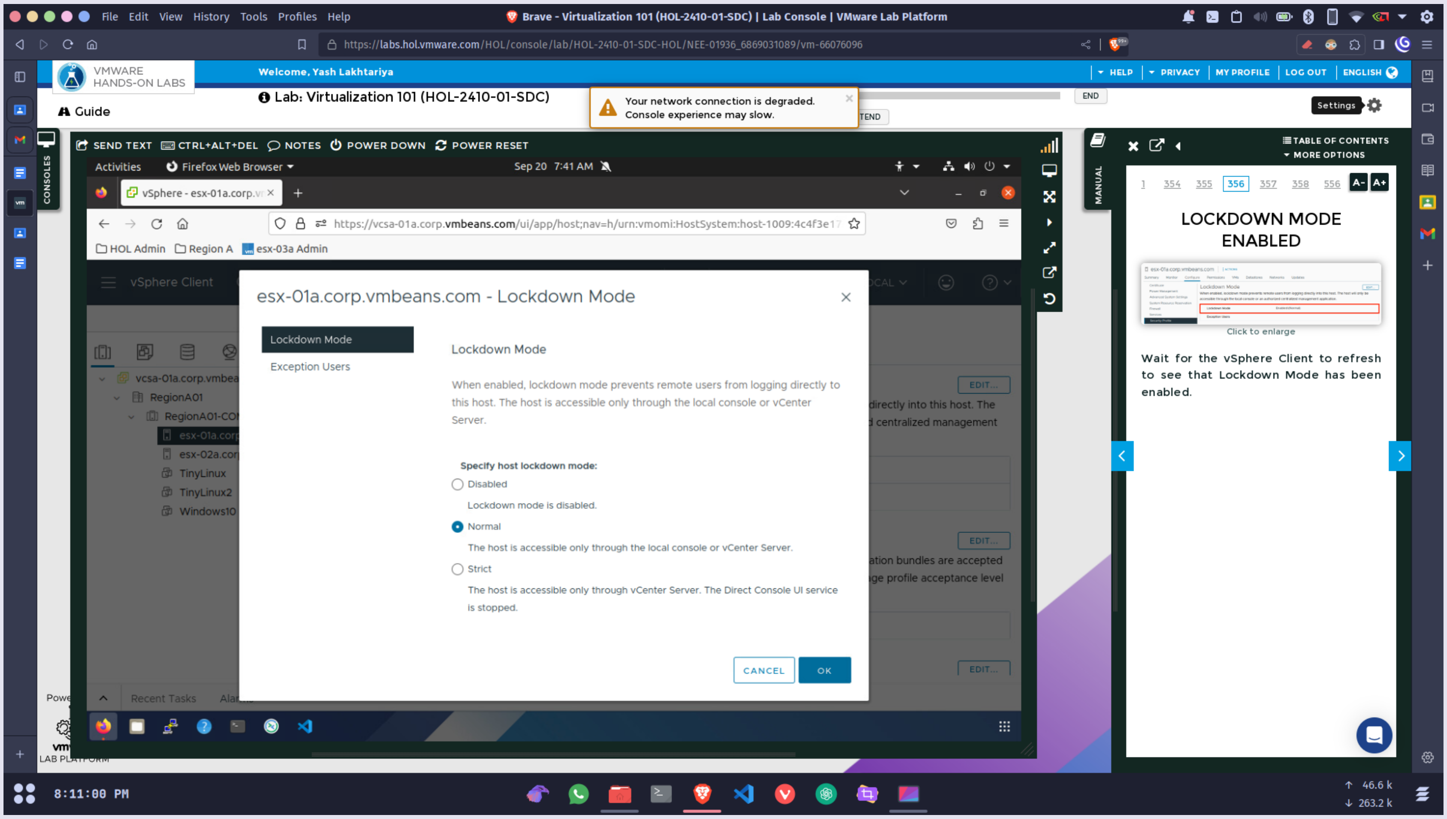
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 51
Virtualization Practical 5

Practical 5 : Configuring the host services and firewall

1. The unauthorized access can be prevented by enabling **host lockdown mode** and also exception users can be added.



esx-01a.corp.vmbeans.com - Lockdown Mode

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

○ Disabled

Lockdown mode is disabled.

● Normal

The host is accessible only through the local console or vCenter Server.

