LAB-1

INFO8855

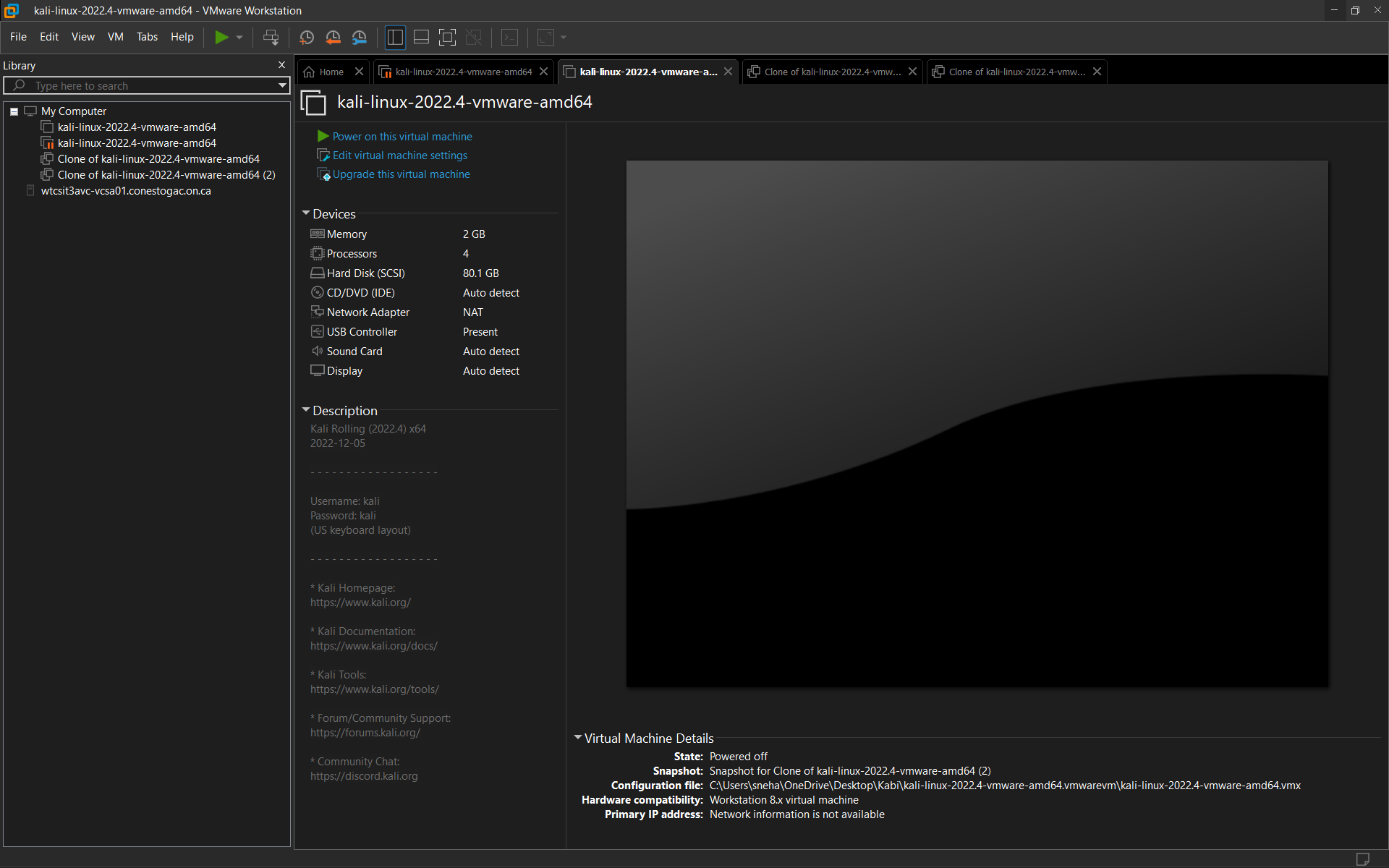
Virtualization and Cloud Security  
  
Kabileshar Ramakrishnan Mohan Kumar  
  
8856188

|  |  |
| --- | --- |
| **TABLE OF CONTENTS** | |
| **CONTENT** | **PAGE NO.** |
| **LAB 1.1-INFO8855 – Master VM Lab** | 3 |
| **Overview** | 3 |
| Description | 3 |
| Screenshots | 3 |
| Reflections | 3 |
| **Task-1** | 3 |
| Description | 3 |
| Screenshots | 4 |
| Reflections | 4 |
| **Task-2** | 5 |
| Description | 5 |
| Screenshots | 5 |
| Reflections | 6 |
| **LAB 1.2-INFO8855 – Master VM Lab** | 8 |
| Overview | 8 |
| **Task-1** | 8 |
| Description | 8 |
| Screenshots | 9 |
| Reflections | 12 |
| Reference | 13 |
| **Task-2** | 14 |
| Description | 14 |
| Screenshots | 15 |
| Reflections | 19 |
| Reference | 19 |
| **Task-3** | 20 |
| Description | 20 |
| Screenshots | 21 |
| Reflections | 24 |
| Reference | 25 |

LAB 1.1-INFO8855 – Master VM Lab  
  
Overview  
  
This lab provides with practice creating a “Golden Master” VM and deploying VMs from the master. A software application or system's final, approved version, known as a Golden Master Image (GMI), acts as the distribution's master copy. It is often produced by a software development team following extensive testing and quality assurance inspections of the system.

The GMI is a precise clone of the software programme or system, complete with all of its attributes and capabilities. To ensure consistency and prevent mistakes when replicating the software in the future, it serves as a reference point.  
  
