



**Ganpat  
University**

॥ विद्यया समाजोत्कर्षः ॥

**Institute of  
Computer  
Technology**

**Name: Tushar Panchal**

**En.No: 21162101014**

**Sub: Virtualization**

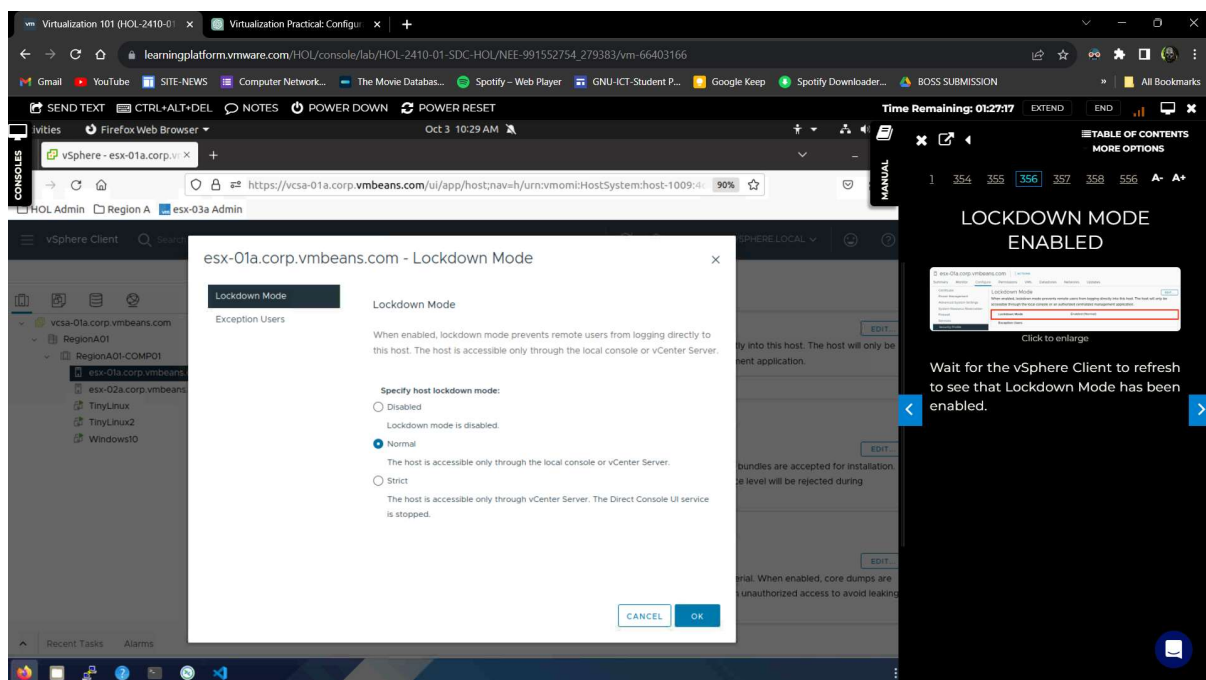
**Branch: CBA**

**Batch:51**

## -----PRACTICAL 05-----

### ❖ 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 :



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

The screenshot shows the vSphere Client interface for the host `esx-01a.corp.vmbeans.com`. The **Lockdown Mode** section is expanded, showing it is currently **Disabled**. A callout box on the right provides instructions for disabling the mode:

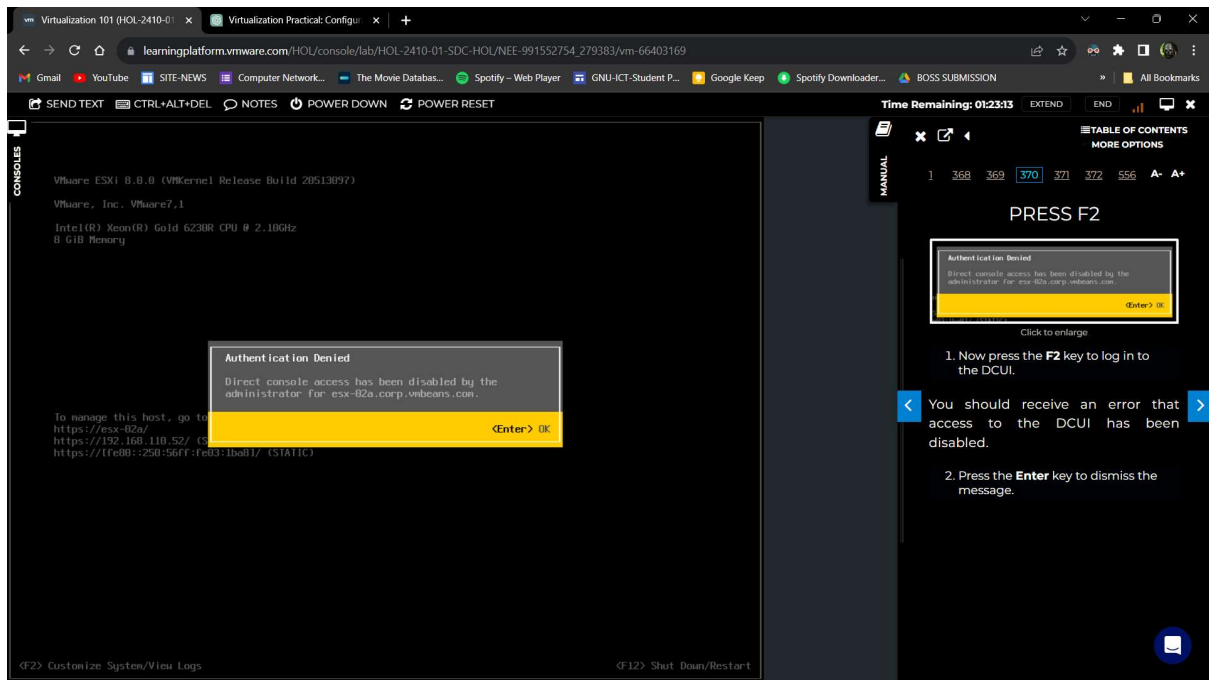
1. Check the **Disabled** radio button
2. Click **OK** to continue

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

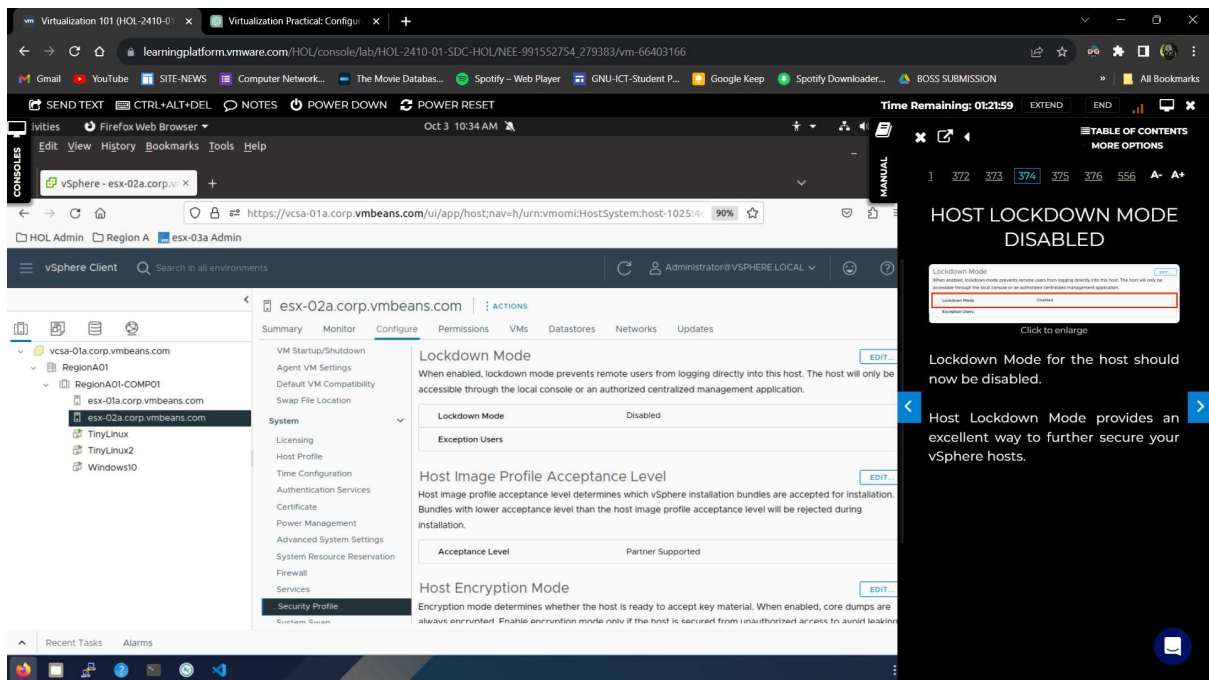
The screenshot shows the vSphere Client interface for the host `esx-02a.corp.vmbeans.com`. The **Lockdown Mode** section is expanded, showing it is currently **Disabled**. A callout box on the right provides instructions for enabling strict lockdown mode:

1. Notice Lockdown Mode is now Enabled

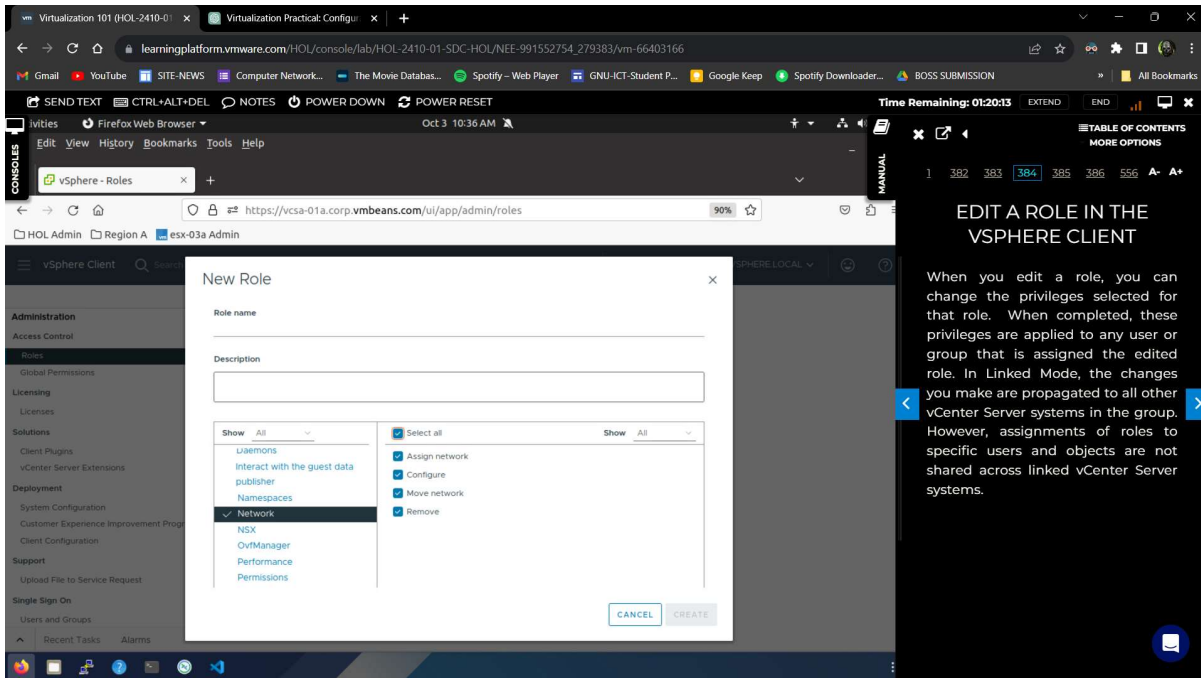
#### 4. Hence, the access for ESX-02A is disabled if not logged in from the main console :



