

Extracting files from a GAIA Snapshot File

Authors:*Michael LeFebvre**Joe Audet***Created:***October 26, 2018***Edited:***May 3, 2019, by Valeri Loukine*

Table of Content

Tools Needed:	1
Use Case.....	1
Create Snapshot.....	2
Download Snapshot.....	3
Extract Snapshot Image File	4
Mount Snapshot Image File	5
Browse and Extract Files from Snapshot Image File	6

Tools Needed:

Linux machine (Splat or Gaia are fine, we use an Ubuntu machine for this)

Use Case

While at a client site performing an R77.30 to R80.10 management server upgrade, we encountered a situation where the customer had built some custom policy installation scripts that ran through scheduled jobs. The files were stored in /usr/local/bin. During the upgrade process these files were wiped out. The customer did not have a copy stored anywhere else as they had done all of the editing through VI on the gateway.

Two options were available:

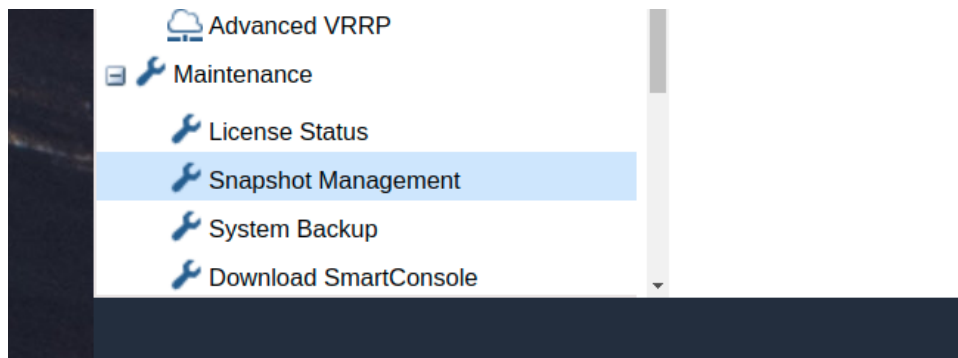
- Revert back to R77.30 snapshot, copy the files, then either revert back to the R80.10 snapshot or repeat the upgrade process
- Find a way to download and open the snapshot, and extract the files from it

While Option #1 was feasible, it is time consuming and not always available, especially if this wasn't discovered right away like it was for this upgrade.

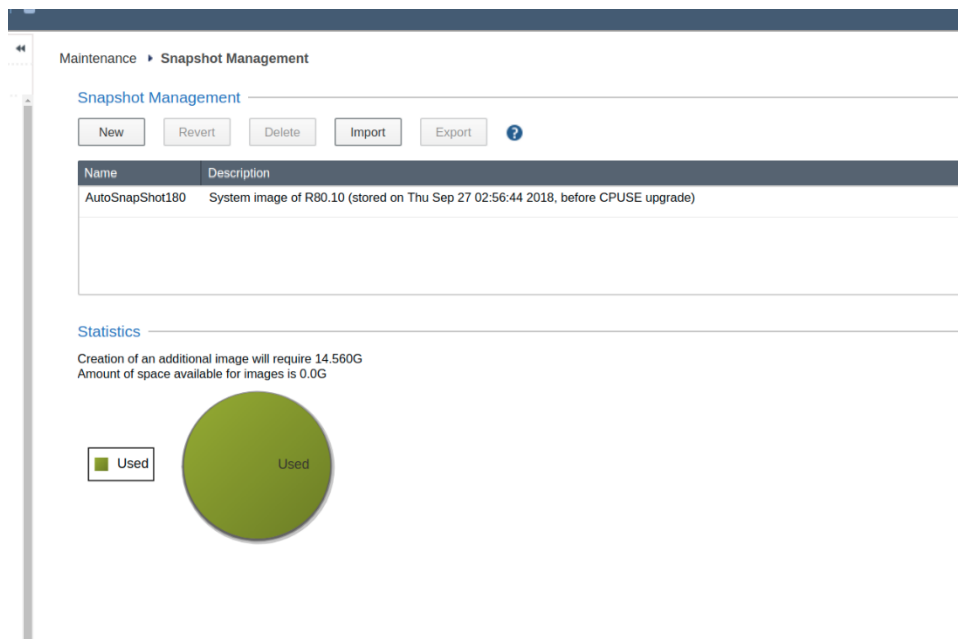
In our example I am using [VMware Workstation](#) with an Ubuntu Desktop VM hosted on my workstation. If you don't have VMware workstation you can also use [Oracle VirtualBox](#).