Task 1 – Create a Base VM  
  
Description

* Created a Virtual machine in VMware workstation
* VM is created with Linux operating System

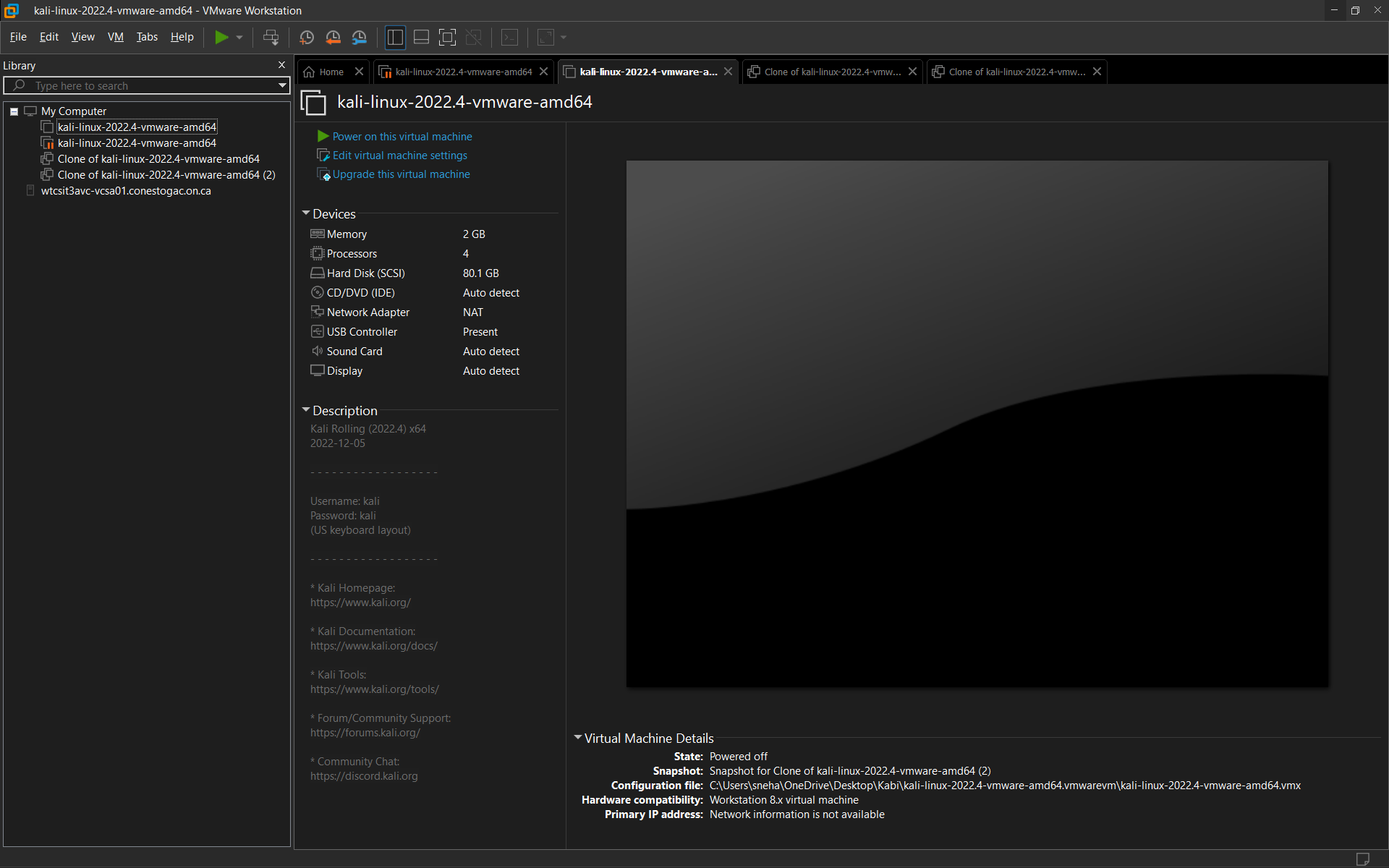
Screenshot  
  
Fig 1.1 VM is created with Kali Linux operating system  
  
Reflection  
  
It is crucial to properly select and configure the base virtual machine (VM) for a Golden Master Image (GMI) so that it has every piece of the final software version. These are some of the most crucial considerations while creating a base VM:

System software: The underlying virtual machine's operating system should have been installed completely from scratch and be compatible with the programme or system.  
  
  
Patches and updates: To make sure that the programme is running on a dependable and safe platform, the base VM should be updated with the most recent security patches and updates.

Software components and dependencies that the finished software programme or system needs to run properly should be included in the base virtual machine (VM).