○ Strict

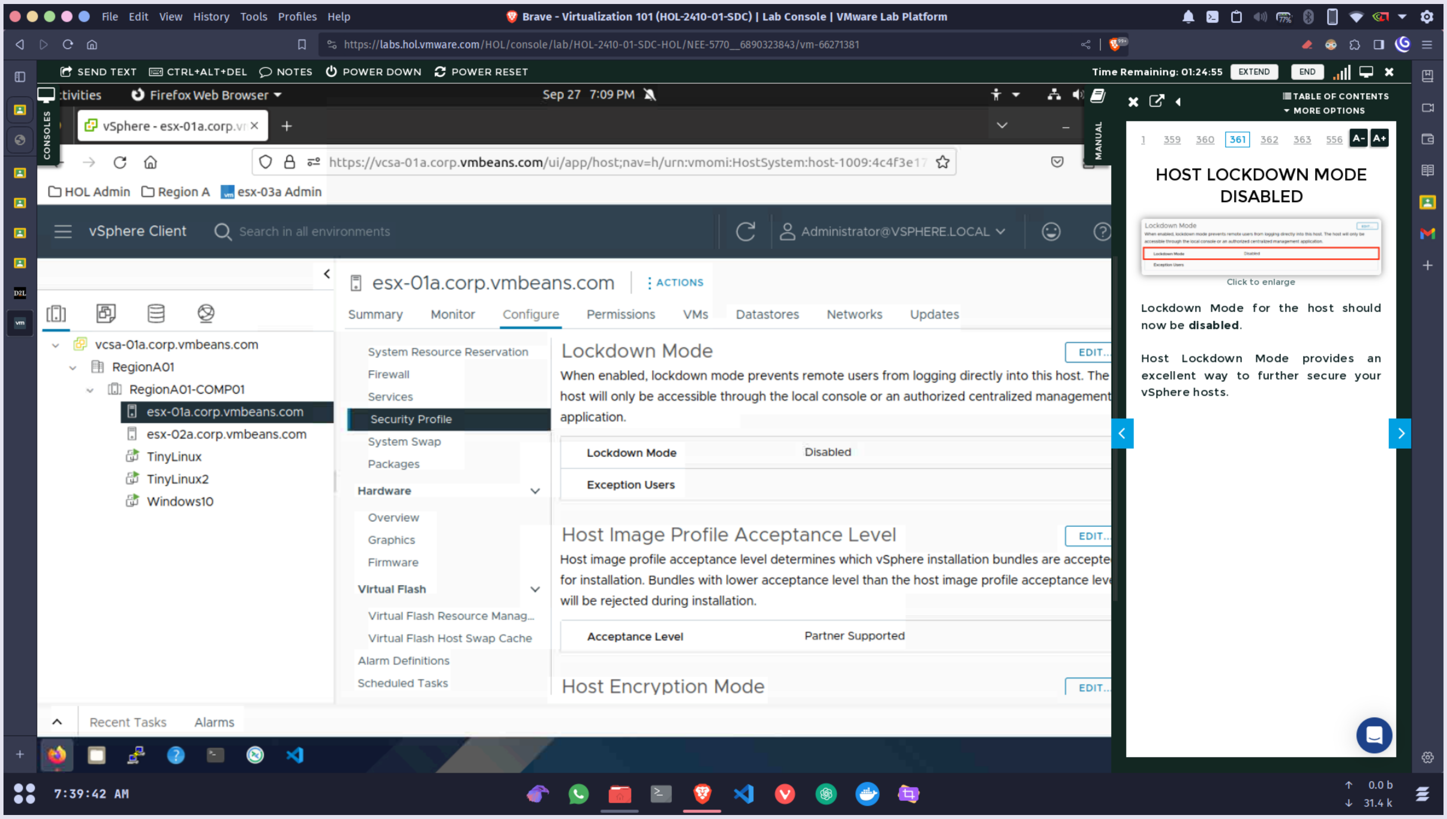
The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

LOCKDOWN MODE ENABLED

Wait for the vSphere Client to refresh to see that Lockdown Mode has been enabled.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 51
Virtualization Practical 5

2. Similarly from the options disable the host lockdown mode for esx01.



Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through the local console or an authorized centralized management application.

Lockdown Mode	Disabled
Exception Users	

Host Image Profile Acceptance Level

Host image profile acceptance level determines which vSphere installation bundles are accepte for installation. Bundles with lower acceptance level than the host image profile acceptance leve will be rejected during installation.