Create Snapshot

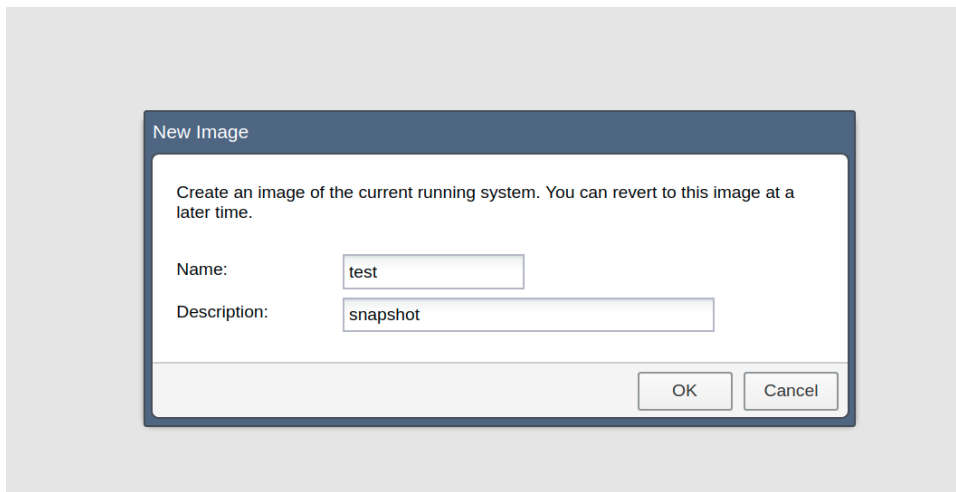
1. Login to WebUI of the management server, go to Maintenance > "Snapshot Management".



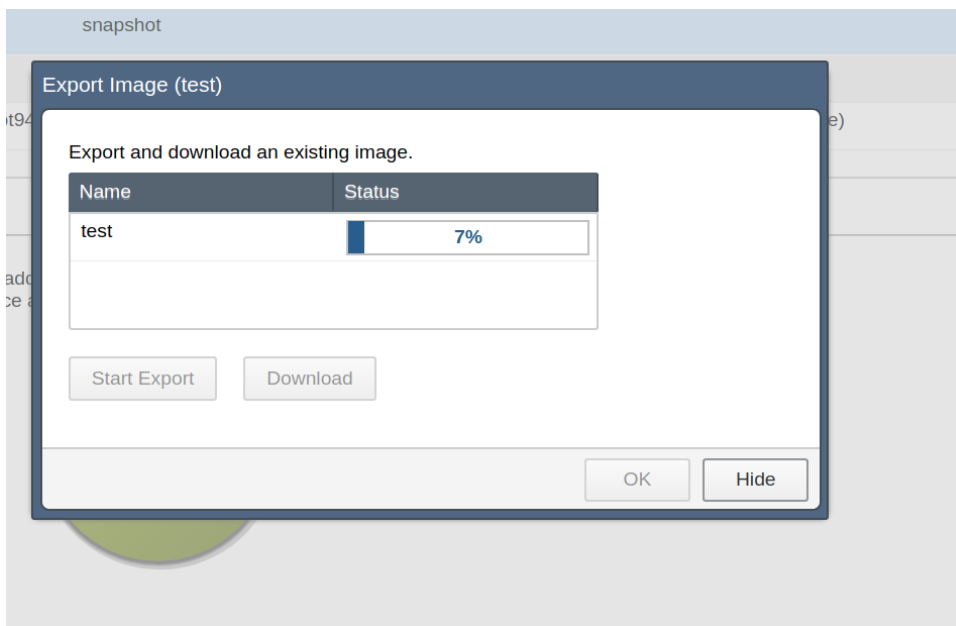
2. Click "New" under Snapshot Management.