Task 2 – Create a Master Image  
  
Description

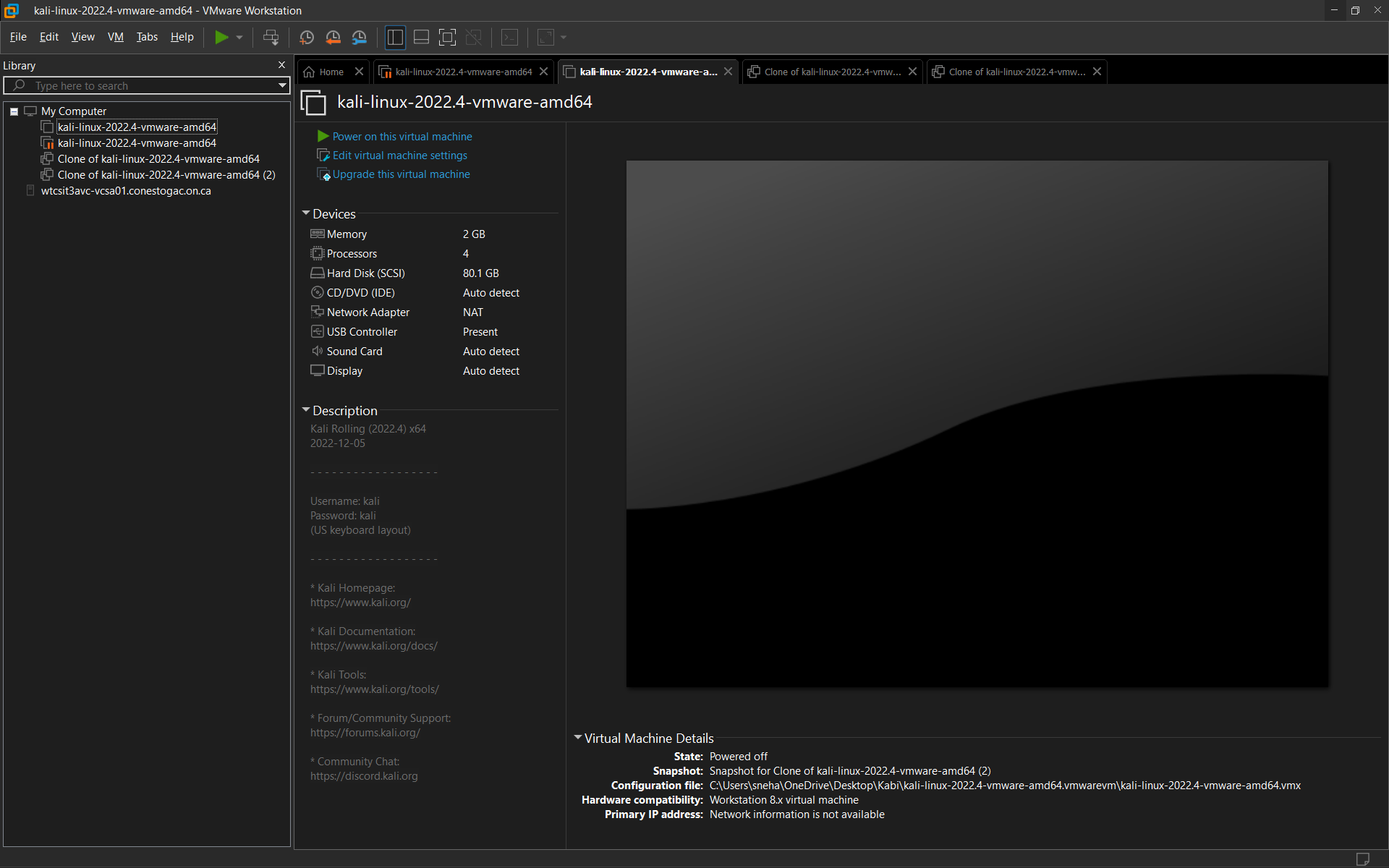
* Created a Virtual machine in VMware workstation
* VM is created with Linux operating System
* Exported an OVF or OVA image of the VM that built in part 1
* Click snapshot manager and click clone
* Successfully cloned from master image

Screenshots  
  
  
Fig 1.2 Cloned image of Virtual machine

Reflection  
Virtual machines are packaged and distributed using the file formats OVF and OVA (VMs). OVF is an open standard for VM packaging, whereas OVA is a compressed version of an OVF file that gathers all the required VM files into a single bundle. This is the fundamental distinction between the two.

Task 3 – Deploy Two VMs from the Master Image  
  
Overview  
  
 Created two VMs by deploying from master image.

* Connected the VMs to the NAT network from the virtual  
  environment.
* Ensured that the VMs can communicate with an external network.

Screenshots  
  
Fig 1.3 Successfully created two vm from Master Image

LAB 1.2-INFO8855 – Private Cloud Infrastructure Lab  
  
Overview

This lab provides with the opportunity to formalize about private cloud environment. Dedicated to a single enterprise, a private cloud environment is a kind of cloud computing infrastructure that offers a virtualized environment that is cut off from other organizations and the public Internet. Compared to a public cloud environment, this configuration offers the organization a higher level of protection, control, and flexibility because the entire infrastructure is set aside for its exclusive use.

An organization's own data centers, protected by its own firewall, are often where virtualized resources and services are deployed in a private cloud environment. As a result, the company has total control over how the cloud environment is managed and configured, including the choice of the operating system, apps, and security settings.  
  
Task 1 – Secure Host Authentication  
In this task NTP and ESXI host is configured to allow user to authenticate Active directory domain.  
  
Description

* For this part of lab successfully created two ESXI host and one Domain namely krm6188-ESXI01 , krm6188-ESXI02 and krama6188-INFRA respectively.
* Logged in to the krm6188-ESXI01 host and navigated to the “Manage”
* Under system configured the NTP servers by clicking “Edit Settings” with IP 152.156.151.46 as given in the document.
* Ensured the status of the server is Running.
* Logged in to the krm6188-ESXI02 host and navigated to the “Manage”
* Under system configured the NTP servers by clicking “Edit Settings” with IP 152.156.151.46 as given in the document.
* Ensured the status of the server is Running.
* In order to add both ESXI host as member of the Domain navigate to the “Security & User”.
* Under Authentications, Added the Domain name as Krm6188vclass.local and ensured that host is joined in the domain.
* Successfully joined the host as the member of the Domain.

