# CSK

Contents

[CSK 1](#_Toc192769214)

[System Hardening: 2](#_Toc192769215)

[Principle of Least Privilege 2](#_Toc192769216)

[Limit Node Access 3](#_Toc192769217)

[Remove Obsolete Packages 11](#_Toc192769218)

[Disable Open ports 14](#_Toc192769219)

[IAM and Roles in AWS 16](#_Toc192769220)

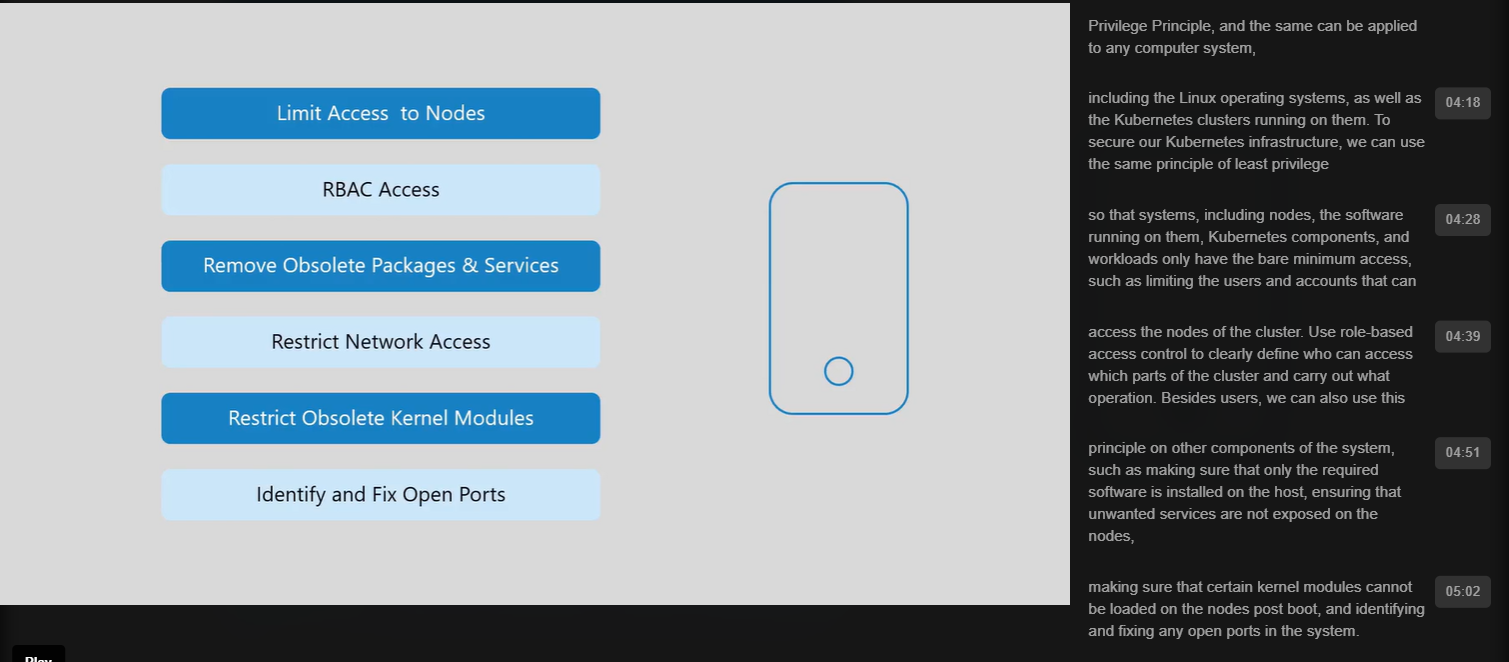
[UFW – Uncomplicated Firewall 16](#_Toc192769221)

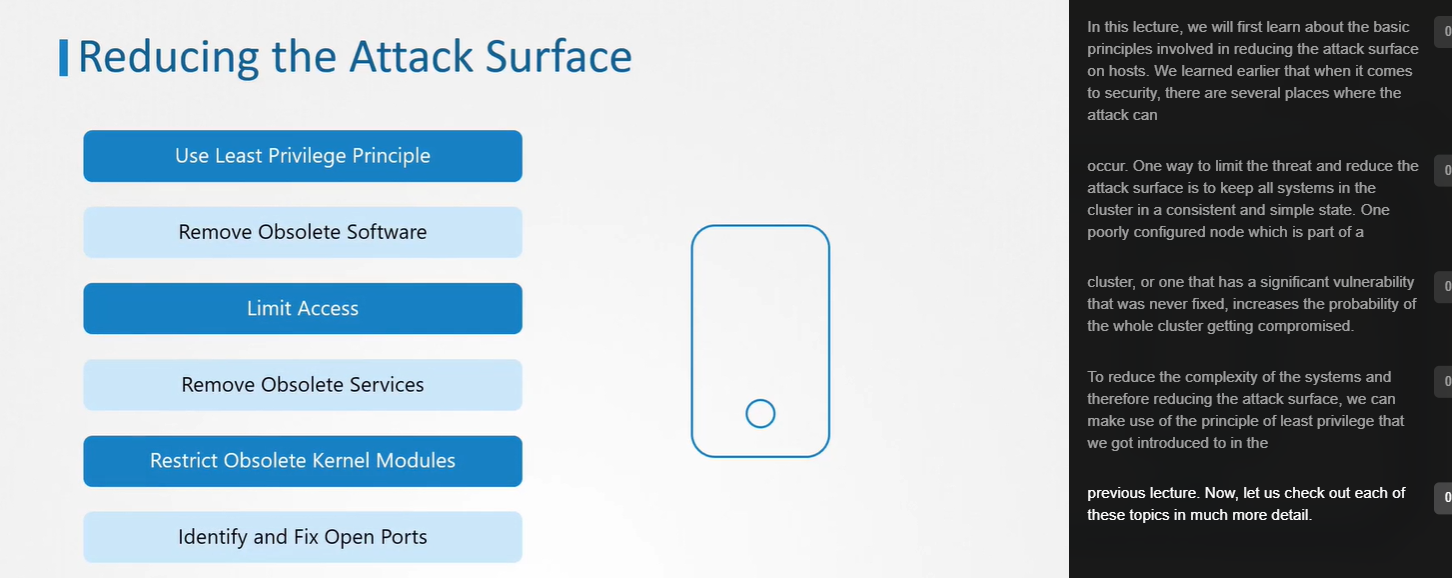
[SysCalls 21](#_Toc192769222)

[Linux Capabilities 41](#_Toc192769223)