3. Give the image a name and description:



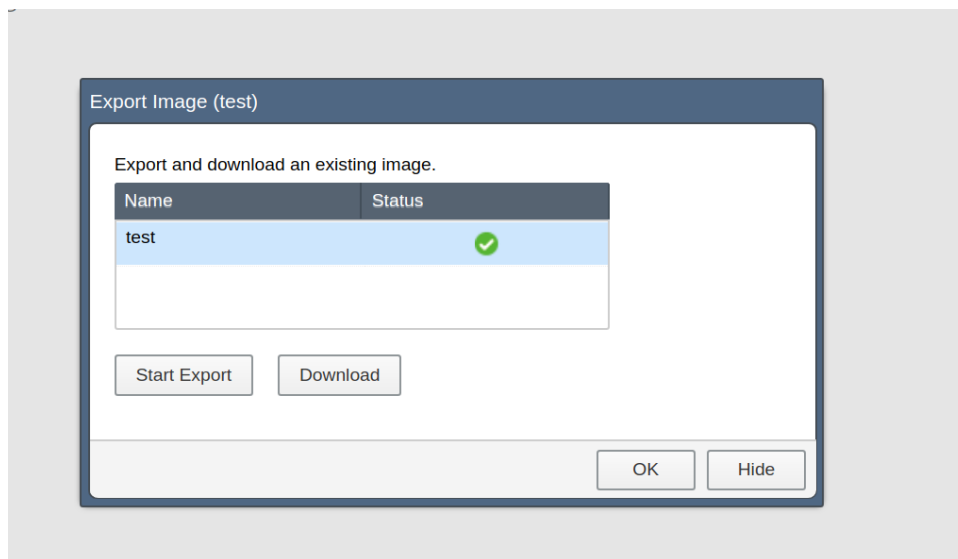
4. Export the snapshot from the WebUI, click start export to begin exporting the snapshot:



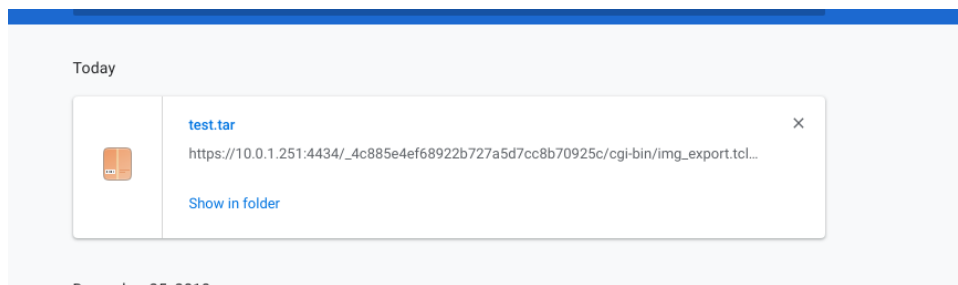
Download Snapshot

While it is possible to perform the extraction on the management server the snapshot was taken from, it is strongly recommended to make a copy of the snapshot and perform the extraction on another machine to avoid potentially destroying the production snapshot file. This is why we used an Ubuntu Desktop VM.

1. After the 'Export Image' status hits 100% you can download the snapshot by clicking "Download":



2. Look for the tar file in your browser download folder on your host machine from which you connected to the WebUI:



3. Now that the snapshot image file has been downloaded to the Ubuntu Desktop VM, you can proceed to mounting the image and extracting the files from it.

Extract Snapshot Image File

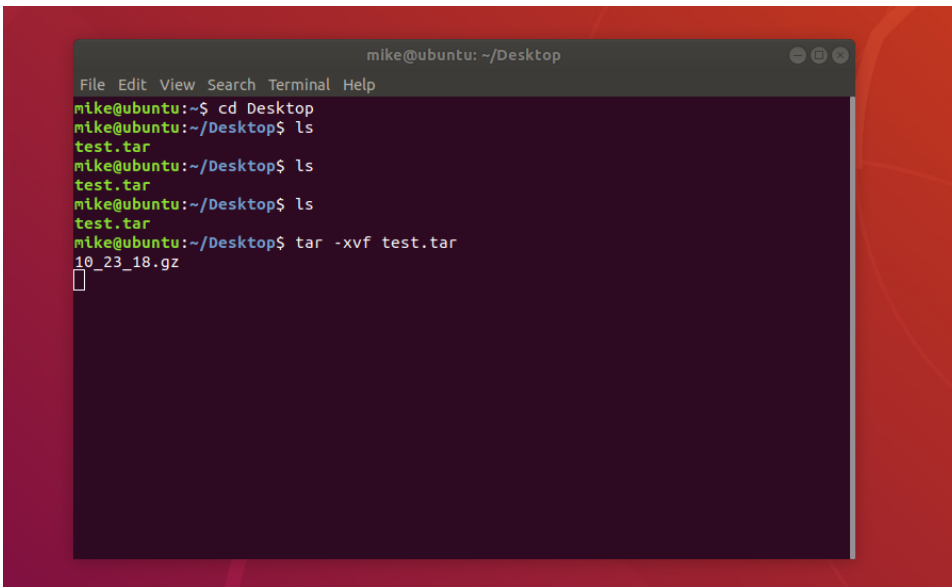
Note: In our example we are showing the full paths of the example screenshots. Your VM file paths will be different, and commands may not be copy and paste ready without some modification.

