Troubleshoot User Access

Andrew Mallett

Author and Trainer

@theurbanpenguin www.theurbanpenguin.com

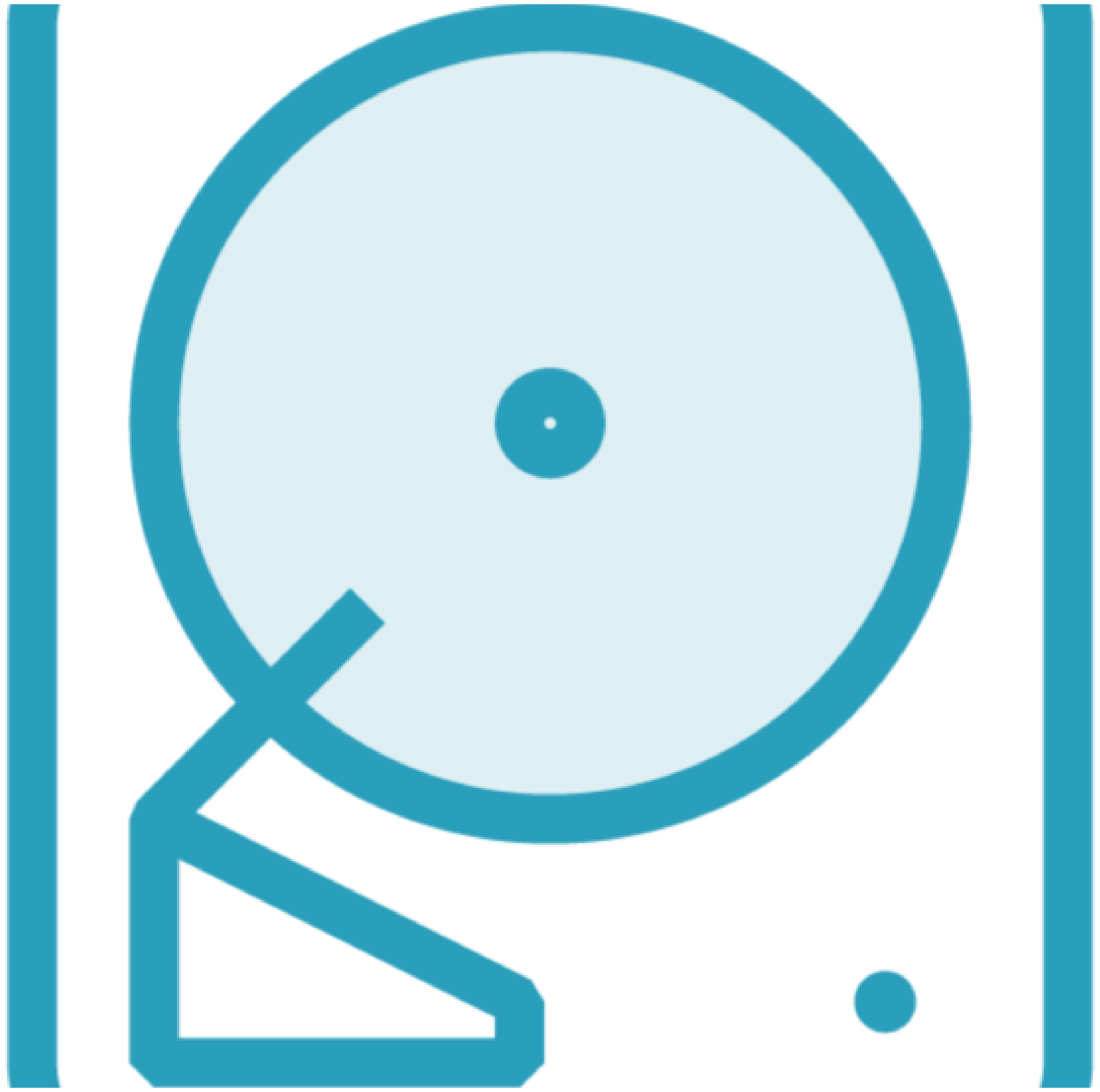
Overview

Managing and Troubleshooting User Issues

- Disk quotas
- Login issues
- Password issues
- File access
- Sudo and privilege escalation