Acceptance Level	Partner Supported

Host Encryption Mode

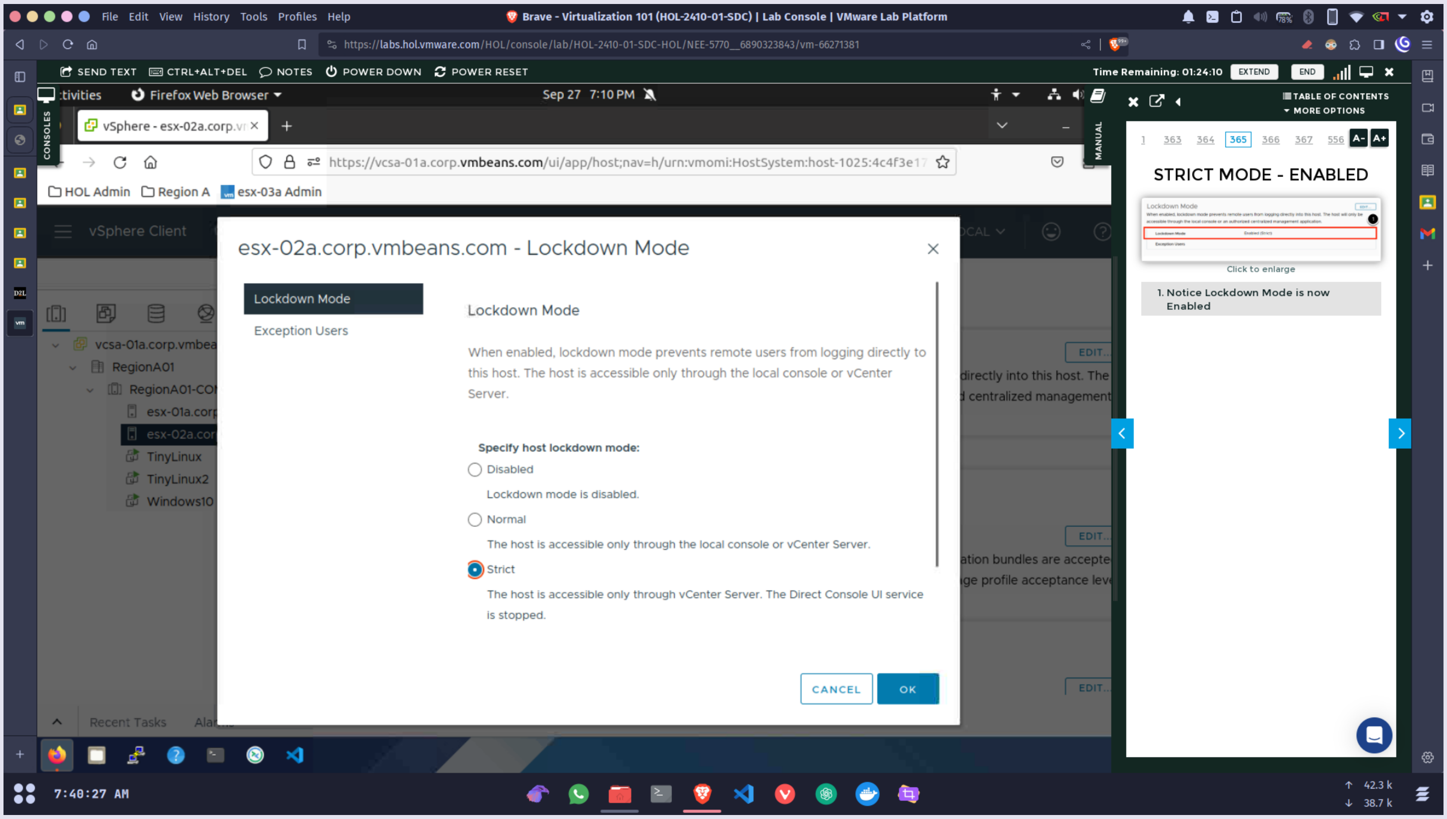
HOST LOCKDOWN MODE DISABLED

Lockdown Mode for the host should now be **disabled**.

Host Lockdown Mode provides an excellent way to further secure your vSphere hosts.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 51
Virtualization Practical 5

3. Now, enable strict lockdown mode for esx02 via its settings.



esx-02a.corp.vmbeans.com - Lockdown Mode

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

○ Disabled

Lockdown mode is disabled.

○ Normal

The host is accessible only through the local console or vCenter Server.

● Strict

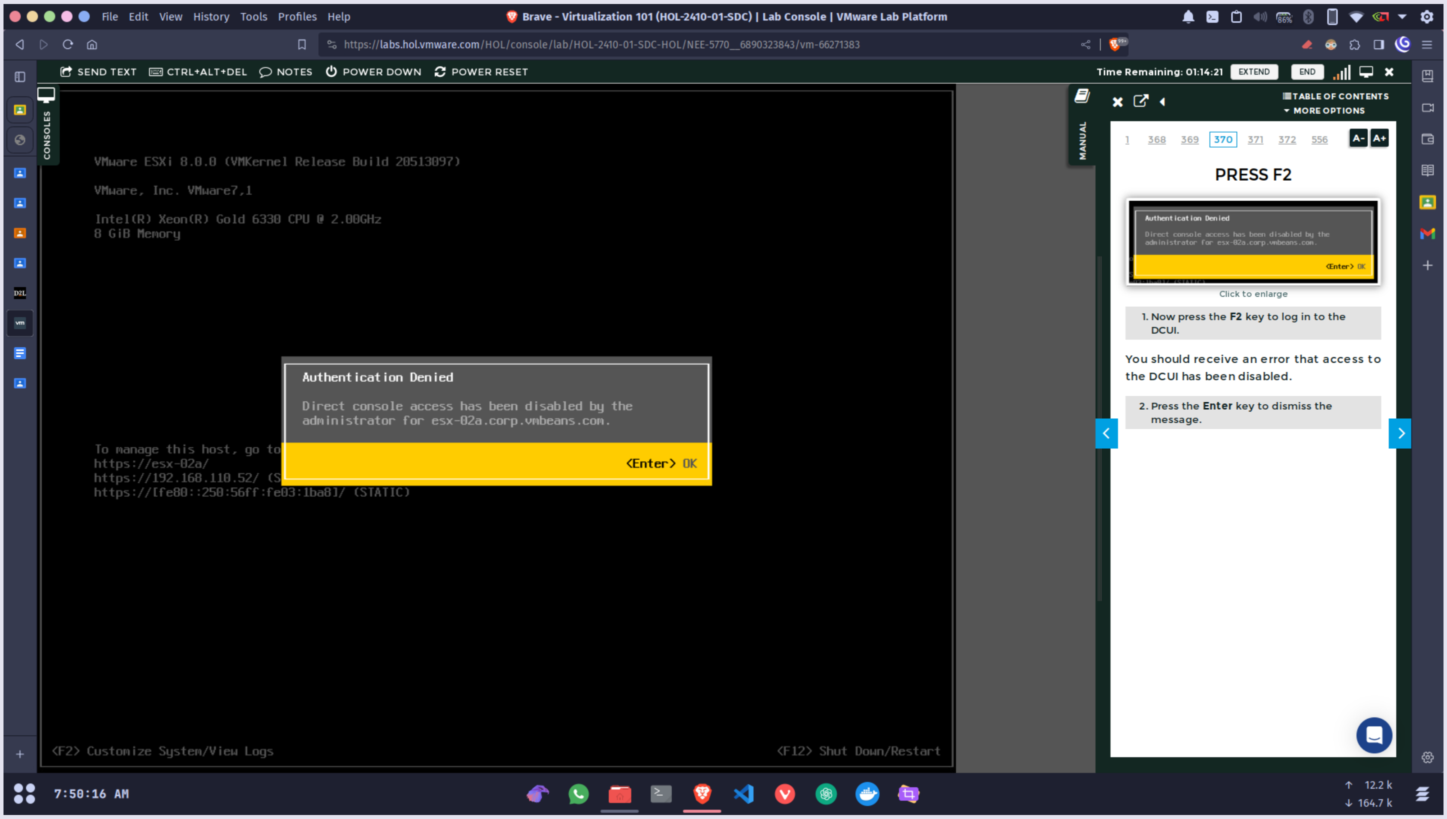
The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

STRICT MODE - ENABLED

1. Notice Lockdown Mode is now Enabled

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 51
Virtualization Practical 5

4. Hence, the access for ESX-02A is disabled if not logged in from the main console.



```
VMware ESXi 8.0.0 (VMKernel Release Build 20513097)

VMware, Inc. VMware7,1

Intel(R) Xeon(R) Gold 6330 CPU @ 2.00GHz
8 GiB Memory


To manage this host, go to
https://esx-02a/
https://192.168.110.52/ (S
https://[fe80::250:56ff:fe03:1ba8]/ (STATIC)

<F2> Customize System/View Logs                    <F12> Shut Down/Restart
```

```
Authentication Denied

Direct console access has been disabled by the
administrator for esx-02a.corp.vmbeans.com.

                                      <Enter> OK
```