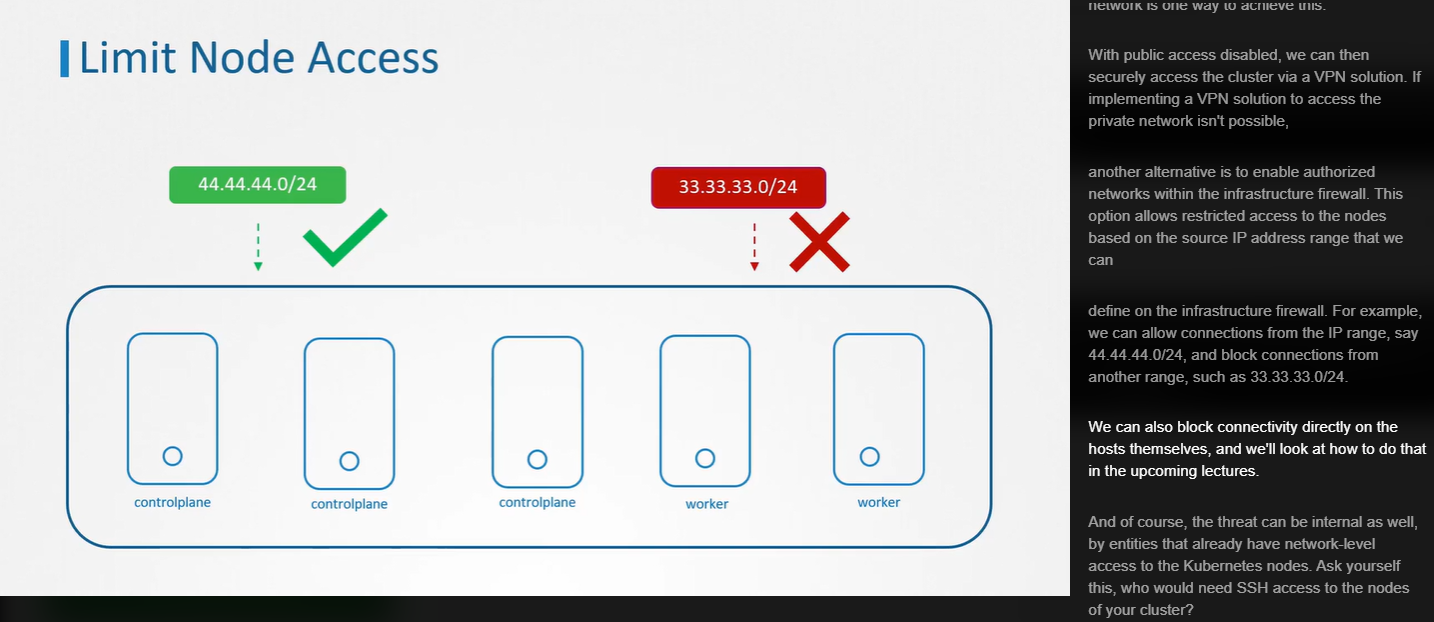
## System Hardening:

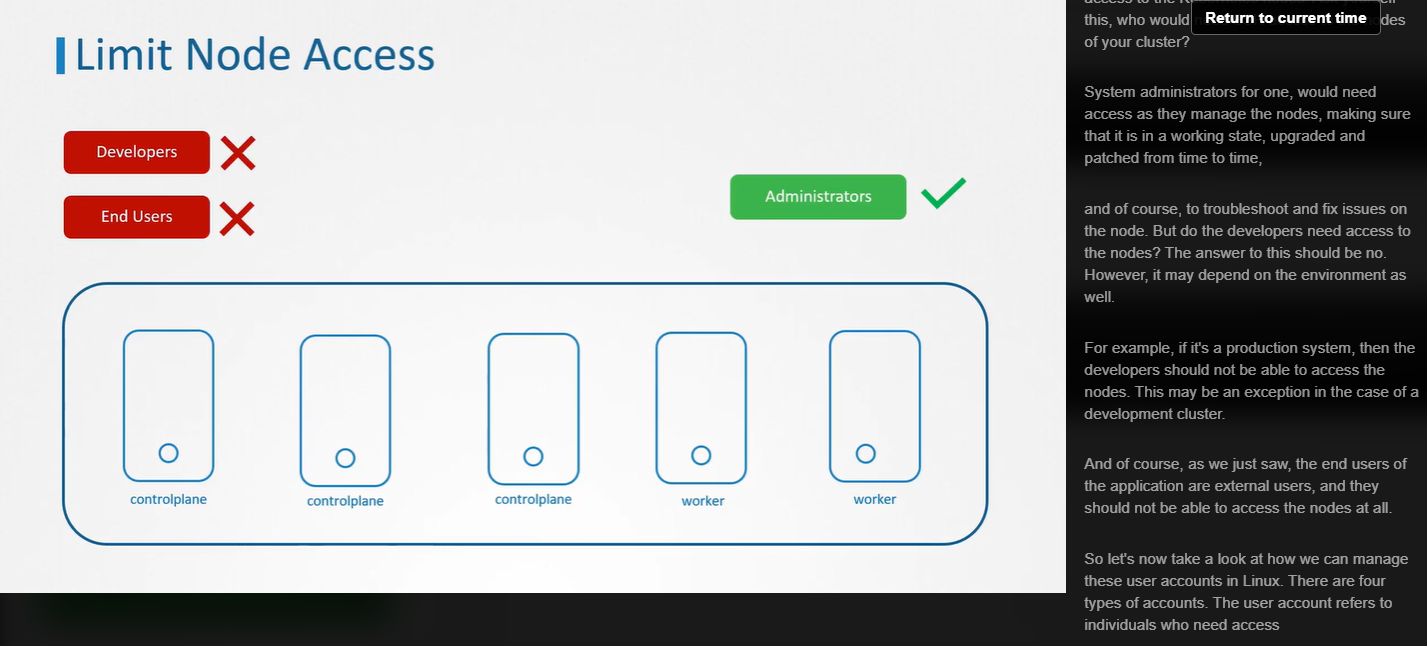
### Principle of Least Privilege



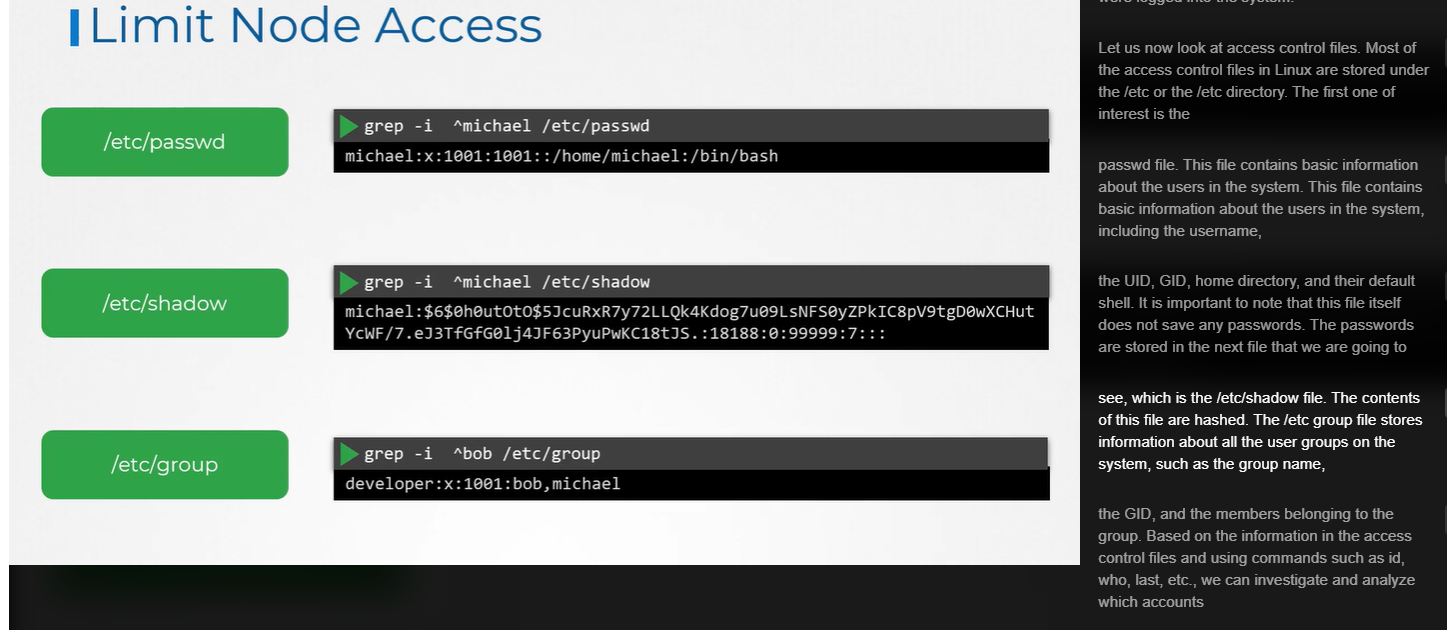


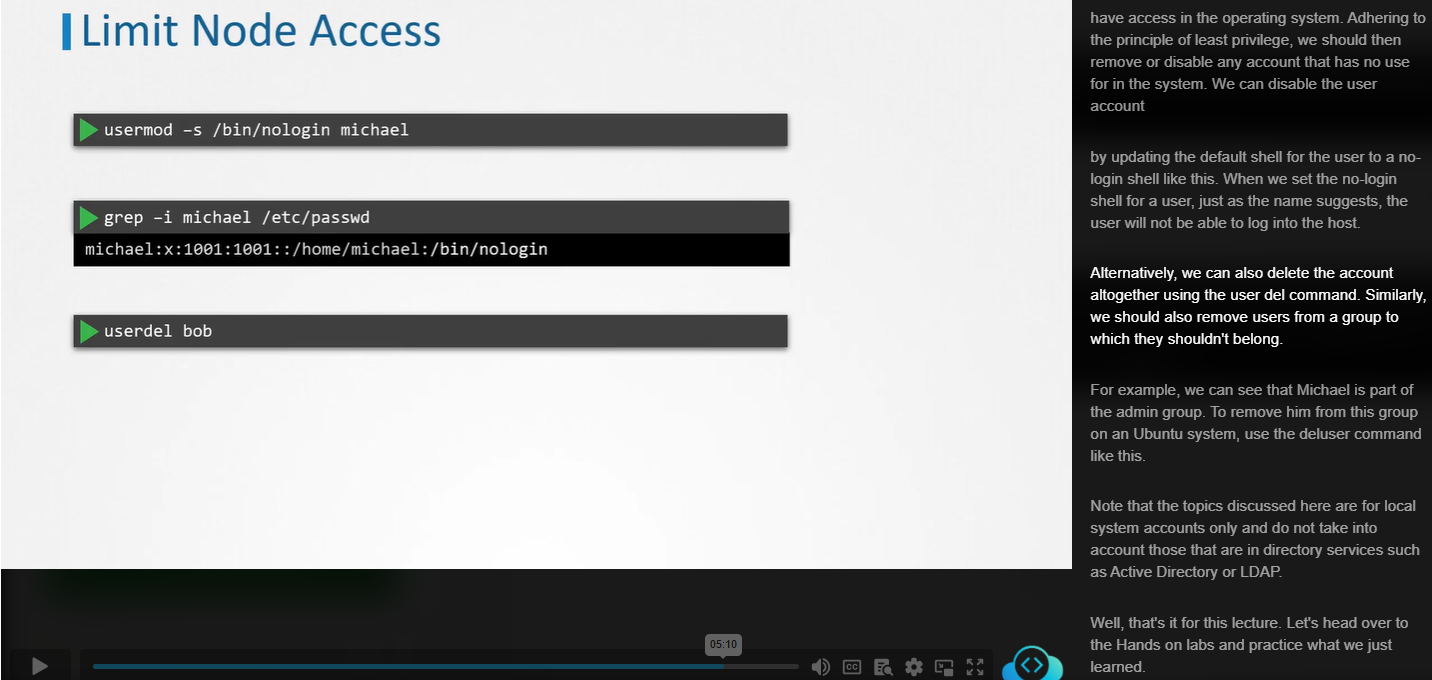
### Limit Node Access





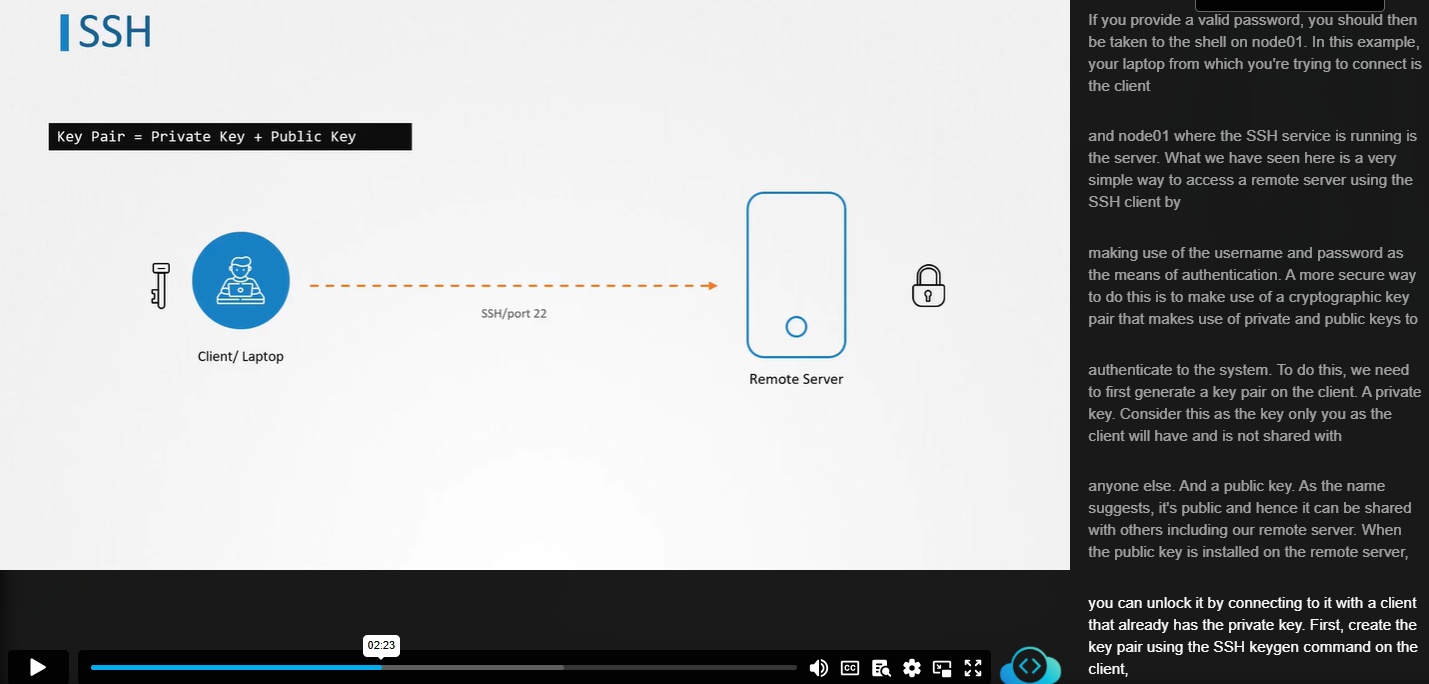




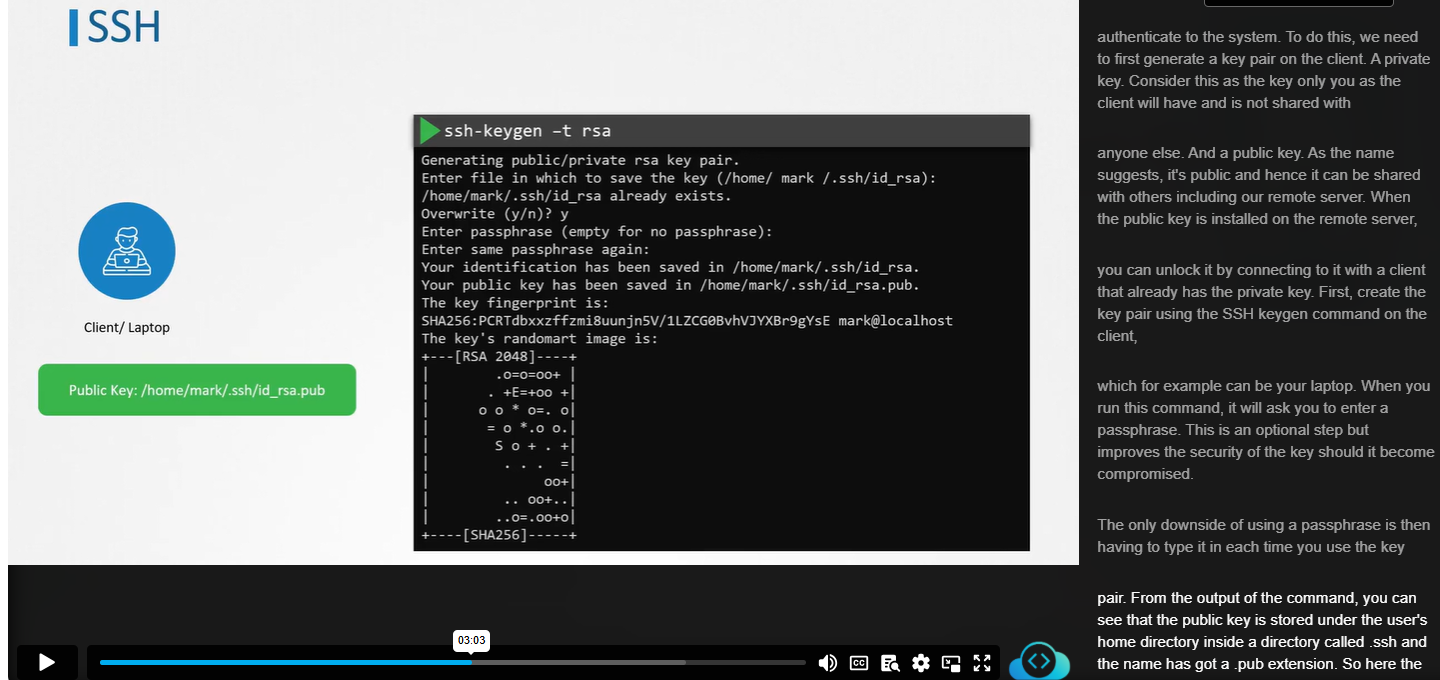