#### 5. Disable the lockdown mode for esx02 :



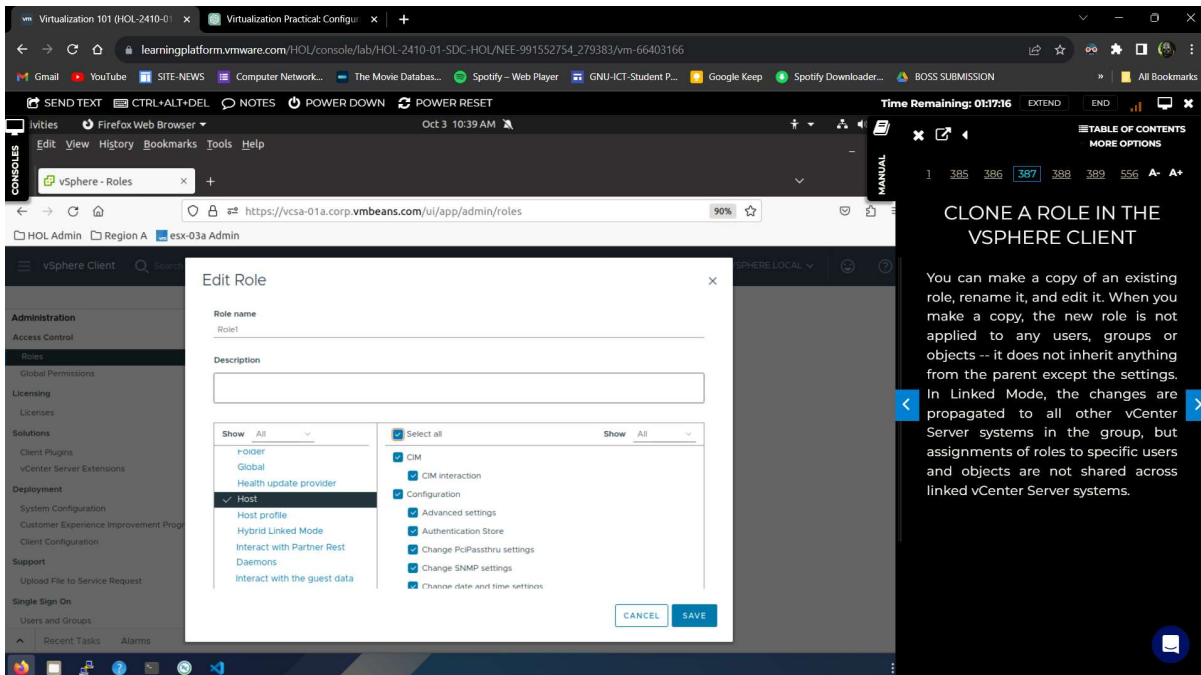
## **6. On clicking the top left menu button, visit administration configurations and create a new role 'Role1' in which give access to all Network rights :**