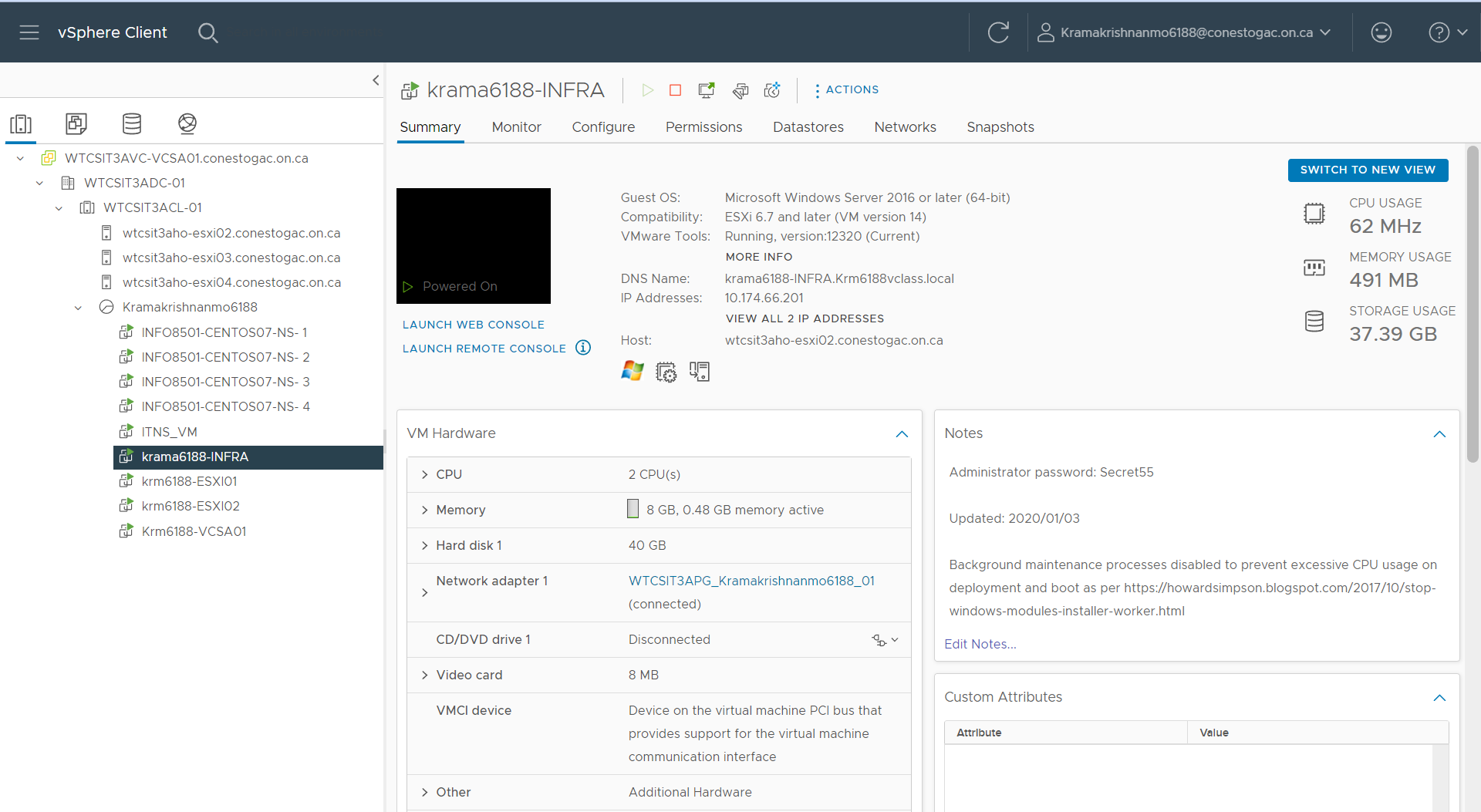
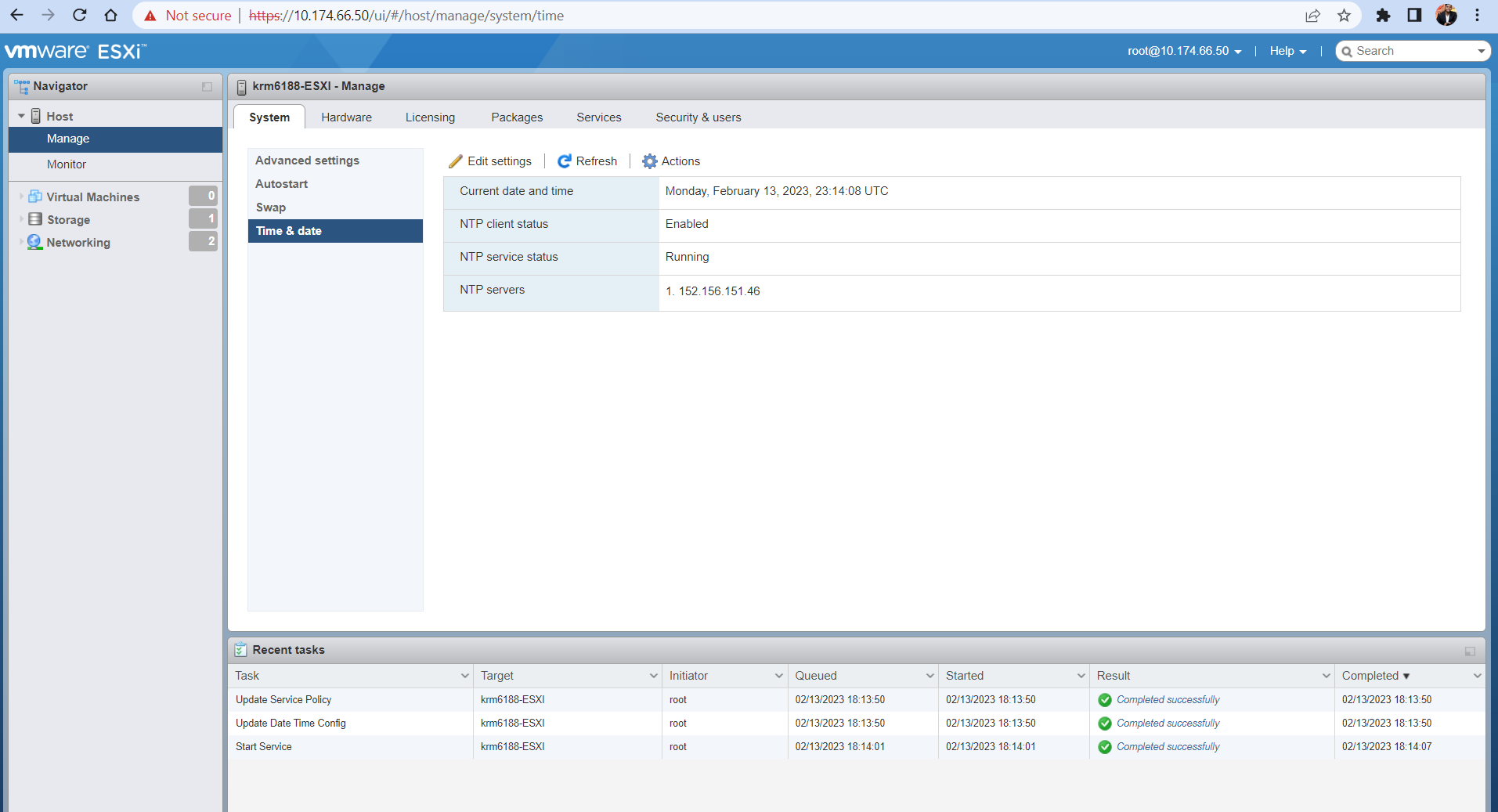