The snapshot will be a **TAR** file format. Inside of this will be the following structure:

- <snapshot_name>.gz
 - <snapshot_name> (no extension – this is a full disk image)

1. Let's extract tar file, we copied the tar file to our desktop:

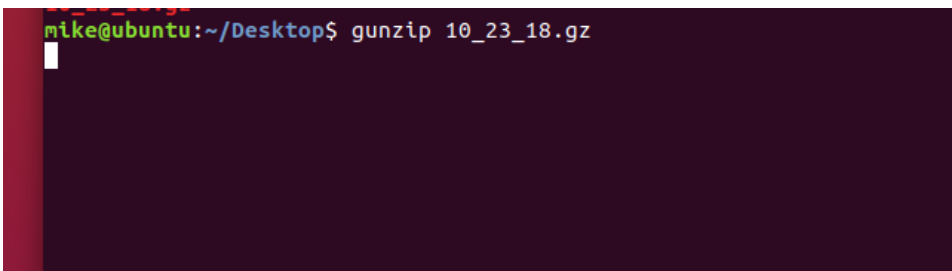
```
"tar -xvf test.tar"
```

A terminal window titled "mike@ubuntu: ~/Desktop" showing the process of extracting a tar file. The user runs "cd Desktop", "ls" (showing "test.tar"), and "tar -xvf test.tar". The output shows "10_23_18.gz" being extracted.

```
mike@ubuntu: ~/Desktop
File Edit View Search Terminal Help
mike@ubuntu:~$ cd Desktop
mike@ubuntu:~/Desktop$ ls
test.tar
mike@ubuntu:~/Desktop$ ls
test.tar
mike@ubuntu:~/Desktop$ ls
test.tar
mike@ubuntu:~/Desktop$ tar -xvf test.tar
10_23_18.gz
```

2. Now that all the files are extracted from the tar file, we need to gunzip the image file which was inside the TAR so it can be mounted:

“gunzip 10_23_18.gz”

A terminal window showing the execution of the "gunzip 10_23_18.gz" command.

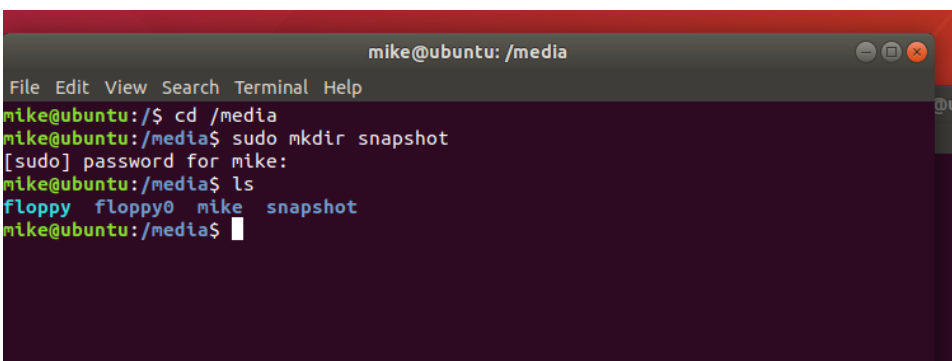
```
mike@ubuntu:~/Desktop$ gunzip 10_23_18.gz
```

Mount Snapshot Image File

1. Next create a directory for the image to be mounted:

“cd /media”

“sudo mkdir snapshot”

