Overview

When you run out of space, it's time to add a new drive to your AC-Hunter system. Here are the steps to make that happen. It will involve a brief outage, so plan for a time when AC-Hunter isn't being actively used.

Most of our documentation is - or is very close to - "run these commands to accomplish a goal." This document is an exception; it should be considered a *guideline* of the steps to be performed instead of a literal list of commands to run. You should inspect each command to make sure it fits your system and keep an eye out for any errors or warnings that may show the command needs to be run in a different way.

As with any steps that involve root-level manipulation of the system, please type carefully and double check your commands before you press enter. In particular, please check the formatting of your changes to /etc/fstab - a typo in this file could make the system unbootable. Be aware that despite our best efforts to document all the steps, differences between your system and ours may mean that you need modified or additional commands.

Approaches

In this document we'll walk through the steps of adding a new (physical or virtual) drive to your AC-Hunter system.

We briefly mention how this might be done with Logical Volume Management at the end, but do not provide the individual steps.

Steps

Prep

Before starting, make sure you have a backup of the system.

Please be careful with these commands. **Don't copy and run anything we have below without being sure you've replaced all drives, partitions, and mount points with the values that match your system.** If you have any questions, please check with someone else before typing these commands as-is could wipe out your system! I've tried to boldface the things that may be different between my machine and yours.

Almost all of these commands need to be run under sudo.

These instructions assume you're only running AC-Hunter and BeaKer on this system. if you're running other docker containers, you'll need to shut down these other containers before transferring them over to the new storage and restart them at the end.

Add new hard drive to the system

For an internal drive, shut the system down and add it. For an external drive, simply plug it into a USB 3.0 or higher port (the USB A ports with the blue plastic center or any USB C port.) We strongly discourage connecting an external drive of any sort to a USB 2.0 port or USB 1.x port; with 2.0 all data transfer will be slow, and with 1.x the transfer will be so slow it can appear the system is hung. Restart the system if you had powered it off above.

If AC-Hunter is on a cloud server it may be possible to add a new volume (additional virtual drive) to the system. Pay close attention to the device name and path under which this volume is mounted. Restart the system if your cloud provider requires it to make the new volume available.

In either case, make sure you're adding a new drive/volume that's big enough to hold your existing Zeek logs, your existing databases, and any growth you need.

Now, find the new drive. Your best helper in this is `lsblk` (list block devices). Here's an example output from one of my systems - your output will be completely different.

```
lsblk
NAME                                                   MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                                                      8:0    0 931.5G  0 disk
|-sda1                                                   8:1    0   500M  0 part
| `-md8                                                  9:8    0   500M  0 raid1 /boot
|-sda2                                                   8:2    0 122.1G  0 part
| `-md9                                                  9:9    0 122.1G  0 raid1
|   `-luks-c6d5ce93-0c36-4fac-a910-27891981fb74 (dm-1) 253:1    0 122.1G  0 crypt /
|-sda3                                                   8:3    0     8G  0 part
| `-md10                                                 9:10   0     8G  0 raid1
|   `-luks-87a5ed22-f369-493e-93e7-ab0476b47ebb (dm-0) 253:0    0     8G  0 crypt [SWAP]
...
sdc                                                      8:32   0 931.5G  0 disk
sr0                                                     11:0    1  1024M  0 rom
```

In this output we have sda providing the root and swap partitions, sr0 as the scsi rom/dvd drive, and sdc as a 930GB drive. Note that sdc is not mounted anywhere, so if I've just added a new 1TB disk it appeared as SDC.

Depending on how your system is set up, it may be already mounted.

As you continue, remember to pay particular attention to any boldfaced parts of commands; these will almost certainly need to be modified for your system. Simply running these commands without substituting the right value for your system will almost certainly destroy existing data.

Mount it

The `mount | less` command will tell you what filesystem type is being used. If the filesystem is any form of FAT (VFAT, ExFAT, etc), please unmount it and reformat it as ext4.