Brave - Virtualization 101 (HOL-2410-01-SDC) | Lab Console | VMware Lab Platform
File Edit View History Tools Profiles Help
https://labs.hol.vmware.com/HOL/console/lab/HOL-2410-01-SDC-HOL/NEE-5770__6890323843/vm-66271383
SEND TEXT
CTRL+ALT+DEL
NOTES
POWER DOWN
POWER RESET
Time Remaining: 01:14:21
EXTEND
END
CONSOLES
MANUAL
TABLE OF CONTENTS
MORE OPTIONS
1 368 369 370 371 372 556
A- A+
7:50:16 AM
12.2 k
164.7 k

PRESS F2

Click to enlarge

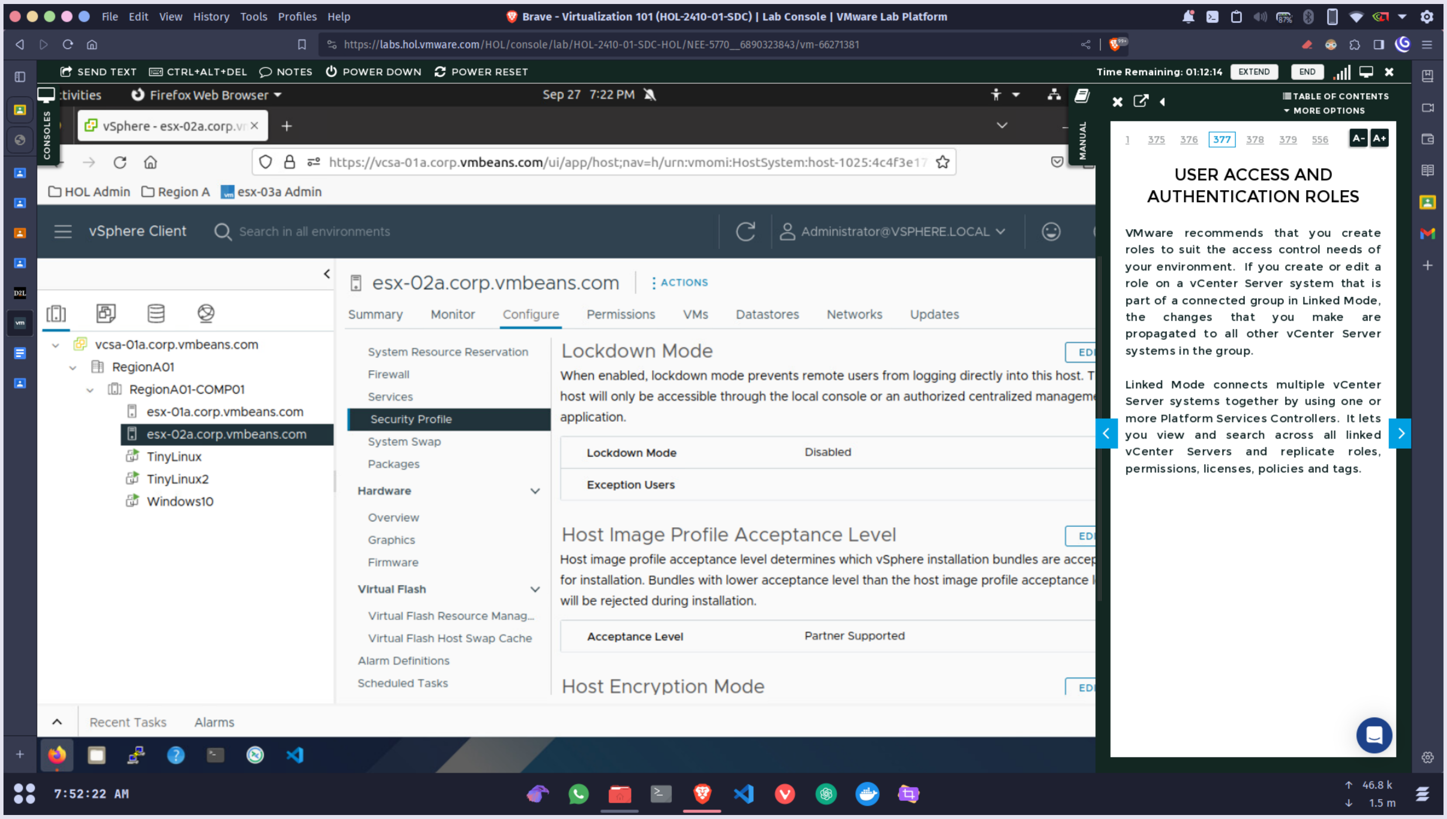
1. Now press the **F2** key to log in to the DCUI.

You should receive an error that access to the DCUI has been disabled.

2. Press the **Enter** key to dismiss the message.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 51
Virtualization Practical 5

5. Disable the lockdown mode for esx02



Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host. T host will only be accessible through the local console or an authorized centralized manageme application.

Lockdown Mode	Disabled
Exception Users	

Host Image Profile Acceptance Level

Host image profile acceptance level determines which vSphere installation bundles are accep for installation. Bundles with lower acceptance level than the host image profile acceptance l will be rejected during installation.