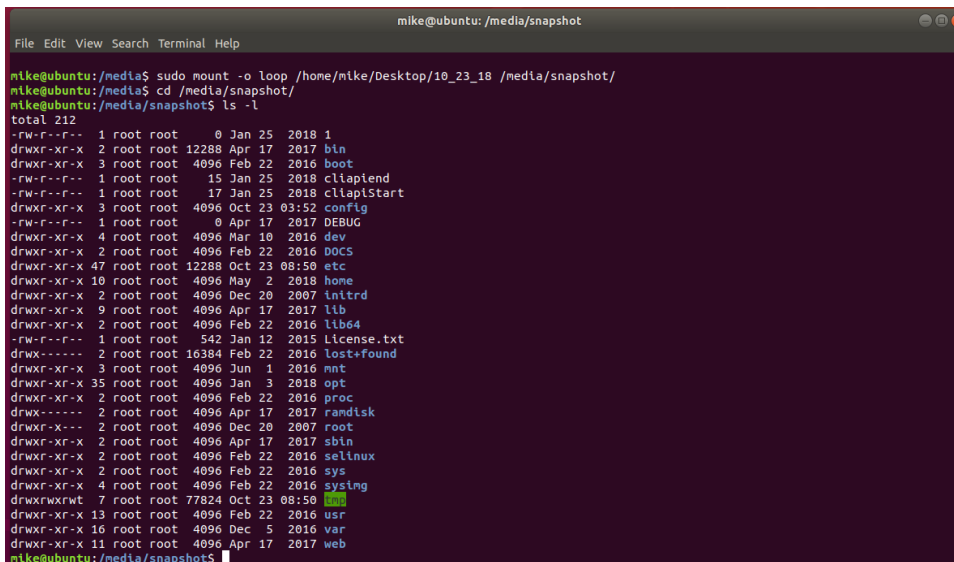
A terminal window titled "mike@ubuntu: /media" showing the creation of a directory. The user runs "cd /media", "sudo mkdir snapshot", and "ls". The output shows "floppy floppy0 mike snapshot".

```
mike@ubuntu: /media
File Edit View Search Terminal Help
mike@ubuntu:/$ cd /media
mike@ubuntu:/media$ sudo mkdir snapshot
[sudo] password for mike:
mike@ubuntu:/media$ ls
floppy floppy0 mike snapshot
mike@ubuntu:/media$
```

2. Now mount the image to /media/snapshot:

“sudo mount -o loop /home/mike/desktop/10_23_18 /media/snapshot”

10_23_18 was the image file inside our example TAR file, you need to find the name of your image file.