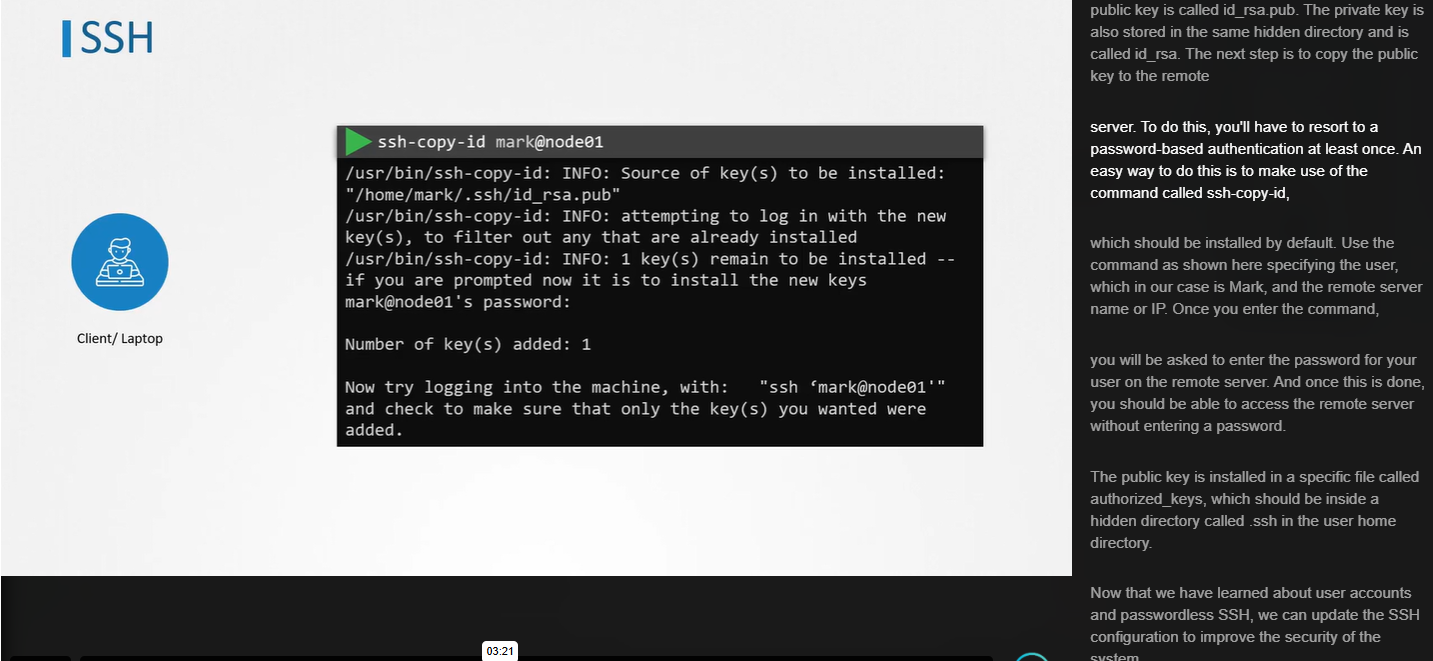


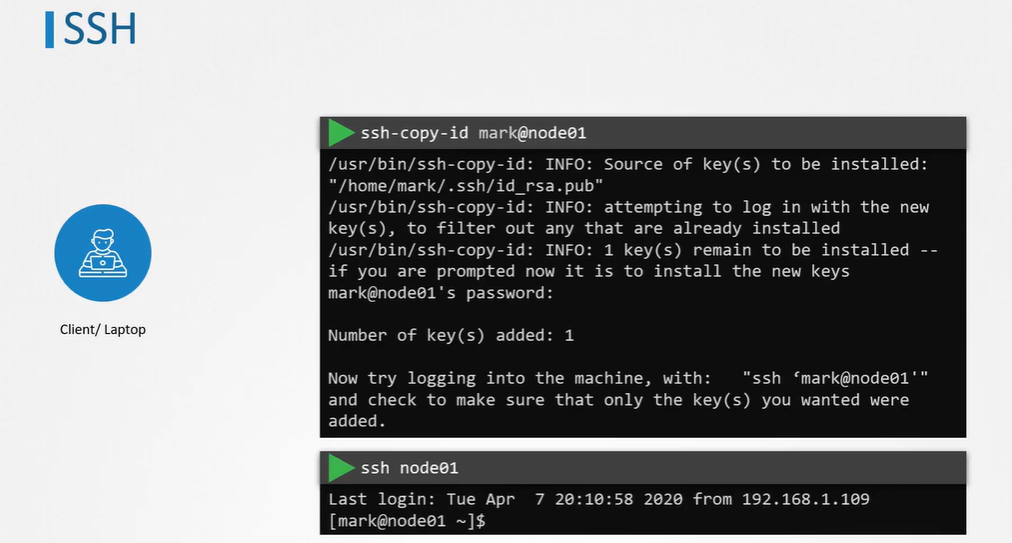
#### Ssh connection to Node –



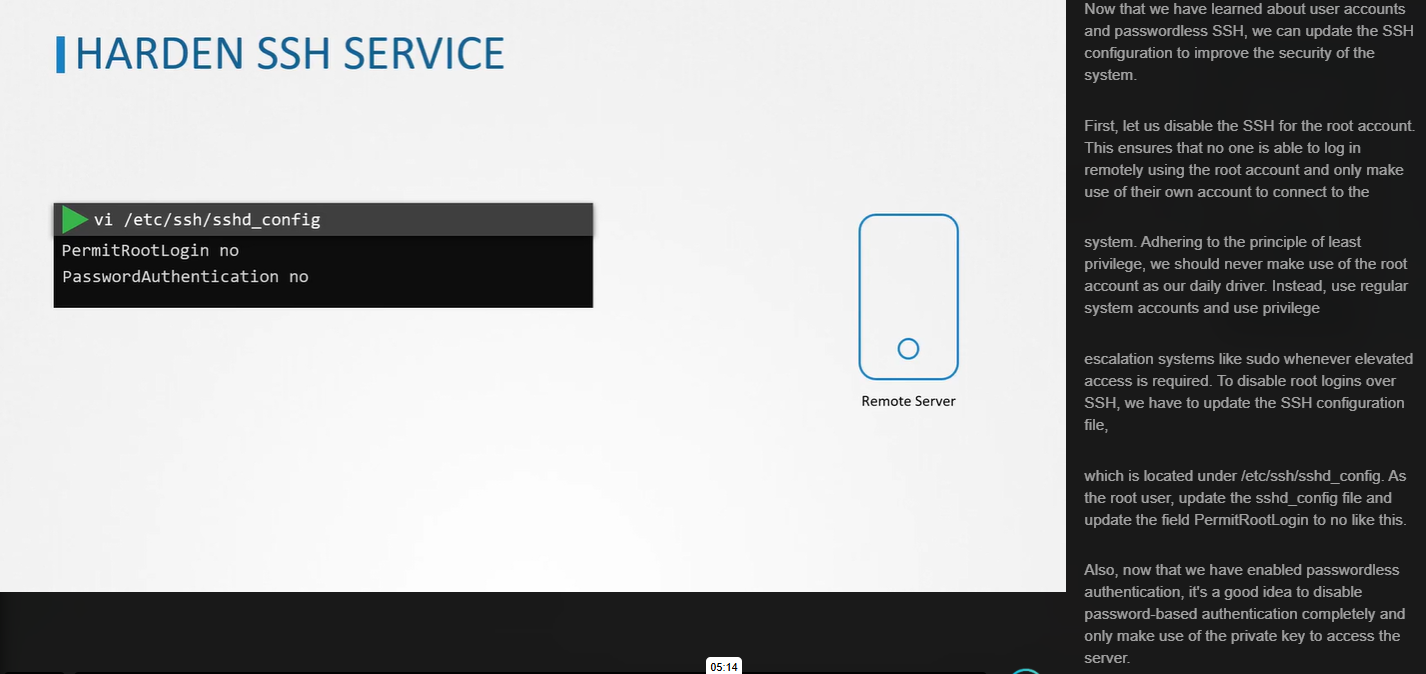
Public and Private Key

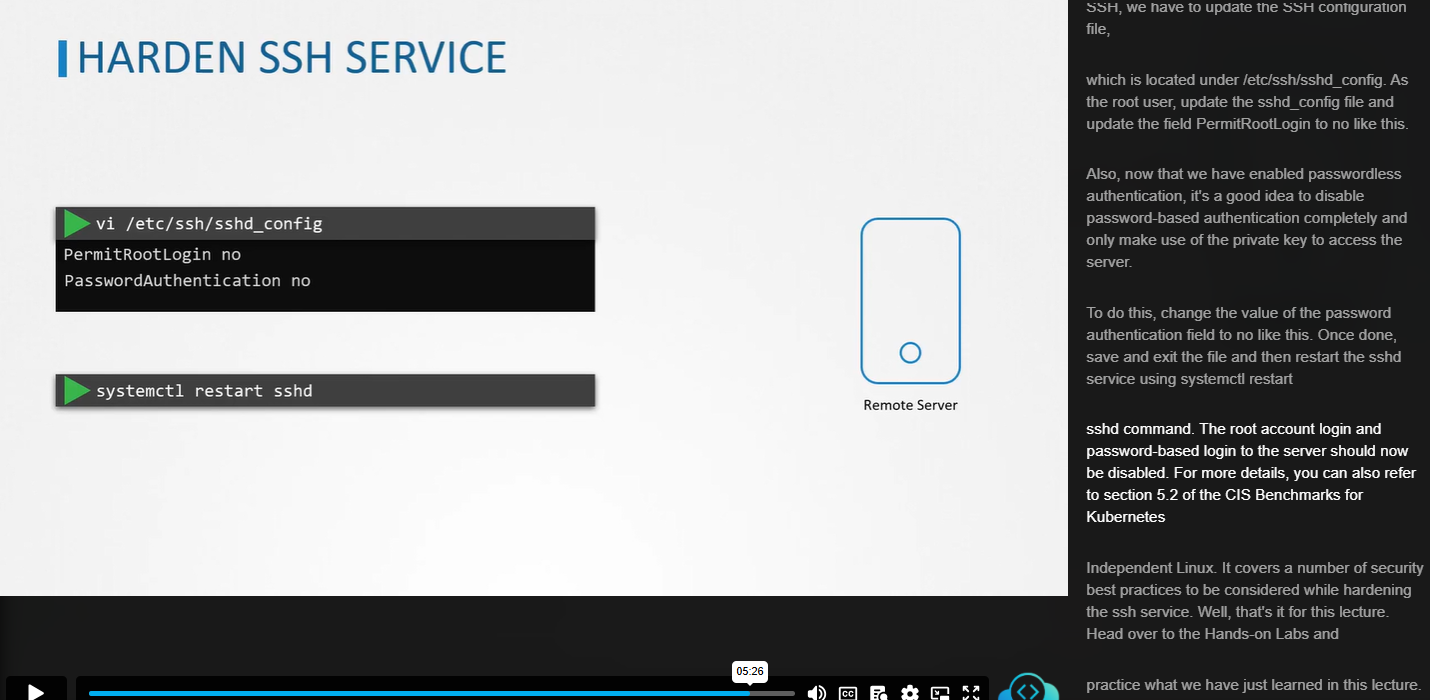


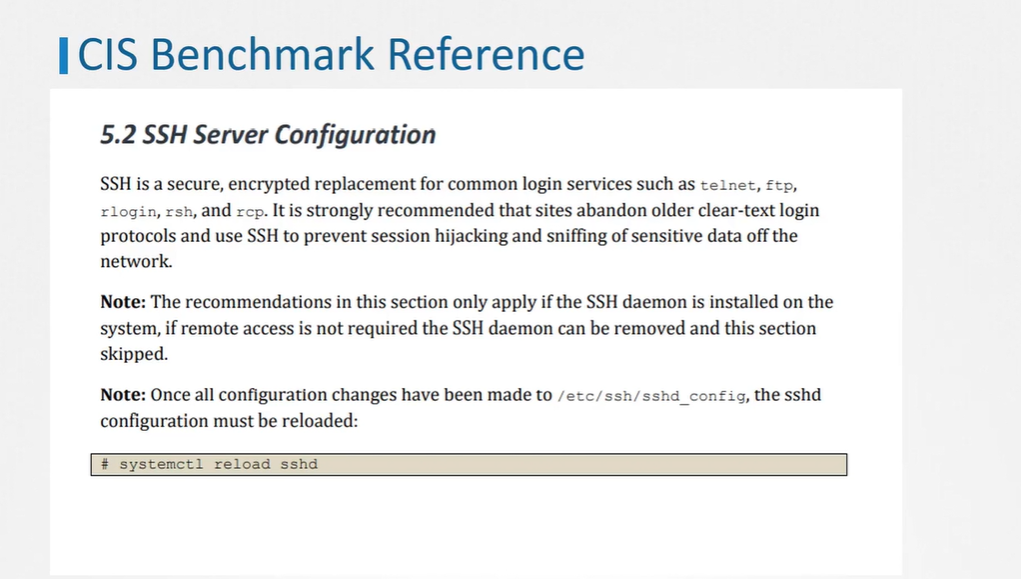




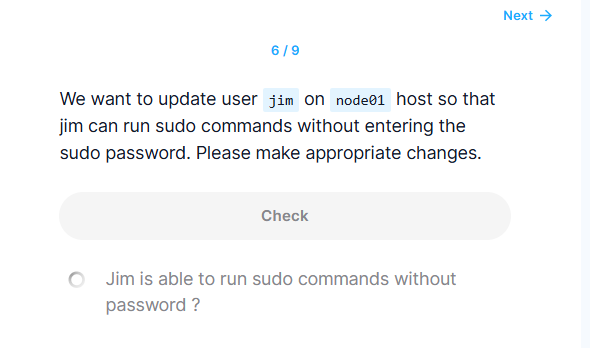