Acceptance Level	Partner Supported

Host Encryption Mode

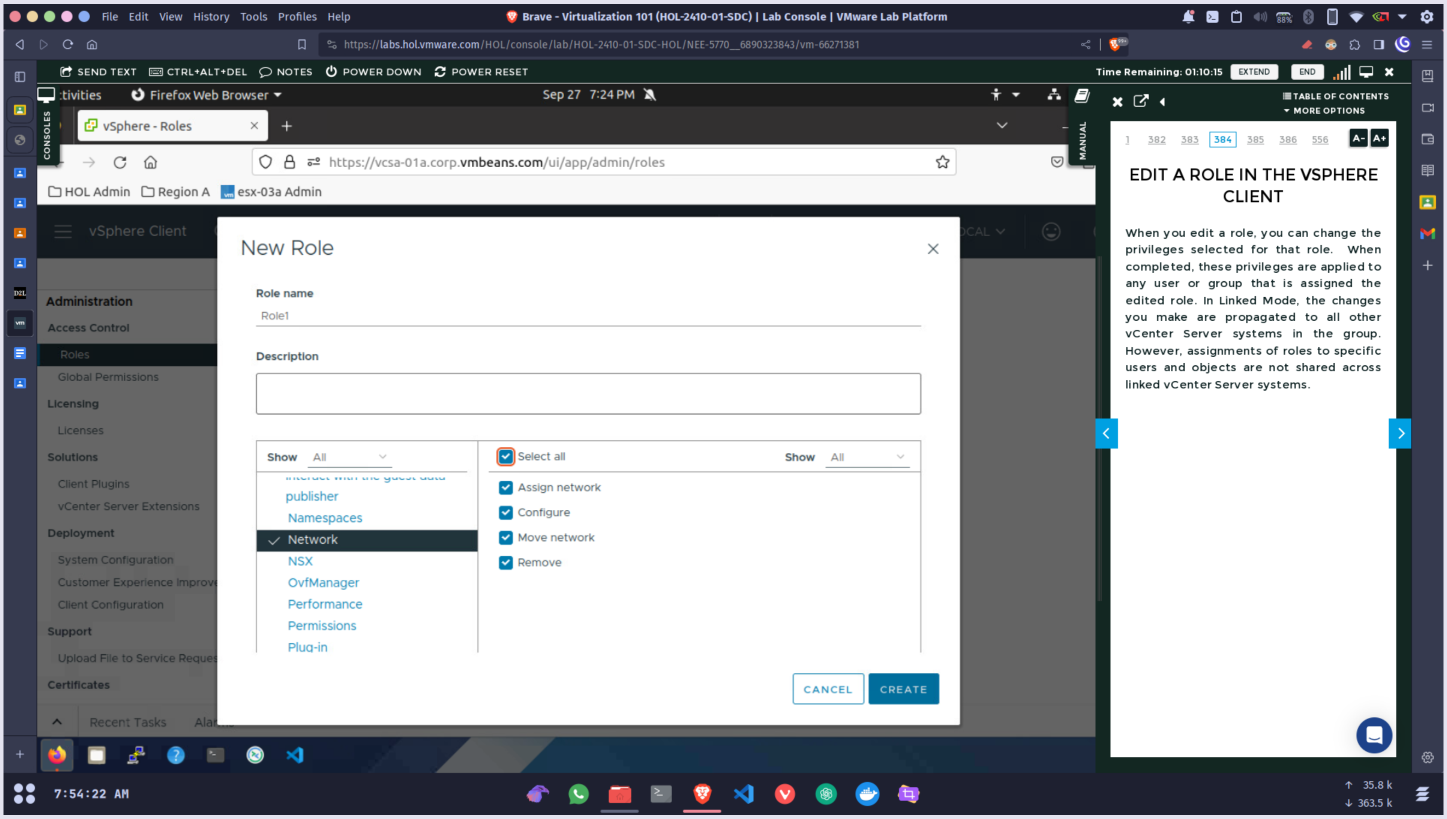
USER ACCESS AND AUTHENTICATION ROLES

VMware recommends that you create roles to suit the access control needs of your environment. If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes that you make are propagated to all other vCenter Server systems in the group.

Linked Mode connects multiple vCenter Server systems together by using one or more Platform Services Controllers. It lets you view and search across all linked vCenter Servers and replicate roles, permissions, licenses, policies and tags.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 51
Virtualization Practical 5

6. On clicking the top left menu button, visit **administration** configurations and create a new role 'Role1' in which give access to all **Network** rights.



New Role

Role name
Role1

Description

Show All

- publisher
- Namespaces
- ✓ Network
- NSX
- OvfManager
- Performance
- Permissions
- Plug-in