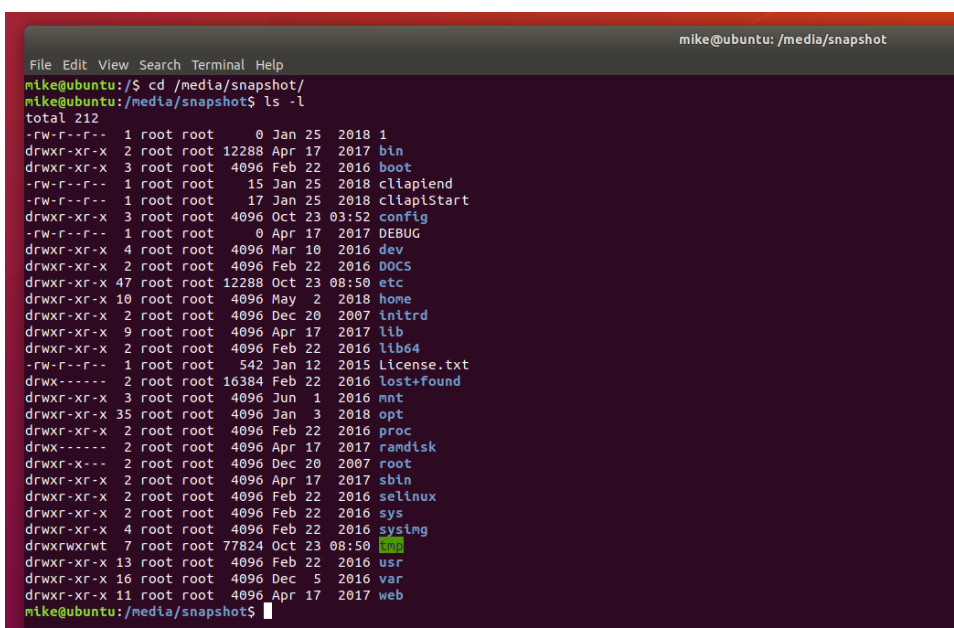


```
mike@ubuntu: /media/snapshot
File Edit View Search Terminal Help
mike@ubuntu:/media$ sudo mount -o loop /home/mike/Desktop/10_23_18 /media/snapshot/
mike@ubuntu:/media$ cd /media/snapshot/
mike@ubuntu:/media/snapshot$ ls -l
total 212
-rw-r--r-- 1 root root 0 Jan 25 2018 1
drwxr-xr-x 2 root root 12288 Apr 17 2017 bin
drwxr-xr-x 3 root root 4096 Feb 22 2016 boot
-rw-r--r-- 1 root root 15 Jan 25 2018 cliapiend
-rw-r--r-- 1 root root 17 Jan 25 2018 cliapiStart
drwxr-xr-x 3 root root 4096 Oct 23 03:52 config
-rw-r--r-- 1 root root 0 Apr 17 2017 DEBUG
drwxr-xr-x 4 root root 4096 Mar 10 2016 dev
drwxr-xr-x 2 root root 4096 Feb 22 2016 DOCS
drwxr-xr-x 47 root root 12288 Oct 23 08:50 etc
drwxr-xr-x 10 root root 4096 May 2 2018 home
drwxr-xr-x 2 root root 4096 Dec 20 2007 initrd
drwxr-xr-x 9 root root 4096 Apr 17 2017 lib
drwxr-xr-x 2 root root 4096 Feb 22 2016 lib64
-rw-r--r-- 1 root root 542 Jan 12 2015 License.txt
drwx----- 2 root root 16384 Feb 22 2016 lost+found
drwxr-xr-x 3 root root 4096 Jun 1 2016 mnt
drwxr-xr-x 35 root root 4096 Jan 3 2018 opt
drwxr-xr-x 2 root root 4096 Feb 22 2016 proc
drwx----- 2 root root 4096 Apr 17 2017 ramdisk
drwxr-xr-x 2 root root 4096 Dec 20 2007 root
drwxr-xr-x 2 root root 4096 Apr 17 2017/sbin
drwxr-xr-x 2 root root 4096 Feb 22 2016 selinux
drwxr-xr-x 2 root root 4096 Feb 22 2016 sys
drwxr-xr-x 4 root root 4096 Feb 22 2016 sysimg
drwxrwxrwt 7 root root 77824 Oct 23 08:50 tmp
drwxr-xr-x 13 root root 4096 Feb 22 2016 usr
drwxr-xr-x 16 root root 4096 Dec 5 2016 var
drwxr-xr-x 11 root root 4096 Apr 17 2017 web
mike@ubuntu:/media/snapshots$
```

Browse and Extract Files from Snapshot Image File

In our example the customer forgot to backup custom scripts in /usr/local/bin. We can copy these scripts out of the now mounted image.

1. Enter “cd /media/snapshot/” to go into the mounted image:



```
mike@ubuntu: /media/snapshot
File Edit View Search Terminal Help
mike@ubuntu:/$ cd /media/snapshot/
mike@ubuntu:/media/snapshot$ ls -l
total 212
-rw-r--r-- 1 root root 0 Jan 25 2018 1
drwxr-xr-x 2 root root 12288 Apr 17 2017 bin
drwxr-xr-x 3 root root 4096 Feb 22 2016 boot
-rw-r--r-- 1 root root 15 Jan 25 2018 cliapiend
-rw-r--r-- 1 root root 17 Jan 25 2018 cliapiStart
drwxr-xr-x 3 root root 4096 Oct 23 03:52 config
-rw-r--r-- 1 root root 0 Apr 17 2017 DEBUG
drwxr-xr-x 4 root root 4096 Mar 10 2016 dev
drwxr-xr-x 2 root root 4096 Feb 22 2016 DOCS
drwxr-xr-x 47 root root 12288 Oct 23 08:50 etc
drwxr-xr-x 10 root root 4096 May 2 2018 home
drwxr-xr-x 2 root root 4096 Dec 20 2007 initrd
drwxr-xr-x 9 root root 4096 Apr 17 2017 lib
drwxr-xr-x 2 root root 4096 Feb 22 2016 lib64
-rw-r--r-- 1 root root 542 Jan 12 2015 License.txt
drwx----- 2 root root 16384 Feb 22 2016 lost+found
drwxr-xr-x 3 root root 4096 Jun 1 2016 mnt
drwxr-xr-x 35 root root 4096 Jan 3 2018 opt
drwxr-xr-x 2 root root 4096 Feb 22 2016 proc
drwx----- 2 root root 4096 Apr 17 2017 ramdisk
drwxr-xr-x 2 root root 4096 Dec 20 2007 root
drwxr-xr-x 2 root root 4096 Apr 17 2017/sbin
drwxr-xr-x 2 root root 4096 Feb 22 2016 selinux
drwxr-xr-x 2 root root 4096 Feb 22 2016 sys
drwxr-xr-x 4 root root 4096 Feb 22 2016 sysimg
drwxrwxrwt 7 root root 77824 Oct 23 08:50 tmp
drwxr-xr-x 13 root root 4096 Feb 22 2016 usr
drwxr-xr-x 16 root root 4096 Dec 5 2016 var
drwxr-xr-x 11 root root 4096 Apr 17 2017 web
mike@ubuntu:/media/snapshots$
```