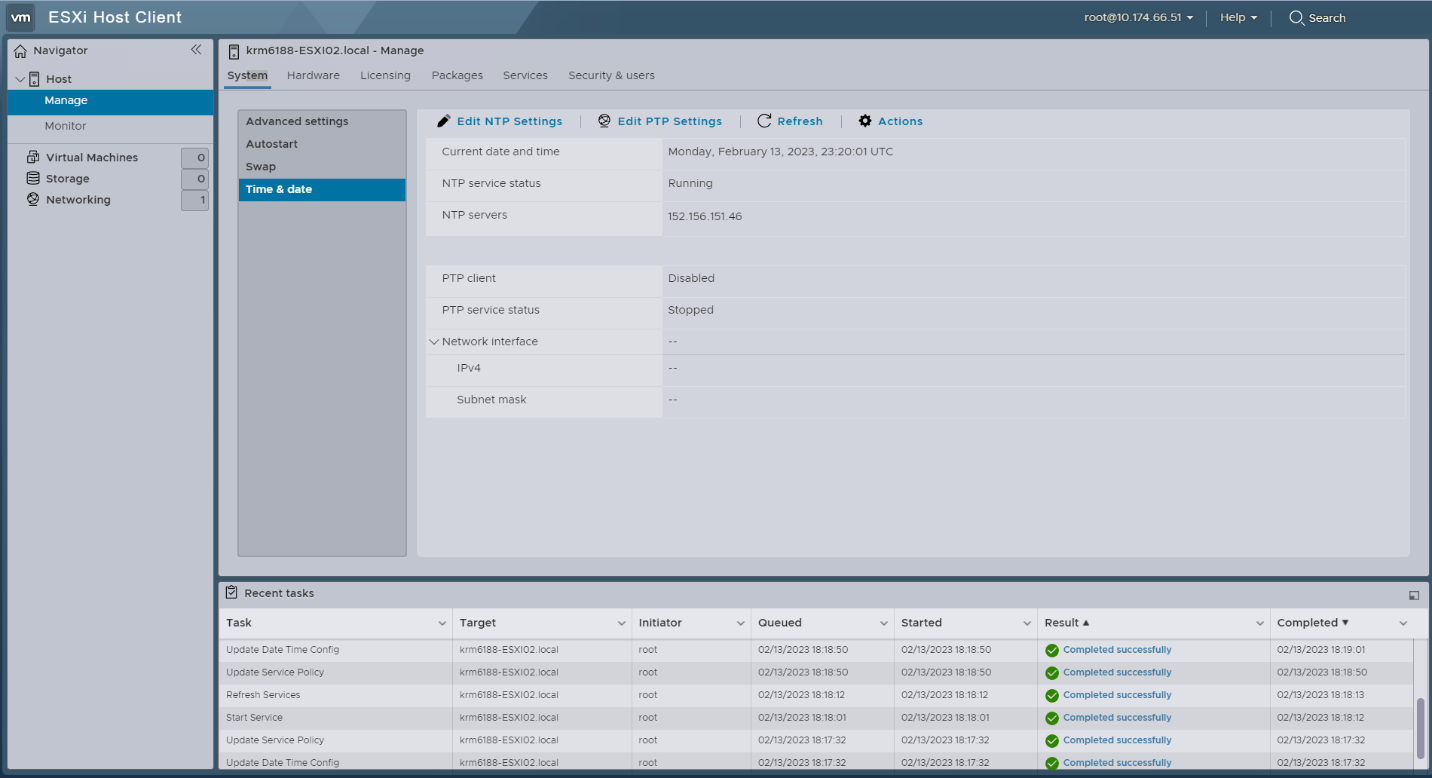