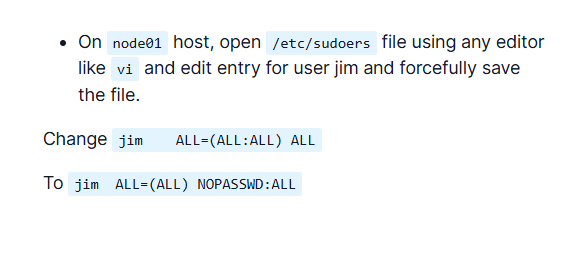






#### Sudo User:





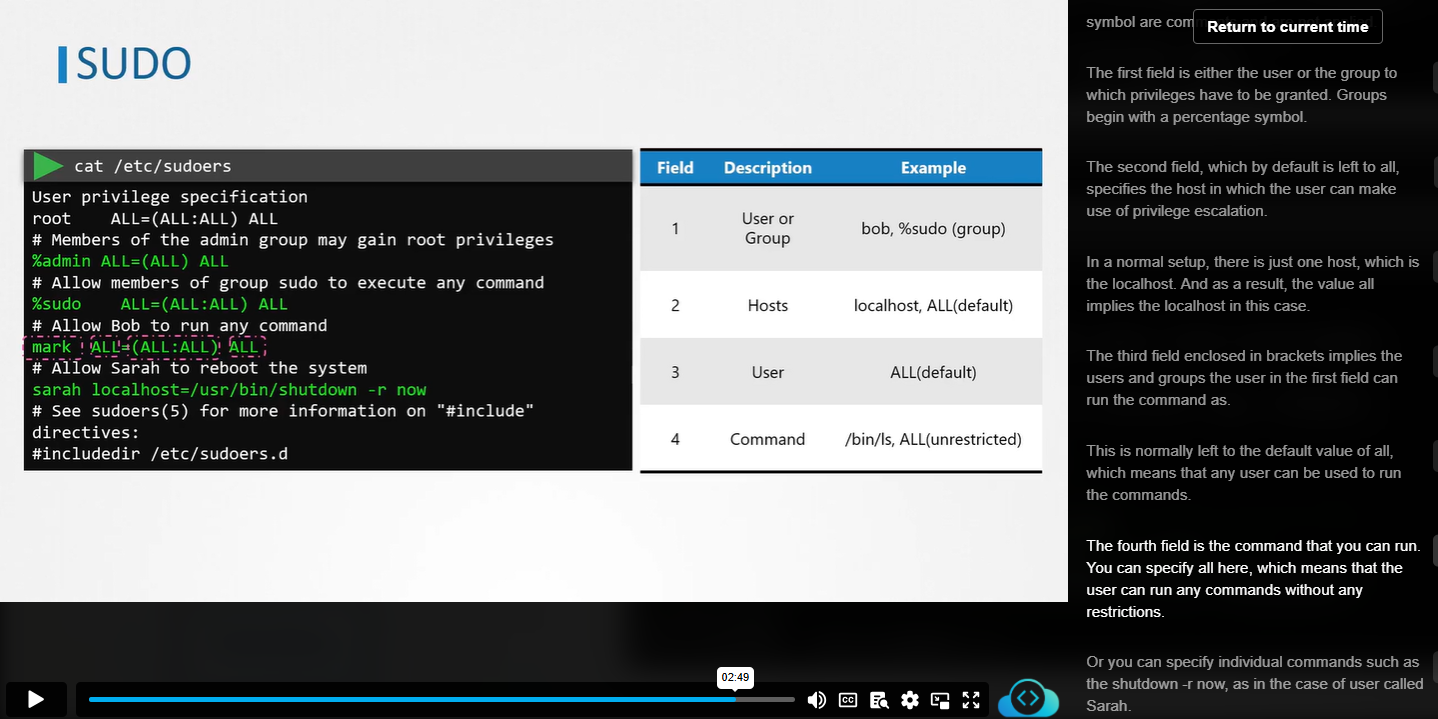
Question 2:

Add a new user rob on node01 host and set password to jid345kjf. We already have a sudo group i.e admin on this host. Make user rob member of the admin group so that he