**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.

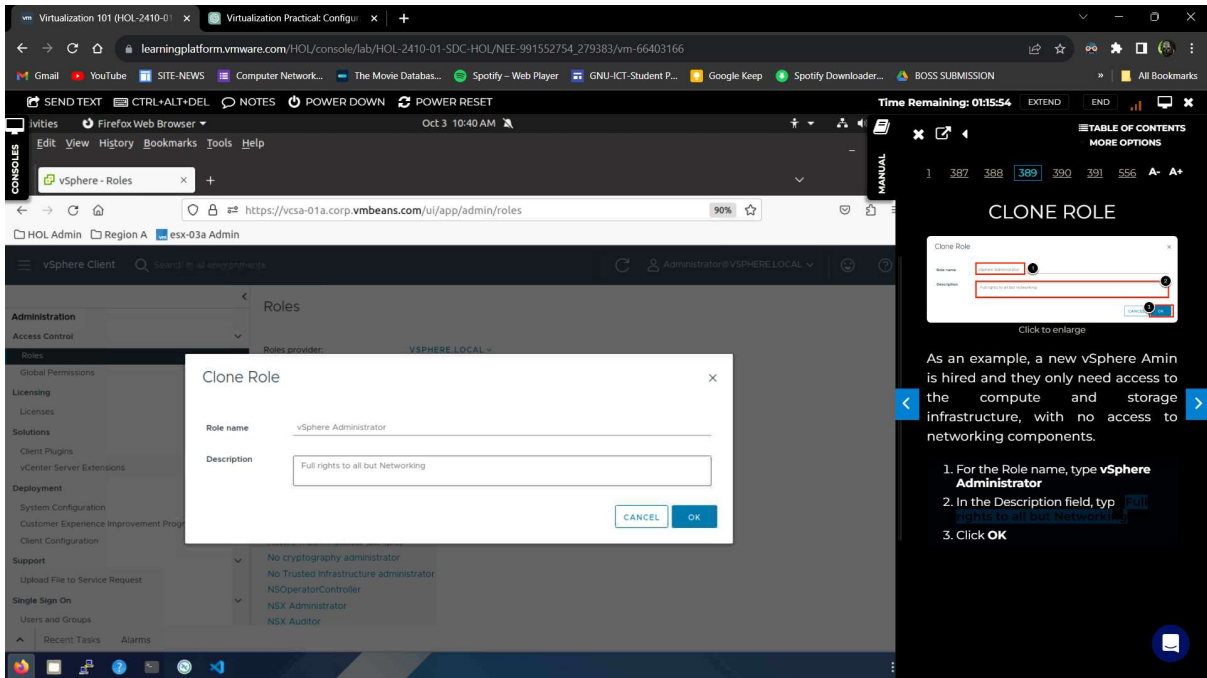
## **7. Edit the role created and change its name and add Host access also :**