Quotas

Disk Quotas



Quotas can be used to limit user's space on a per user of per group basis

- install quotas
- check quota modules
- mount options
- enable quotas
- create limits
- report on usage

```
$ sudo apt update
$ sudo apt install -y quota
$ quota --version
```

Installing Quota Tools

We will use the Ubuntu system and install the quota management tools.

```
$ find /lib/modules/ -type f -name '*quota_v*.ko*'
$ sudo apt install linux-image-extra-virtual
$ find /lib/modules/ -type f -name '*quota_v*.ko*'
```

Cloud-Based = Cut Down

In general, cloud-based systems including Vagrant, will have a smaller customized install base. This means that we may not have the quota filesystem modules needed. If they are missing, we can install them.

Demo

To begin we will install the quota tools and drivers:

- Install quota
- Check kernel modules and install if required

Configuring Quotas

```
$ sudo vim /etc/fstab
add options usrquota,grpquota
$ sudo mount -o remount /
$ mount -t ext4
$ sudo quotacheck -ugm /
$ ls /aquota*
$ sudo modprobe quota_v1 && sudo modprobe quota_v2
$ sudo quotaon -v /
```

Quotas are Configured Per Filesystem

We now must configure quotas which are set as mount options on filesystems. We can add eiter or both options for users and groups. We establish the databases with quotacheck. We can reboot or load the modules and enable quotas for the root filesystem. We just need to set quotas for our users or groups

Demo

Enable Quotas:

- Root filesystem
- Set quotas
- Report on quotas

I Can't Login!

Login Issues

Gather Information:

- login name, what name are they typing including case
- passwd -S <user>
- chage -L <user>
- console or ssh?
- message displayed
- lastb

Demo

Research Login Issues:

- SSH settings
- Password aging and locking
- Lastb

Password Quality

Default Quality

Minimum 6 characters
1 Uppercase
1 Lowercase
1 Number

```
$ grep '^password' /etc/pam.d/common-password
$ man pam_unix | less +/obscure
```

Default Password Complexity

The password complexity is set in the common-password file and the pam_unix.so module. The complexity rules are made by the obscure option.

```
$ sudo vim /etc/pam.d/common-password
password [success=1 default=ignore] pam_unix.so sha512 minlen=4
```

Reduce or Increase Password Length / Remove Default Complexity

The default minimum length of a password is 6 characters. We can increase or lower the value. Here we set it to 4 characters and have also remove the obscure keyword taking away the password complexity rules.

```
$ sudo vim /etc/pam.d/common-password
password [success=1 default=ignore] pam_unix.so sha512 minlen=8 obscure remember=5
```

Remember Old Passwords

Here we set the minimum length to 8 characters, we restore the complexity requirement additionally adding password history where the last 5 password are stored for a use in the /etc/security/opasswd file.

Demo

Investigating Password Complexity:

- common-password
- pam_unix
- /etc/security/opasswd

File Access

Troubleshoot File Access

We need to consider the user, their groups, the file mode, ACLS and MACLS such as SELinux.

Never forget the user may not have the correct path or filename.

ID Command

1ST

User ID : Check the User Permissions

2ND

Groups: Check permissions for the groups the use belongs to

3RD

No more than 64 groups: More than 64 group memberships will cause problems

```
$ sudo ausearch -m AVC -ts recent
```

SELinux

If SELinux is enforcing mode where installed, check to see if SELinux is blocking access.

Escalation

```
$ sudo -l
$ sudo --preserve-env=EDITOR visudo

Defaults env_keep += "EDITOR"
```

Checking Sudo Escalation

A user can always check what they are allowed to do with sudo -l. Often though the problem relates to environment variables not being carried through. My approach is to add the variables I need for each command, but we could also allow variables in the sudoers file.

Demo

Investigating Sudo and Variables:

- --preserve-env
- env_keep

Summary

Managing and User Access

- Disk quotas
- Login issues
- Password issues
- File access
- Sudo and privilege escalation

Up Next:
Diagnose Issues Using Systemd