☑ Select all   Show All

☑ Assign network
☑ Configure
☑ Move network
☑ Remove

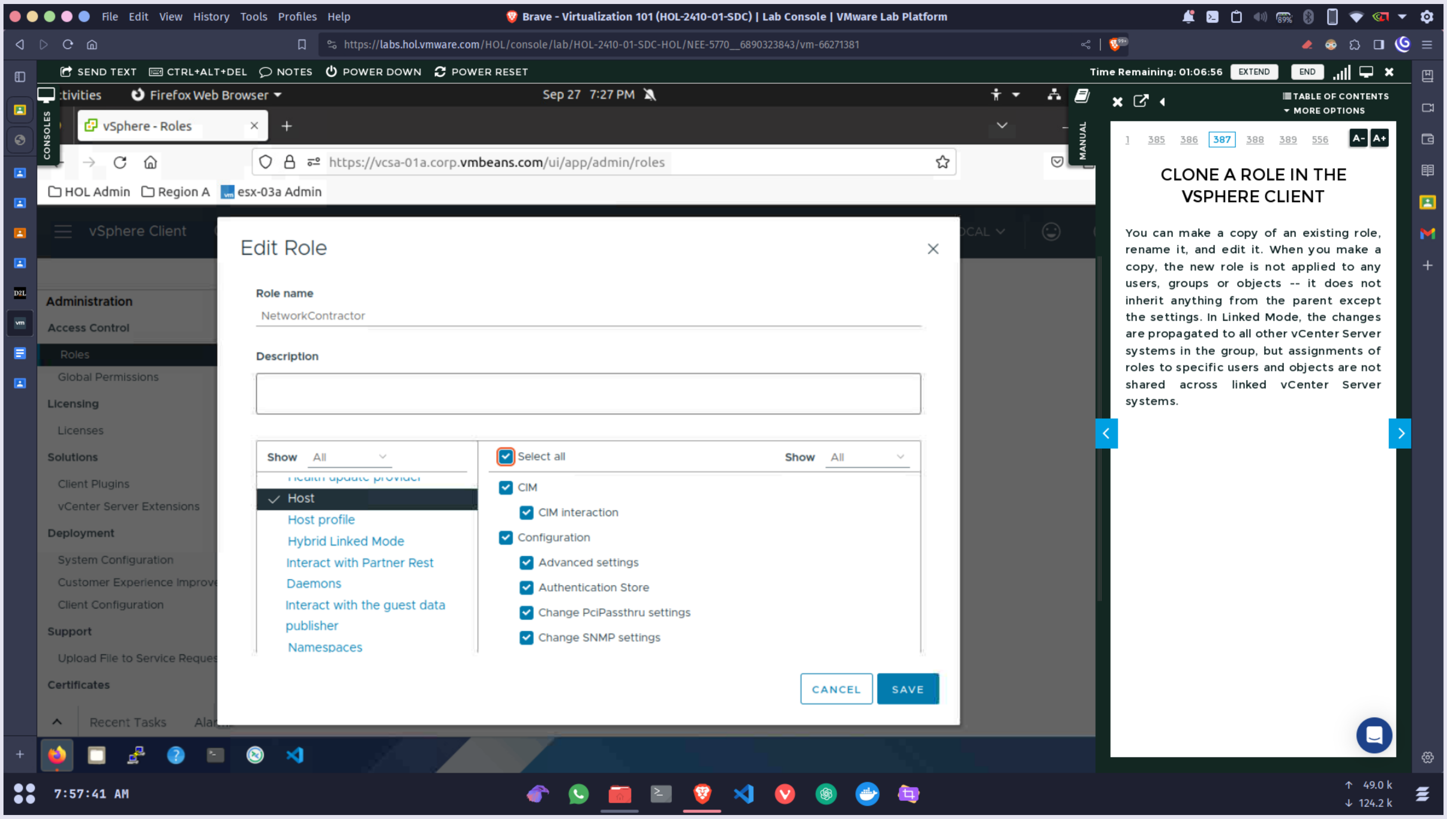
CANCEL   CREATE

EDIT A ROLE IN THE VSPHERE CLIENT

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group that is assigned the edited role. In Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. However, assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 51
Virtualization Practical 5

7. Edit the role created and change its name and add Host access also.



Edit Role

Role name
NetworkContractor

Description

Show All
Health update provider
✓ Host
Host profile
Hybrid Linked Mode
Interact with Partner Rest
Daemons
Interact with the guest data publisher
Namespaces

☑ Select all   Show All
☑ CIM
  ☑ CIM interaction
☑ Configuration
  ☑ Advanced settings
  ☑ Authentication Store
  ☑ Change PciPassthru settings
  ☑ Change SNMP settings