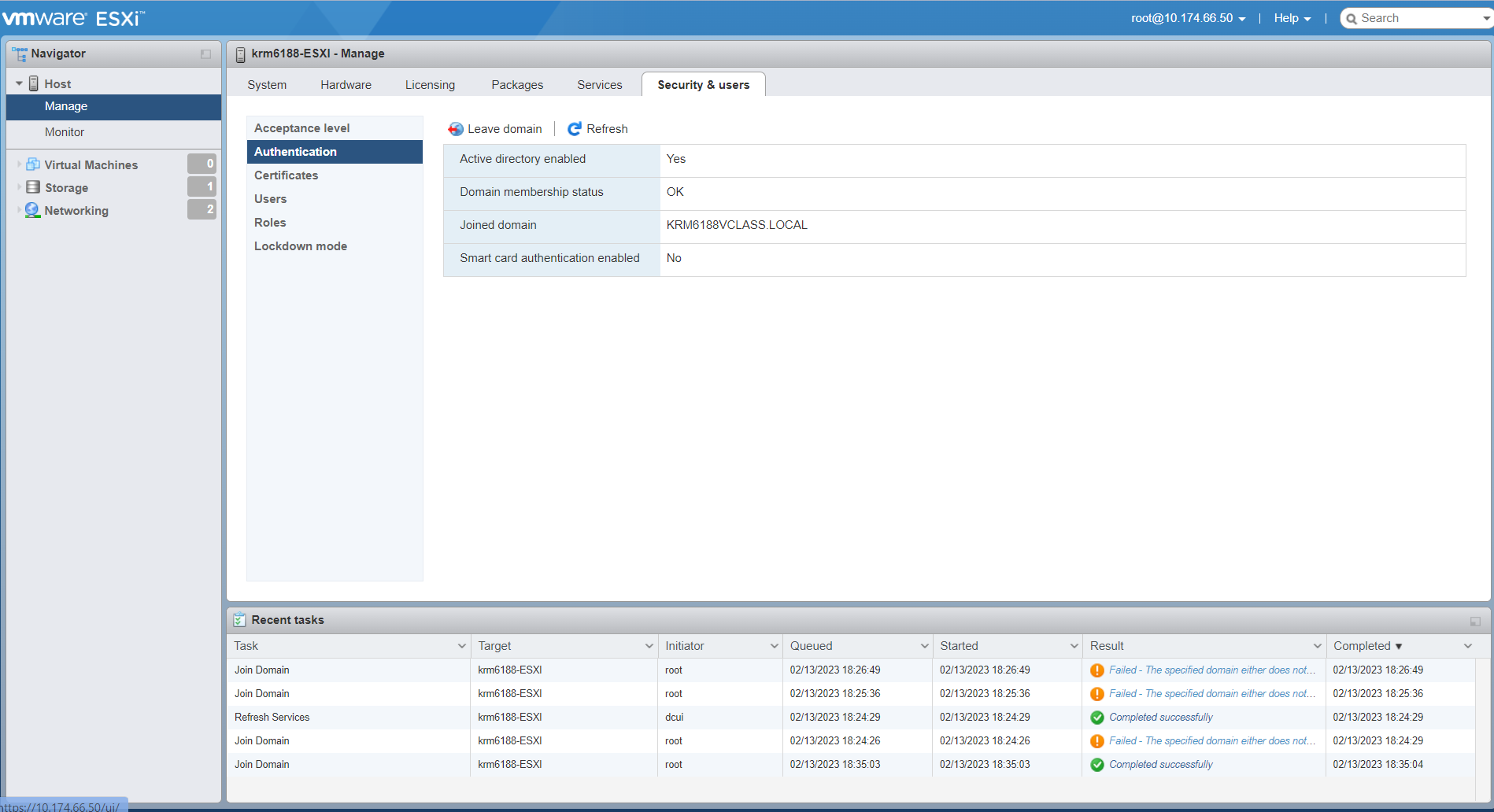
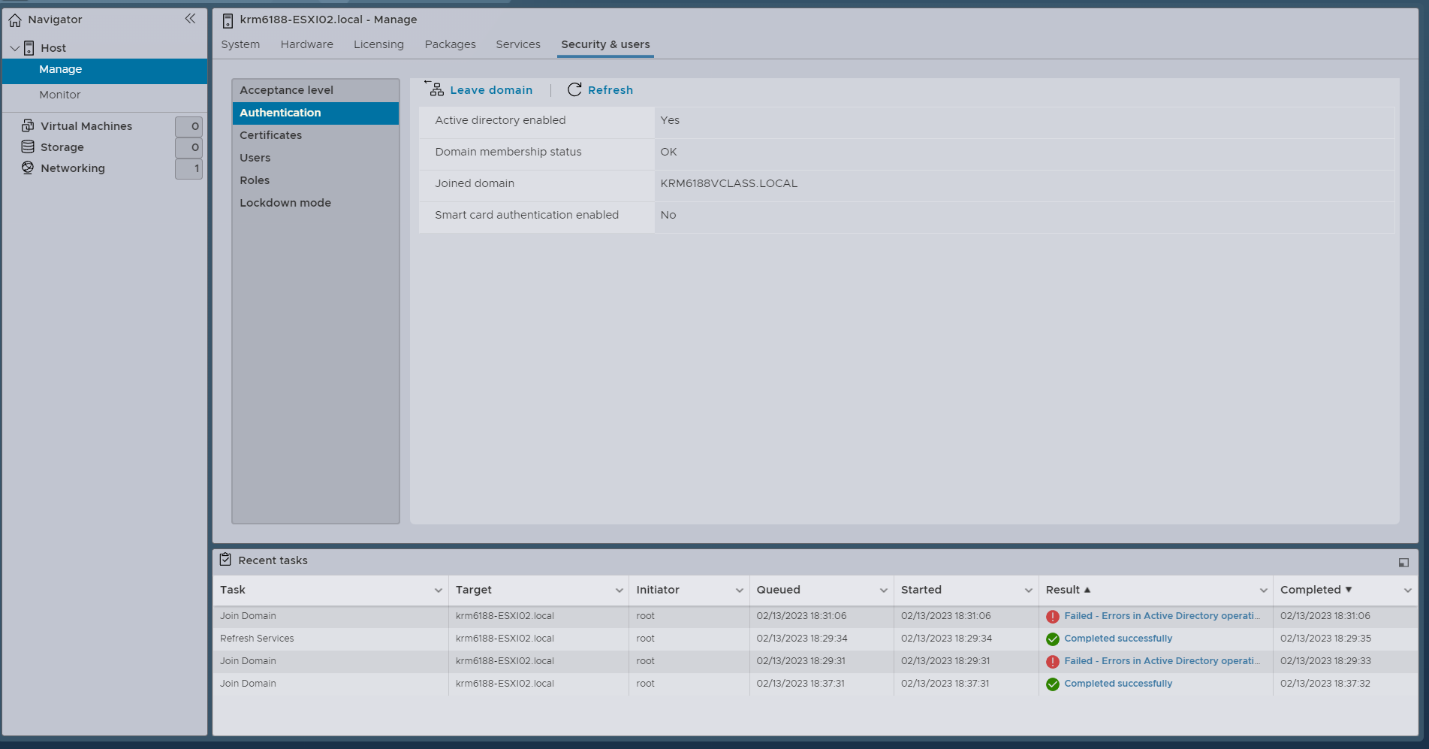