If the new drive isn't mounted at all, please create the mountpoint:

```
sudo mkdir -p /mnt/achdata
```

Next we need to find the unique identifier for our new drive. In Linux this is called the UUID (Universally Unique ID). The "blkid" command will list them all, but we only care about drive **sdc**:

```
sudo blkid | grep /dev/sdc
/dev/sdc: UUID="7b888f4c-0493-4870-8a57-638fac33c3dc" TYPE="ext4"
```

Instead of asking your system to mount whatever happens to be on /dev/sdc - which can change in the future! - we're going to locate and mount the new storage by its UUID.

Add the following entries to /etc/fstab. Grab the

```
UUID="hex_uuid"
```

from the above output (including the equals sign and double quotes) and put it in the first line you add to /etc/fstab below:

```
sudo nano /etc/fstab
```

```
UUID="7b888f4c-0493-4870-8a57-638fac33c3dc" /mnt/achdata ext4 defaults 0 0
/mnt/achdata/zeek/remotelogs/ /opt/zeek/remotelogs/ none defaults,bind 0 0
/mnt/achdata/zeek/remotelogs/ /opt/bro/remotelogs/ none defaults,bind 0 0
/mnt/achdata/volumes/ /var/lib/docker/volumes/ none defaults,bind 0 0
```

Now, mount *just* the new drive (*not* the bind mounts):

```
mount /mnt/achdata
```

and create the directories that will hold the zeek logs and docker content:

```
sudo mkdir -p /mnt/achdata/zeek/remotelogs/
sudo mkdir -p /mnt/achdata/volumes/
sudo chown root.root /mnt/achdata/zeek /mnt/achdata/volumes
```

Shut down AC-Hunter and BeaKer

AC-Hunter and BeaKer will not be available for use from when you run the following commands until you reach the end of this document.

```
sudo hunt down
sudo beaker down
```

At this point, running

```
sudo docker ps
```

should have no running containers - it should only show a header line starting with "CONTAINER….". If you have other containers running, please contact support@activecountermeasures.com before proceeding.

Now shut down docker:

```
sudo systemctl stop docker.service
sudo systemctl stop docker.socket
sudo systemctl status docker.service
sudo systemctl status docker.socket
```

Both of the previous commands should show "Active: inactive (dead)...". Contact support if they don't.

Move Zeek logs to the new drive

```
cd /mnt/achdata/
```

```
sudo chown root.root zeek
sudo chmod 755 zeek
sudo chown dataimport.dataimport zeek/remotelogs/
```

Do a test run of the file transfer. Make sure all paths in rsync commands end in slashes. Also, note that the "--dry-run" and "--remove-source-files" options start with two dashes; some word processors may replace this with a single dash, unfortunately.

```
sudo rsync --dry-run -av /opt/zeek/remotelogs/
/mnt/achdata/zeek/remotelogs/ --remove-source-files
```

If all looks good, rerun the above without "--dry-run" to actually move the files:

```
sudo rsync -av /opt/zeek/remotelogs/ /mnt/achdata/zeek/remotelogs/
--remove-source-files
```

If you get errors in this transfer, figure out why before continuing.

Move databases to the new drive

```
cd /mnt/achdata/
sudo chown root.root volumes
sudo chmod 701 volumes
```

Do a test run of the file transfer. Make sure all paths in rsync commands end in slashes:

```
sudo rsync --dry-run -av /var/lib/docker/volumes/
/mnt/achdata/volumes/ --remove-source-files
```

If all looks good, rerun the above without "--dry-run" to actually move the files:

```
sudo rsync -av /var/lib/docker/volumes/ /mnt/achdata/volumes/
--remove-source-files
```

If you get errors in this transfer, figure out why before continuing.

Cleanup old links and directories

The following commands clean up the original trees in which the Zeek logs and docker content were stored.

```
sudo rm -f /opt/zeek/remotelogs/remotelogs
sudo rmdir /opt/zeek/remotelogs || sudo rm -f /opt/zeek/remotelogs
sudo mkdir -p /opt/zeek/remotelogs
sudo chown dataimport.dataimport /opt/zeek/remotelogs
sudo rm -f /opt/bro/remotelogs/remotelogs
sudo rmdir /opt/bro/remotelogs || sudo rm -f /opt/bro/remotelogs
sudo mkdir -p /opt/bro/remotelogs
sudo chown dataimport.dataimport /opt/bro/remotelogs
sudo find /var/lib/docker/volumes/ -type d -delete
sudo mkdir /var/lib/docker/volumes/
sudo chown root.root /var/lib/docker/volumes
sudo chmod 701 /var/lib/docker/volumes/
```