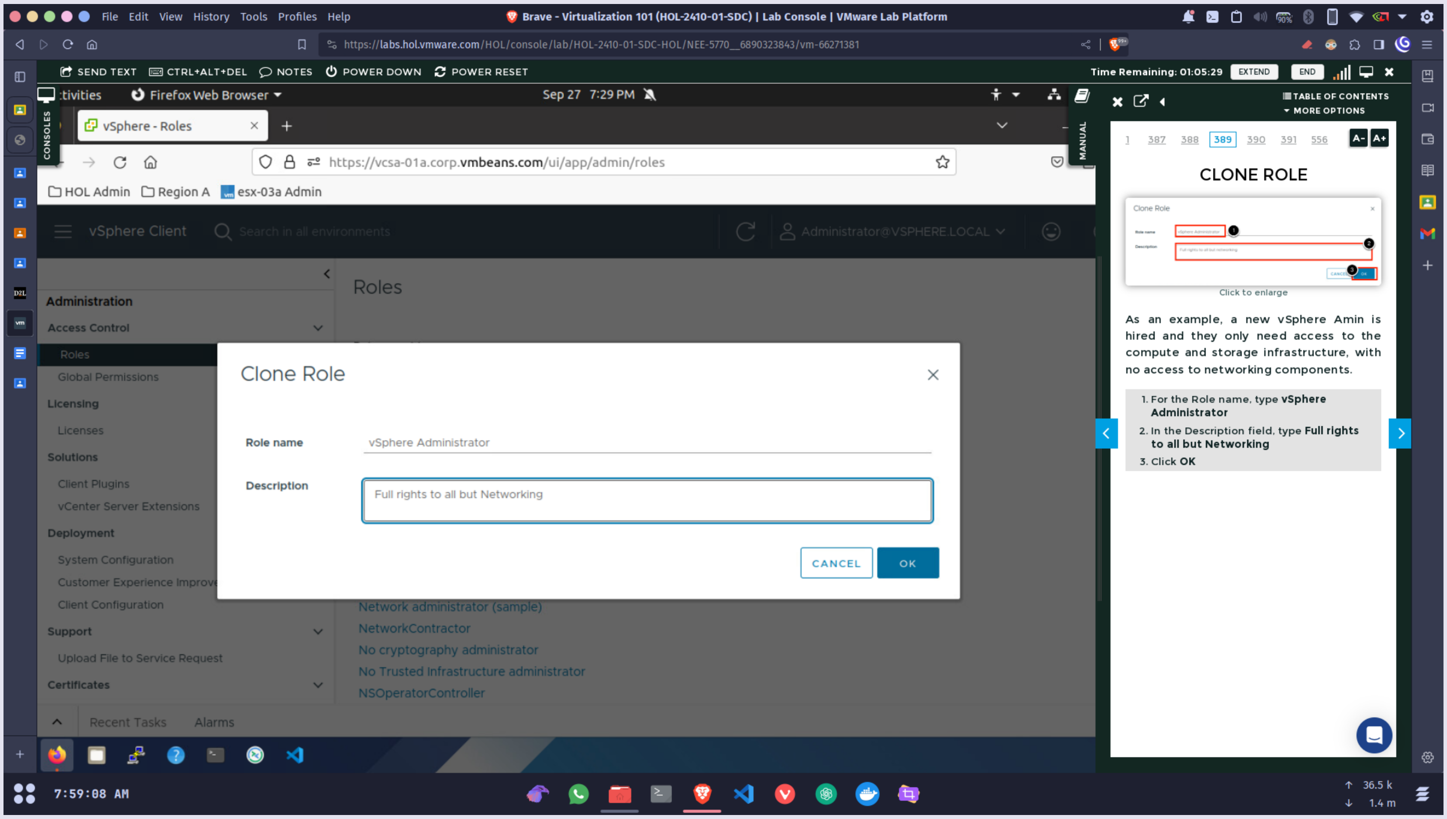
CANCEL   SAVE

CLONE A ROLE IN THE VSPHERE CLIENT

You can make a copy of an existing role, rename it, and edit it. When you make a copy, the new role is not applied to any users, groups or objects -- it does not inherit anything from the parent except the settings. In Linked Mode, the changes are propagated to all other vCenter Server systems in the group, but assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 51
Virtualization Practical 5

8. Clone the Administrator role and assign name and description.



Clone Role

Role name: vSphere Administrator

Description: Full rights to all but Networking

CANCEL OK

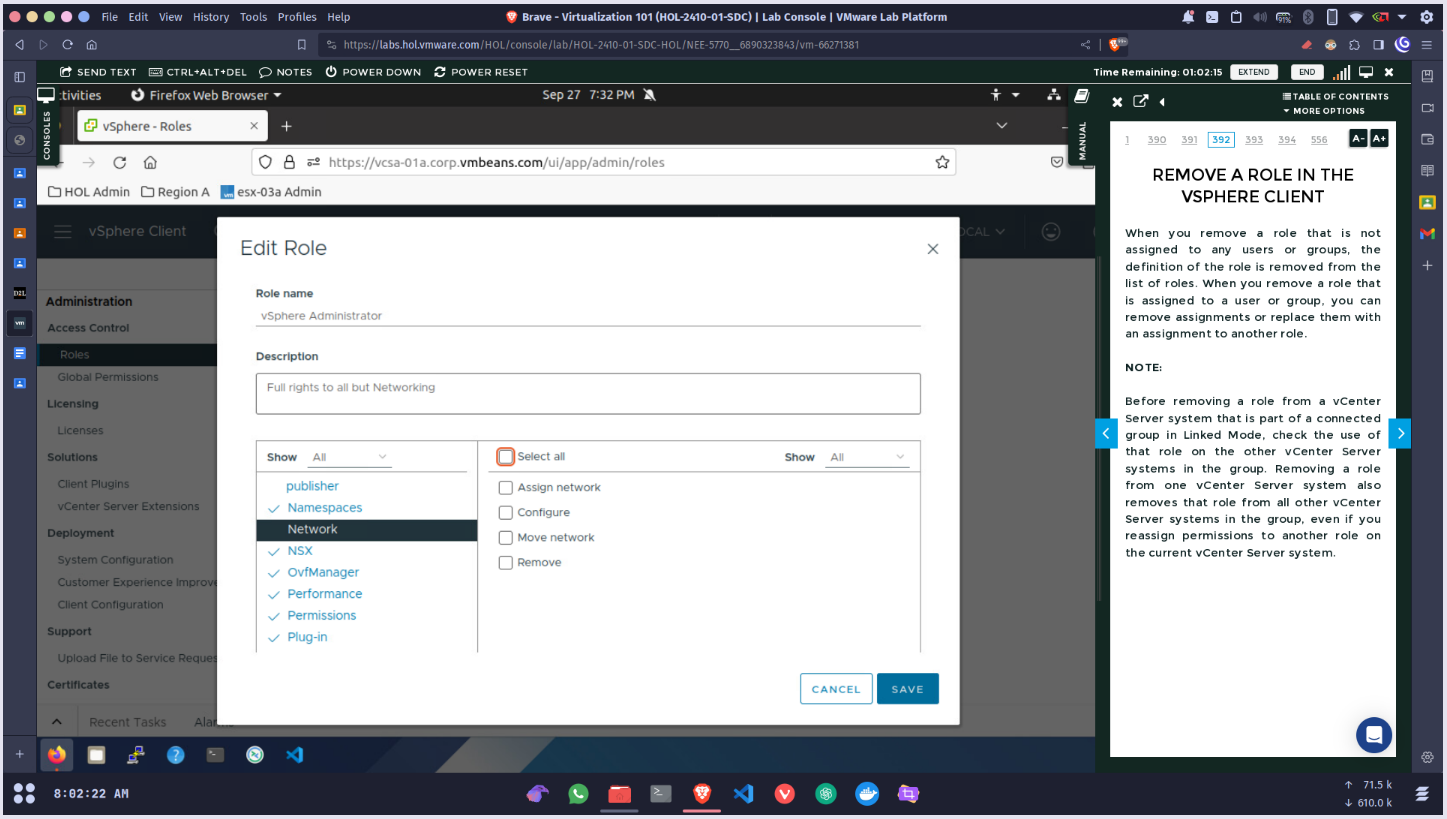
CLONE ROLE

As an example, a new vSphere Amin is hired and they only need access to the compute and storage infrastructure, with no access to networking components.