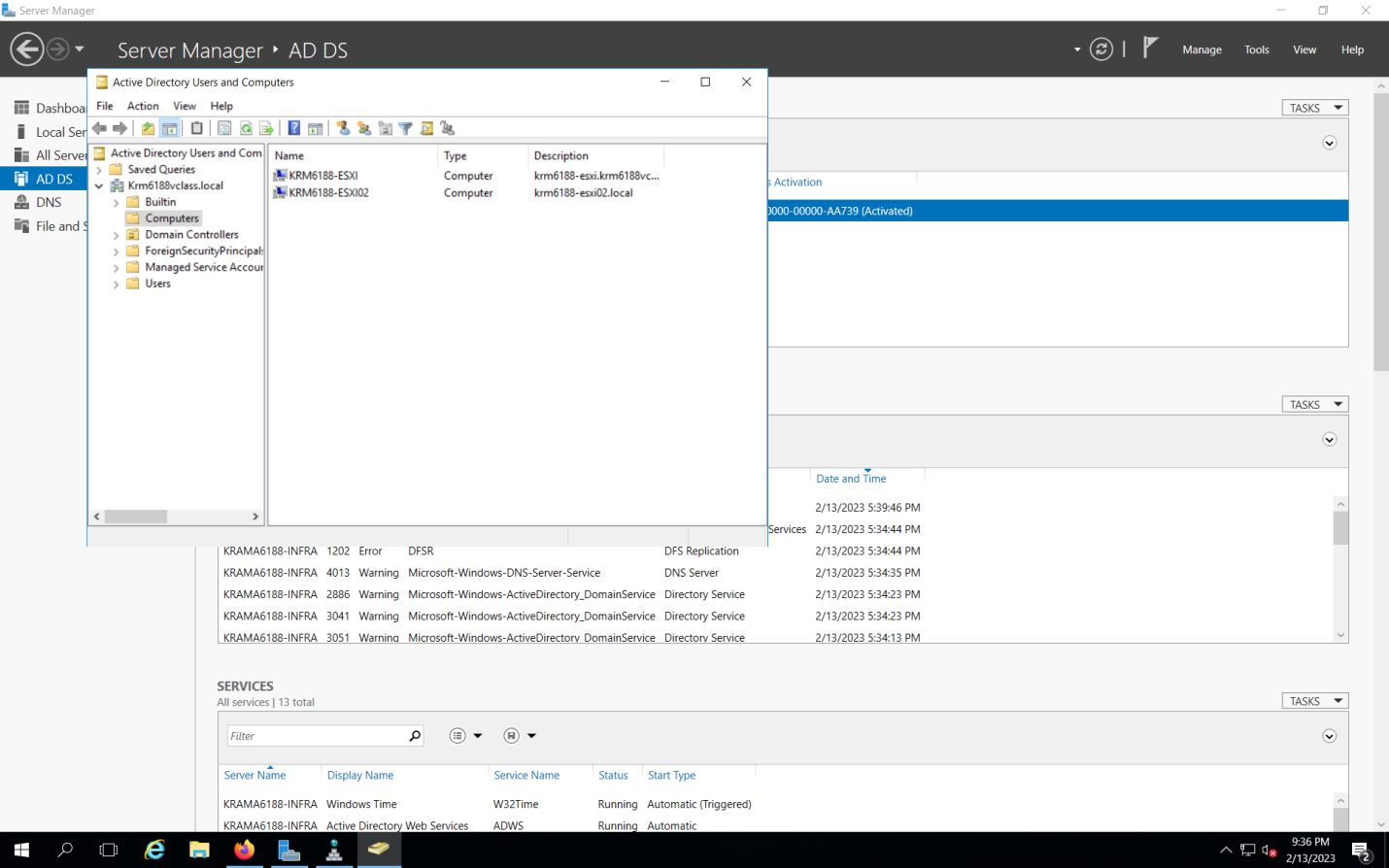
Screenshots  