2. On the original management box script files existed in /usr/local/bin because this is mounted /media/snapshot/, we enter “cd /media/snapshot/usr/local/bin” to get to see the files:

```

mike@ubuntu: /media/snapshot/usr/local/bin
File Edit View Search Terminal Help
mike@ubuntu: /media/snapshot/usr/local/bin$ ls -l
total 4128
-rwxr-xr-x 1 root root 1975 Apr 28 2015 adp_mon.sh
-rw-rw-r-- 1 root root 0 Sep 8 2016 CKP_mutex::checkpoint_rand_mutex
-rw-rw-r-- 1 root root 0 Sep 8 2016 CKP_mutex::_ckpReg_Mutex_
-rw-rw-r-- 1 root root 0 Sep 8 2016 CKP_mutex::fwcd_crl_mutex
-rw-rw-r-- 1 root root 0 Sep 8 2016 CKP_mutex::opt_CPmDs-R77_customers_bld24ngxmgt1_CPsuite-R77_fw1_database__SessionCache_1
-rwxrwx--- 1 root users 1480 Sep 8 2016 dbedit_generate.ksh
-rwxrwx--- 1 root users 1524 Sep 8 2016 dbload.ksh
-rwxrwx--- 1 root users 1516 Mar 22 2016 dbload_log.kshx.old
-rwxrwx--- 1 root users 1757 Jul 11 2016 dbload_old.ksh
-rwxrwx--- 1 root users 1447 Dec 7 2016 fwpush_calrv31_FW_Cluster.ksh
-rwxrwx--- 1 root users 1461 Jun 3 2016 fwpush_calrv31_UTM_Cluster.ksh
-rwxrwx--- 1 root users 1462 Nov 16 2017 fwpush_casjs11fw_cloud.ksh
-rwxrwx--- 1 root users 1474 Nov 16 2017 fwpush_casjs11fw_genesys.ksh
-rwxrwx--- 1 root users 1412 Jun 3 2016 fwpush_CO_BLD_CLOUD.ksh
-rwxrwx--- 1 root users 1393 Jun 3 2016 fwpush_CO_BLD_DMZ.ksh
-rwxrwx--- 1 root users 1411 Jun 3 2016 fwpush_CO_BLD_DMZPCI.ksh
-rwxrwx--- 1 root users 1430 Jun 3 2016 fwpush_CO_BLD_DMZPCI_STM.ksh
-rwxrwx--- 1 root users 1412 Jun 3 2016 fwpush_CO_BLD_DMZ_STM.ksh
-rwxrwx--- 1 root users 1417 Jun 3 2016 fwpush_CO_BLD_INTERNET.ksh
-rwxrwx--- 1 root users 1412 Jun 3 2016 fwpush_CO_BLD_PARTNER.ksh
-rwxrwx--- 1 root users 1398 Jun 3 2016 fwpush_CO_BLD_PCI3.ksh
-rwxrwx--- 1 root users 1398 Jun 3 2016 fwpush_CO_BLD_PCI4.ksh
-rwxrwx--- 1 root users 1393 Jun 3 2016 fwpush_CO_BLD_STM.ksh
-rwxrwx--- 1 root users 1412 Jun 3 2016 fwpush_CT_HFD_CLOUD.ksh
-rwxrwx--- 1 root users 1393 Jun 3 2016 fwpush_CT_HFD_DMZ.ksh
-rwxrwx--- 1 root users 1411 Jun 3 2016 fwpush_CT_HFD_DMZPCI.ksh
-rwxrwx--- 1 root users 1417 Jun 3 2016 fwpush_CT_HFD_INTERNET.ksh
-rwxrwx--- 1 root users 1686 Jun 3 2016 fwpush_CT_HFD_PARTNER.ksh
-rwxrwx--- 1 root users 1393 Jun 3 2016 fwpush_CT_HFD_PCI.ksh
-rwxrwx--- 1 root users 1407 Jun 3 2016 fwpush_CT_HFD_TEST.ksh
-rwxrwx--- 1 root users 1397 Sep 13 2017 fwpush_pawyn21_Cluster.ksh
-rwxrwx--- 1 root users 1447 Dec 7 2016 fwpush_uts1cs1_fw_Cluster.ksh
-rwxrwx--- 1 root users 1461 Jun 3 2016 fwpush_uts1cs1_UTM_Cluster.ksh
-rwxrwx--- 1 root users 1462 Nov 16 2017 fwpush_vaash31fw_cloud.ksh
-rwxrwx--- 1 root users 1474 Nov 16 2017 fwpush_vaash31fw_genesys.ksh
-rwxrwx--- 1 root users 1121 Feb 26 2015 fwrotate-logs.ksh
-rwxrwx--- 1 root users 997 Jan 9 2017 status.ksh
-rwxr-xr-x 1 root root 6284 Apr 28 2015 tile-dev
-rwxr-xr-x 1 root root 3855782 Apr 28 2015 tile-gdb
-rwxr-xr-x 1 root root 212154 Apr 28 2015 tile-monitor
-rwxr-xr-x 1 root root 3646 Apr 28 2015 tilemon.sh
mike@ubuntu: /media/snapshot/usr/local/bin$