1. For the Role name, type **vSphere Administrator**
2. In the Description field, type **Full rights to all but Networking**
3. Click **OK**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 51
Virtualization Practical 5

9. Now, edit the cloned role's rights and remove all access to Network rights.



Edit Role

Role name: vSphere Administrator

Description: Full rights to all but Networking

Show: All

- publisher
- ✓ Namespaces
- Network
- ✓ NSX
- ✓ OvfManager
- ✓ Performance
- ✓ Permissions
- ✓ Plug-in

□ Select all   Show: All

- □ Assign network
- □ Configure
- □ Move network
- □ Remove

CANCEL SAVE

REMOVE A ROLE IN THE VSPHERE CLIENT

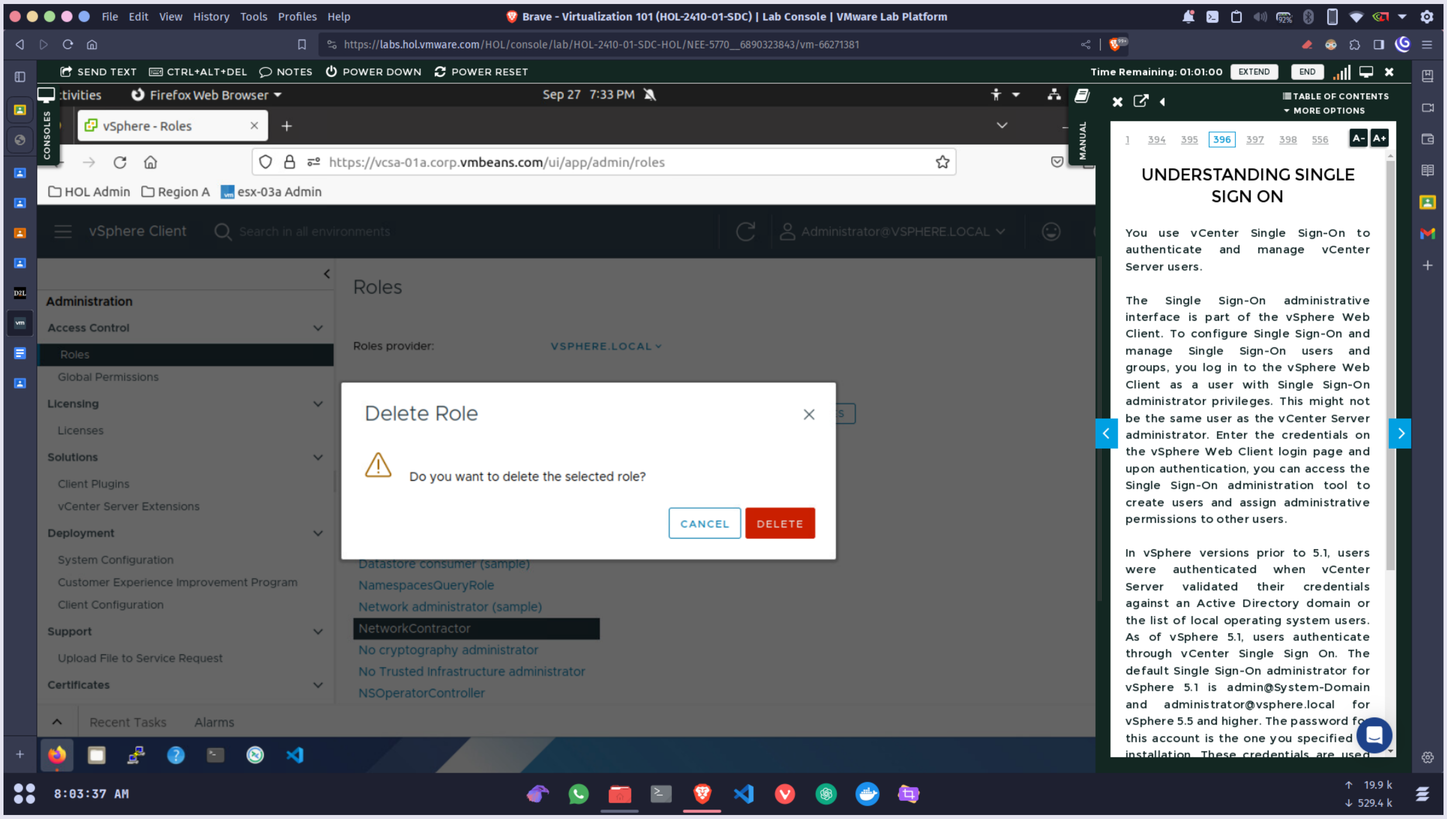
When you remove a role that is not assigned to any users or groups, the definition of the role is removed from the list of roles. When you remove a role that is assigned to a user or group, you can remove assignments or replace them with an assignment to another role.

NOTE:

Before removing a role from a vCenter Server system that is part of a connected group in Linked Mode, check the use of that role on the other vCenter Server systems in the group. Removing a role from one vCenter Server system also removes that role from all other vCenter Server systems in the group, even if you reassign permissions to another role on the current vCenter Server system.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 51
Virtualization Practical 5

10. Delete the role NetworkContractor.



Roles

Roles provider: VSPHERE.LOCAL

Delete Role

Do you want to delete the selected role?

CANCEL DELETE

Datastore consumer (sample)
NamespacesQueryRole
Network administrator (sample)
NetworkContractor
No cryptography administrator
No Trusted Infrastructure administrator
NSOperatorController

UNDERSTANDING SINGLE SIGN ON

You use vCenter Single Sign-On to authenticate and manage vCenter Server users.

The Single Sign-On administrative interface is part of the vSphere Web Client. To configure Single Sign-On and manage Single Sign-On users and groups, you log in to the vSphere Web Client as a user with Single Sign-On administrator privileges. This might not be the same user as the vCenter Server administrator. Enter the credentials on the vSphere Web Client login page and upon authentication, you can access the Single Sign-On administration tool to create users and assign administrative permissions to other users.

In vSphere versions prior to 5.1, users were authenticated when vCenter Server validated their credentials against an Active Directory domain or the list of local operating system users. As of vSphere 5.1, users authenticate through vCenter Single Sign On. The default Single Sign-On administrator for vSphere 5.1 is admin@System-Domain and administrator@vsphere.local for vSphere 5.5 and higher. The password fo this account is the one you specified installation. These credentials are used

<u>Conclusion</u> : Thus, host services can be accessed, edited and roles can be used to define access rights to ESXi clients and hosts.