can become a sudo user. Do not to add the user directly in the sudoers file.

Answer:

* SSH into node01 host and create user rob:  
  adduser rob
* Make it member of admin group

usermod rob -G admin



*Create a user named jim on node01 host and configure password-less ssh access from controlplane host (from user root) to node01 host (to user jim).*

* ssh into node01 host from controlplane host

ssh node01

* Create user jim on node01 host

adduser jim (set any password you like)

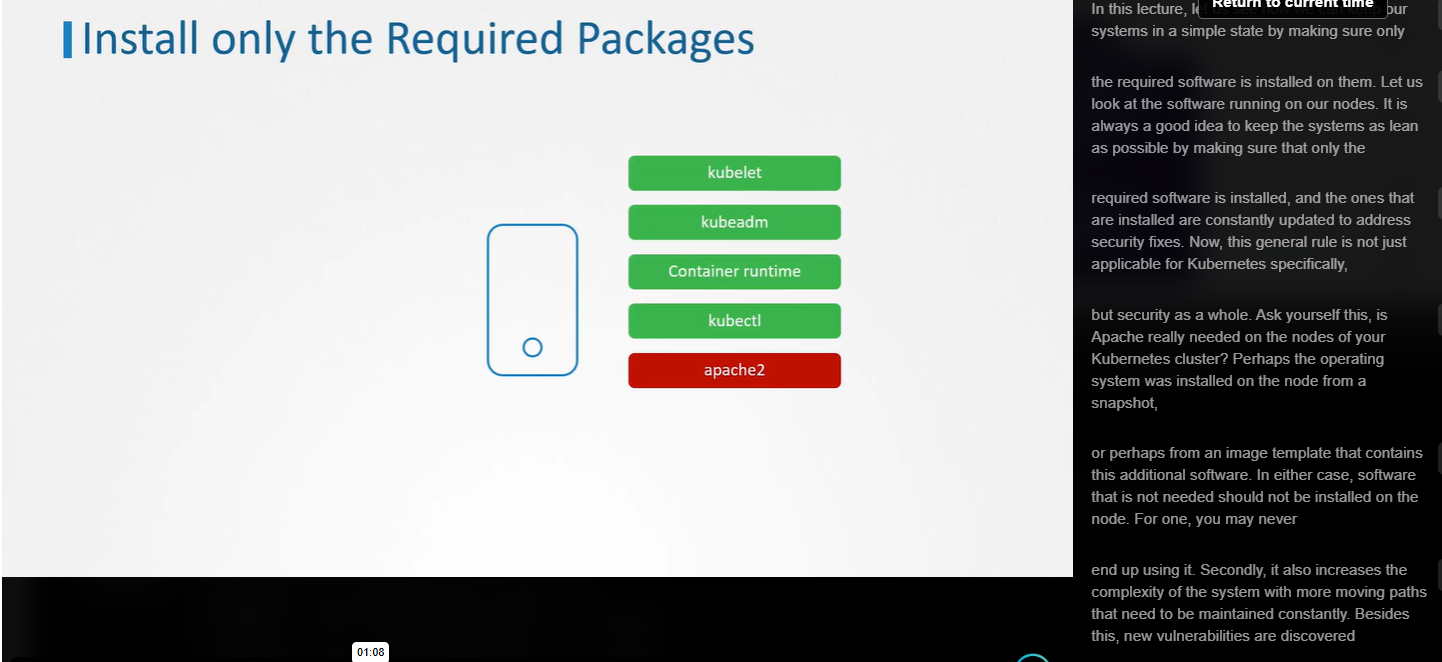
* Return back to controlplane host and copy ssh public key