```

3. From here we copy the files out, example /home/mike/desktop/scripts

“mkdir /home/mike/Desktop/scripts”
“sudo cp *.ksh /home/mike/Desktop/scripts”

```

mike@ubuntu: /media/snapshot/usr/local/bin
File Edit View Search Terminal Help

mike@ubuntu: /media/snapshot/usr/local/bin$ mkdir /home/mike/Desktop/scripts
mike@ubuntu: /media/snapshot/usr/local/bin$ sudo cp *.ksh /home/mike/Desktop/scripts
mike@ubuntu: /media/snapshot/usr/local/bin$

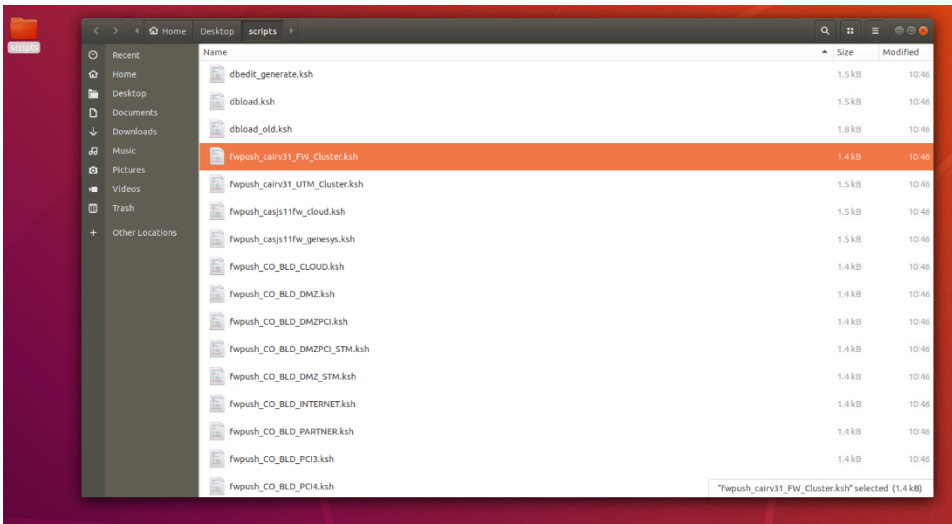
```

4. The owner of the files is root. Let’s change the permissions so everyone can access the files on the Linux VM:

“sudo chmod 777 /home/mike/desktop/scripts/*.ksh”:

```
mike@ubuntu: /media/snapshot/usr/local/bin
File Edit View Search Terminal Help
mike@ubuntu: /media/snapshot/usr/local/bin$ sudo chnod 777 /home/mike/Desktop/scripts/*.ksh
mike@ubuntu: /media/snapshot/usr/local/bin$
```

5. Now we can see the files on our desktop in “scripts” folder and we have full permission.



6. Copy the files you need somewhere and you are all set!