Tell Linux to present those files back in the old locations

The following commands use the second, third, and fourth lines you added to /etc/fstab to set up two "bind mounts". These instruct the linux kernel to 1) present everything found under /mnt/achdata/zeek/remotelogs/ under both /opt/zeek/remotelogs/ and /opt/bro/remotelogs/, and 2) present everything found under /mnt/achdata/volumes under /var/lib/docker/volumes/ too. Bind mounts are similar to symbolic links, but work around a limitation in docker that doesn't respect symbolic links in the way you'd expect.

```
sudo mount /opt/zeek/remotelogs/
sudo mount /opt/bro/remotelogs/
sudo mount /var/lib/docker/volumes/
```

Check that these directories are mounted in the new drive space:

```
sudo df -h /opt/zeek/remotelogs/
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdc        1.6T  1.1G  1.5T   1% /opt/zeek/remotelogs

sudo df -h /opt/bro/remotelogs/
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdc        1.6T  1.1G  1.5T   1% /opt/bro/remotelogs

sudo df -h /var/lib/docker/volumes/
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdc        1.6T  1.1G  1.5T   1% /var/lib/docker/volumes
```

Your sizes will differ, but the "Size" column should match the size of the new drive you added.

Reboot

```
sudo reboot
```

Because you've made changes to the directory trees used on that Linux system (and any running processes may still be using the old content trees), a full reboot is *strongly* recommended.

Restart containers and check that everything works

Please run

```
sudo hunt up -d
sudo beaker up -d
sleep 60
sudo docker ps
```

You should see a list of running docker containers: 4 or 5 for AC-Hunter and 2 for beaker. The CREATED and STATUS times for all containers should be within a minute or so of each other.

Check that these directories are mounted in the new drive space:

```
sudo df -h /opt/zeek/remotelogs/
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdc        1.6T  1.1G  1.5T   1% /opt/zeek/remotelogs

sudo df -h /opt/bro/remotelogs/
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdc        1.6T  1.1G  1.5T   1% /opt/bro/remotelogs

sudo df -h /var/lib/docker/volumes/
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdc        1.6T  1.1G  1.5T   1% /var/lib/docker/volumes
```

Finally, log in to your AC-Hunter web interface and look up a recent connection in BeaKer.

Closing thoughts

Logical Volume Management

While we don't cover it in this FAQ, you may be able to simply add space that's already on your system to your "/opt/zeek/remotelogs/" , "/var/lib/docker/volumes/", and/or "/" mount points if your system was set up using Logical Volume Management (LVM). To see if this is enabled at all, please run:

```
sudo vgdisplay
```

If you do *not* have LVM enabled, this will likely return "`No volume groups found`".

If you get anything else you may be able to add space to the logical volume (LV) that's currently too small. Please check with your sysadmin to walk through these steps.

SELinux

We strongly discourage using SELinux on your AC-Hunter system; the AC-Hunter suite (and especially the Docker software on which it runs) is not currently compatible with SELinux' restrictions.

With that said, if you are using SELinux and have followed the above steps, you should relabel your files so that the directories and files you've moved have the correct selinux labels. The best way to do this is to run:

```
sudo touch /.autorelabel
sudo reboot
```

If this is not possible, there's a second approach of running:

```
fixfiles relabel
```

, but the changed labels will not apply to running applications (which will eventually require a reboot anyways.)

Resizing a cloud volume

If you followed the above steps to add a volume on a cloud instance, it may be possible to add more space to that volume later if more space is needed. Please consult your cloud provider's documentation for the steps and costs.

Unfortunately, it is extremely difficult to safely *shrink* a volume if you made it too big, and many providers simply do not offer that option.

Archiving logs

One final way to recover space is to move any old logs to archival storage. AC-Hunter's automatic log transfer and import process is only interested in logs from the previous 72 complete hours; anything older than this can be deleted or moved to secondary storage as appropriate.

Improving this document

If you find mistakes or things that should be included but aren't, we'd appreciate your feedback. Please contact support@activecountermeasures.com with any suggestions.