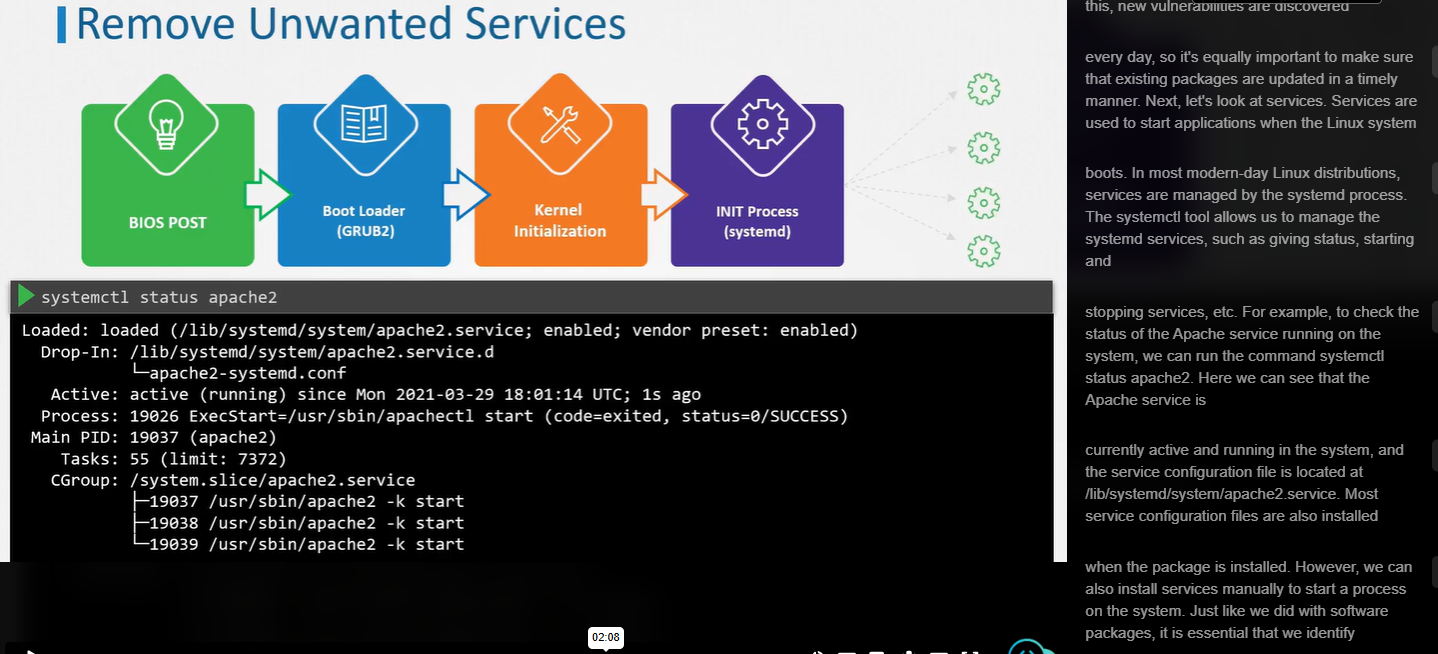
ssh-copy-id -i ~/.ssh/id\_rsa.pub jim@node01

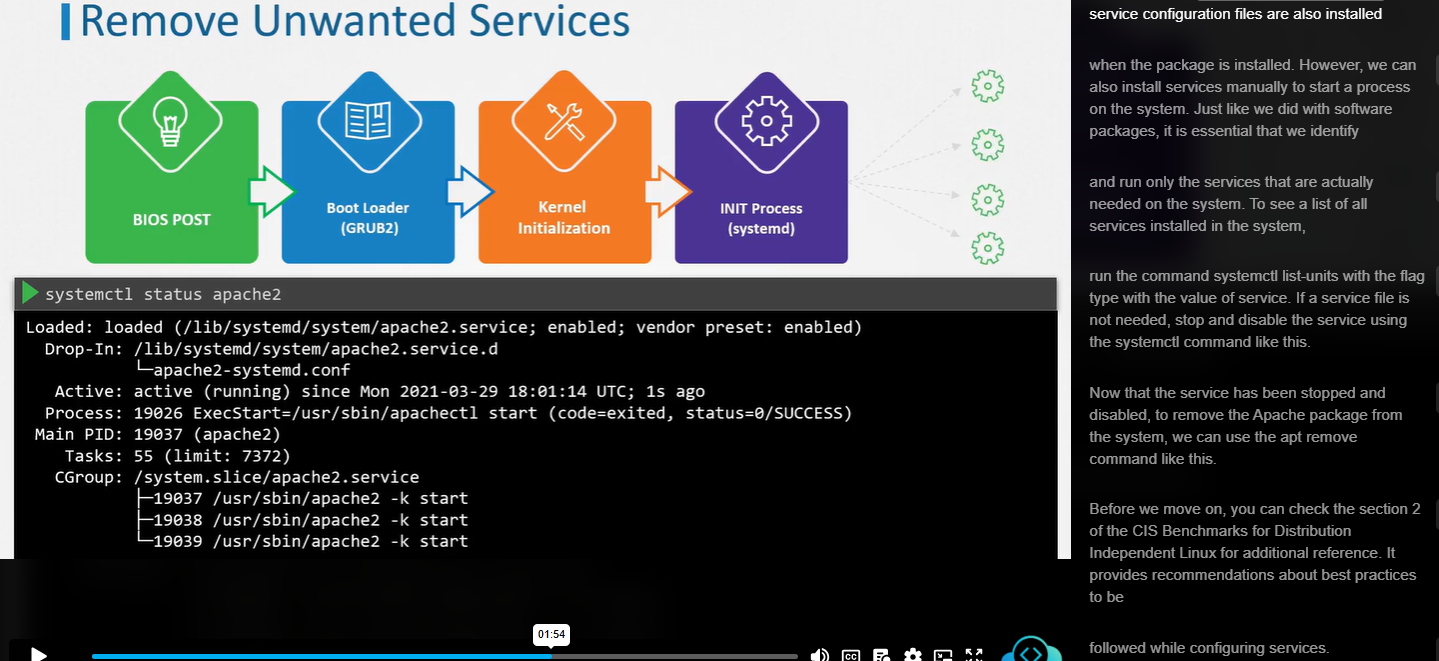
* Test ssh access from controlplane host

ssh jim@node01

### Remove Obsolete Packages







List all the services

$systemctl list-units –type service

To stop the service and disable it

$systemctl stop apache2

$systemctl disable apache2

To remove the apache

$apt remove apache2

<https://www.cisecurity.org/cis-benchmarks/>

Go to the **`Operating Systems`** section and search for the **`Distribution Independent Linux`**. Expand it to see more options, then download CIS Benchmark.