**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.

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



CLONE ROLE

Clone Role

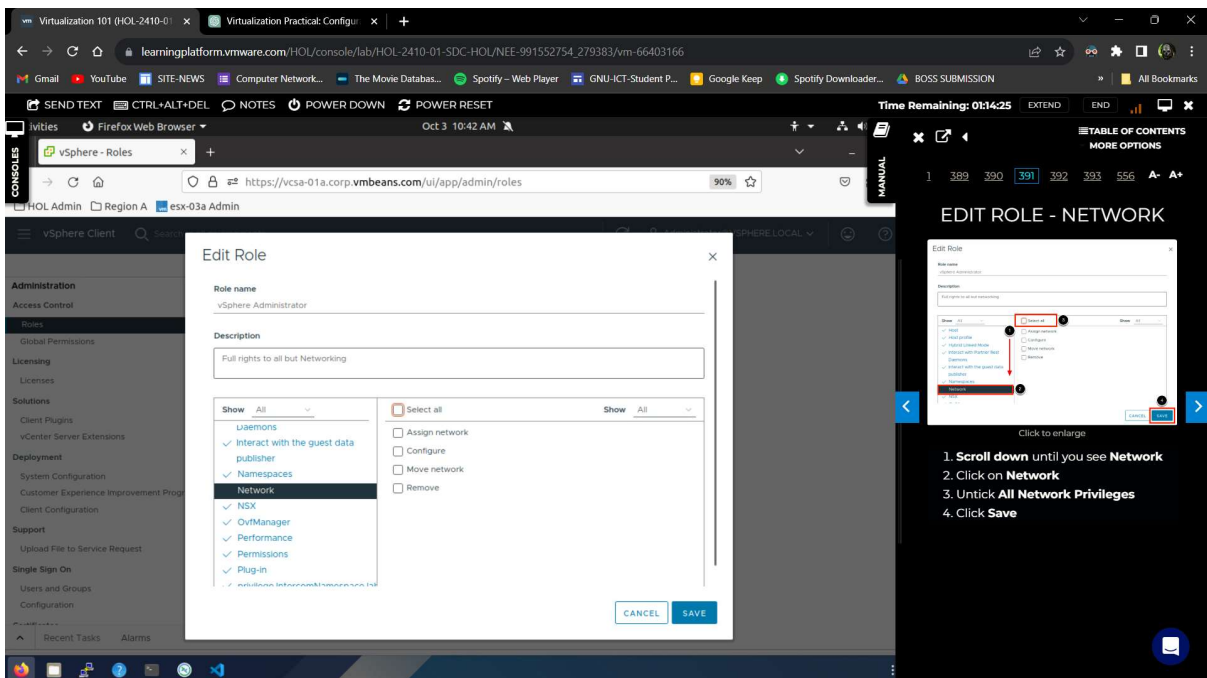
Role name: vSphere Administrator

Description: Full rights to all but Networking

As an example, a new vSphere Admin 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**

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



EDIT ROLE - NETWORK

Edit Role

Role name: vSphere Administrator

Description: Full rights to all but Networking

Network

1. Scroll down until you see **Network**

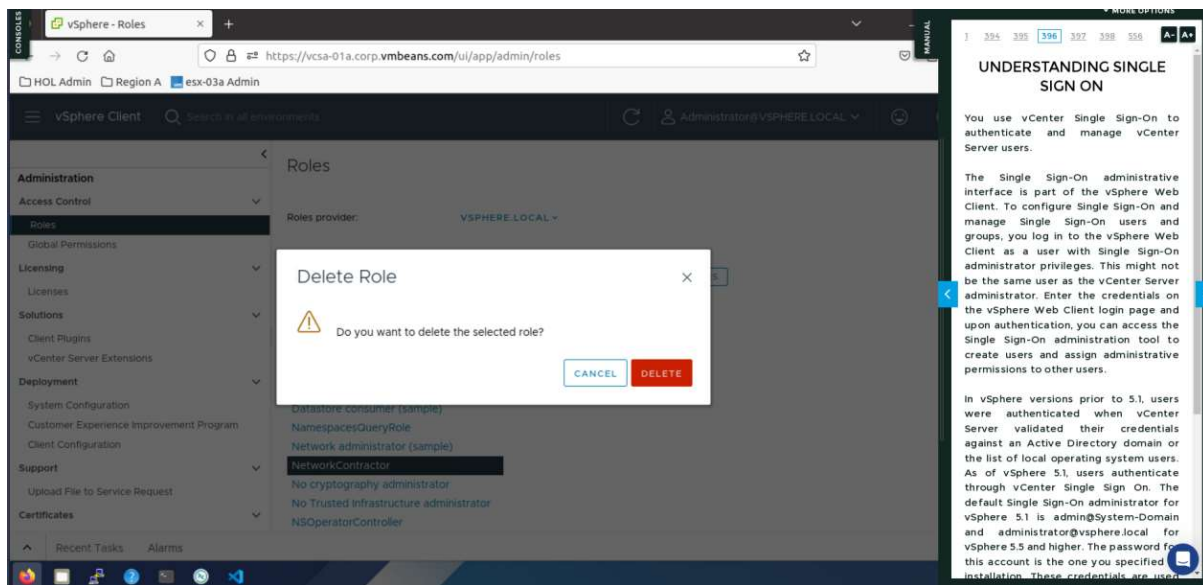
2. Click on **Network**

3. Untick **All Network Privileges**

4. Click **Save**



## 10. Delete the role NetworkContractor :



### » **Conclusion :**

this practical exercise provided hands-on experience in configuring host access control and firewall settings in a VMware virtualization environment. It emphasized the importance of securing host access and creating customized roles with specific rights to meet organizational requirements.