C written
root@finnix:/# update-grub
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.16.0-4-amd64
Found initrd image: /boot/initrd.img-3.16.0-4-amd64
done
root@finnix:/# cd /boot
root@finnix:/boot# mkdir boot
root@finnix:/boot# mv grub boot/
root@finnix:/boot# ln -s boot/grub
root@finnix:/boot# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@finnix:/boot# vim /etc/network/interfaces.d/linode-default
```

File   Edit   View   Search   Terminal   Help

```
auto lo eth0
iface lo inet loopback
iface lo inet6 loopback
iface eth0 inet dhcp
iface eth0 inet6 auto
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

-- INSERT --   5,22   All

```
iface lo inet loopback
iface lo inet6 loopback
iface eth0 inet dhcp
iface eth0 inet6 auto
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
</network/interfaces.d/linode-default" [New] 5L, 103C written
root@finnix:/boot# vim /etc/hosts
```

File   Edit   View   Search   Terminal   Help

```
ff02::1          ip6-allnodes
ff02::2          ip6-allrouters

192.81.130.199   linode3073559
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 6L, 138C written
root@finnix:/boot# exit
root@ttyS0:~# # disconnect GNU screen with ^a^d
```

File   Edit   View   Search   Terminal   Help

```
roberto@manzanillo:~$ ssh connexer@lish-fremont.linode.com
Linux lish-fremont.linode.com 4.8.3-x86_64-linode76 #1 SMP Thu Oct 20 19:05:39 E
DT 2016 x86_64
Linodes located in this data center:
linode3073559          Fremont, CA

Linodes located in other data centers:
node02                 Dallas, TX
node01                 Newark, NJ
[connexer@lish-fremont.linode.com]# linode3073559
[linode3073559@fremont752 lish] Fri May  5 08:41:44 EDT 2017
[linode3073559@fremont752 lish] Linode Shell (lish) Console starting...
[linode3073559@fremont752 lish] [detached from 743.linode3073559]
[linode3073559@fremont752 lish]# reboot 1
```

File   Edit   View   Search   Terminal   Help

```
roberto@manzanillo:~$ ssh connexer@lish-fremont.linode.com
Linux lish-fremont.linode.com 4.8.3-x86_64-linode76 #1 SMP Thu Oct 20 19:05:39 E
DT 2016 x86_64
Linodes located in this data center:
linode3073559          Fremont, CA

Linodes located in other data centers:
node02                 Dallas, TX
node01                 Newark, NJ
[connexer@lish-fremont.linode.com]# linode3073559
[linode3073559@fremont752 lish] Fri May  5 08:41:44 EDT 2017
[linode3073559@fremont752 lish] Linode Shell (lish) Console starting...
[linode3073559@fremont752 lish] [detached from 743.linode3073559]
[linode3073559@fremont752 lish]# reboot 1
Jobs Inserted
[linode3073559@fremont752 lish]#
Job 48952639 - Lish initiated shutdown completed.
[linode3073559@fremont752 lish]#
[linode3073559@fremont752 lish] [detached from 16561.linode3073559]
[linode3073559@fremont752 lish]# linode3073559
Unknown command 'linode3073559'
[linode3073559@fremont752 lish]#
[linode3073559@fremont752 lish] Closing Connection
[connexer@lish-fremont.linode.com]# linode3073559
```

File   Edit   View   Search   Terminal   Help

```
error: symbol `grub_video_fb_get_region' not found.
Loading, please wait...
Please unlock disk /dev/sdc (root): ▊
```

File Edit View Search Terminal Help

```
error: symbol `grub_video_fb_get_region' not found.
Loading, please wait...
Please unlock disk /dev/sdc (root):
cryptsetup: root set up successfully
/dev/mapper/root: clean, 21074/1163264 files, 289449/4652544 blocks
[  184.307086] systemd-fsck[238]: /dev/sda: clean, 330/65536 files, 49653/262144
 blocks

Debian GNU/Linux 8 finnix ttyS0

finnix login:
```

```
/dev/mapper/root: clean, 21090/1163264 files, 289501/4652544 blocks
[   12.606320] systemd-fsck[238]: /dev/sda: clean, 330/65536 files, 49653/262144
 blocks

Debian GNU/Linux 8 finnix ttyS0

finnix login: root
Password:
Last login: Fri May  5 13:40:20 UTC 2017 on ttyS0
Linux finnix 3.16.0-4-amd64 #1 SMP Debian 3.16.39-1 (2016-12-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@finnix:~# echo linode3073559 >/etc/hostname
root@finnix:~# hostname -F /etc/hostname
root@finnix:~# logout

Debian GNU/Linux 8 linode3073559 ttyS0

linode3073559 login:
```

Dealing With FDE Server Issues

- Notification of server reboot

  - Linode can be configured to email/text you when a server reboots so you know to access the console and provide the passphrase

  - Beware if the server in question is your mail server

- Out of band access

  - Linode offers lish (linode shell) for access to the virtual server's console

  - If the server is bootable, troubleshoot normally

  - If the server is not bootable, use Linode's minimalist Linux environment (Finnix) to troubleshoot

File   Edit   View   Search   Terminal   Help

Date: Fri, 5 May 2017 06:00:12 -0400 (EDT)
From: Linode Alerts <noreply@linode.com>
To: linode@   .com
Subject: Linode Events Notification -

Hello   ! The following activity has recently occurred:

 * linode3073559 - (48945305) System Shutdown - Completed Fri, 05 May 2017 09:52
:49 GMT
 * linode3073559 - (48945306) System Boot - Rescue Mode - Completed Fri, 05 May
2017 09:52:49 GMT

You can change your notification settings via
https://manager.linode.com/profile.

File   Edit   View   Search   Terminal   Help

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: Fri, 5 May 2017 09:45:08 -0400 (EDT)
From: Linode Alerts <noreply@linode.com>
To: linode@        .com
Subject: Linode Events Notification -

Hello        ! The following activity has recently occurred:

 * linode3073559 - (48952639) Lish initiated shutdown - Completed Fri, 05 May 20
17 13:34:21 GMT
 * linode3073559 - (48952640) Lish initiated boot: Debian Jessie w/ FDE - Comple
ted Fri, 05 May 2017 13:34:43 GMT
 * linode3073559 - (48952988) Lassie initiated boot: Debian Jessie w/ FDE - Comp
leted Fri, 05 May 2017 13:41:30 GMT


You can change your notification settings via
https://manager.linode.com/profile.




- - 21/21: Linode Alerts          Linode Events Notification -      -- (all)
```

Questions?

Evaluate this session

Secure Cloud: Linode With Full Disk Encryption

Session videos will be posted to the LinuxFest Northwest YouTube channel.

Thank you!