Fig 1.1 VM’s Created for ESXI

  
Fig 1.2 NTP for krm6188-ESXI01  
  
  
Fig 1.3 NTP for krm6188-ESXI02  
  
  
Fig 1.4 krm6188-ESXI01 added to the domain  
  
  
Fig 1.5 krm6188-ESXI02 added to the domain  
  
  
Fig 1.6 Both Hosts are successfully added to the domain  
  
  
Reflection  
Both Active Directory authentication and Network Time Protocol settings are necessary for a reliable and secure IT environment. Some of the advantage are:  
  
Centralized authentication is possible with Active Directory thanks to a feature that lets users log in only once and access network resources without continuously entering their credentials. This makes it simpler to manage user accounts and permissions and allows users to more quickly access the resources they need.

Access Control: Thanks to Active Directory's fine-grained access control functionality, administrators can permit or deny access to specific resources based on a user's identity, group membership, or other variables. Controlling access to critical information is now easier as a result.

Configuring NTP is important for the following reason Computers must be able to synchronize their clocks with a reliable time source in order to guarantee that events are accurately timestamped and that logs and other data are consistent across the network (NTP). This is also important for security and compliance reasons since precise timestamps are essential for analyzing security incidents and demonstrating compliance with standards. Security: NTP frequently offers cryptographic authentication, which ensures that time synchronization messages are coming from a reliable source and haven't been altered with. This helps thwart attacks that rely on fake timestamps, such as replay attacks and man-in-the-middle attacks.  
  
Reference  
  
**Advantages of Active Directory authentication:**

"Benefits of Active Directory": <https://www.microsoft.com/en-us/security/business/identity-and-access-management/benefits-of-active-directory>

"Why use Active Directory?": <https://www.techrepublic.com/article/why-use-active-directory/>

**Importance of configuring NTP:**

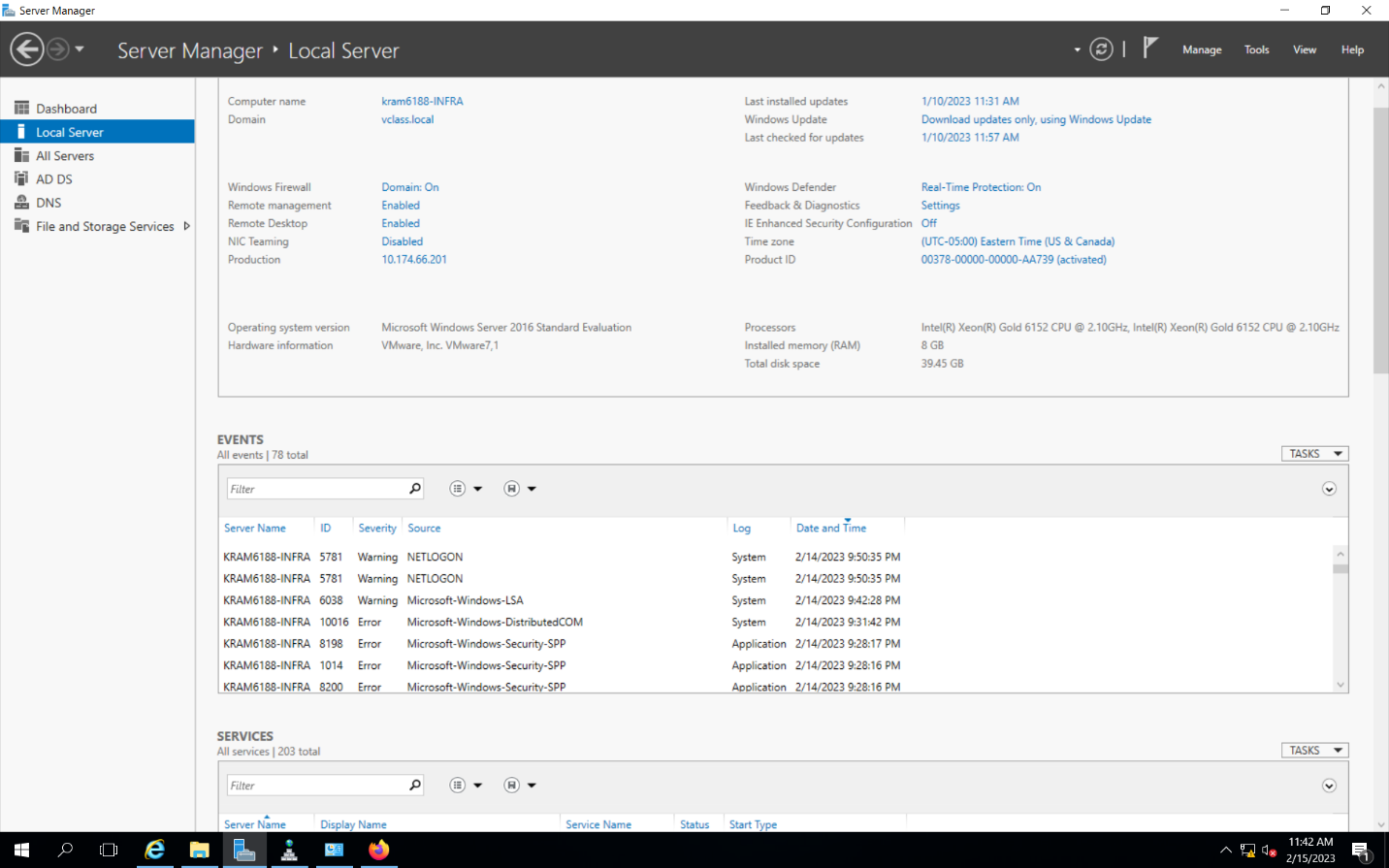
"Why is NTP important?": <https://www.greywizard.com/why-is-ntp-important/>

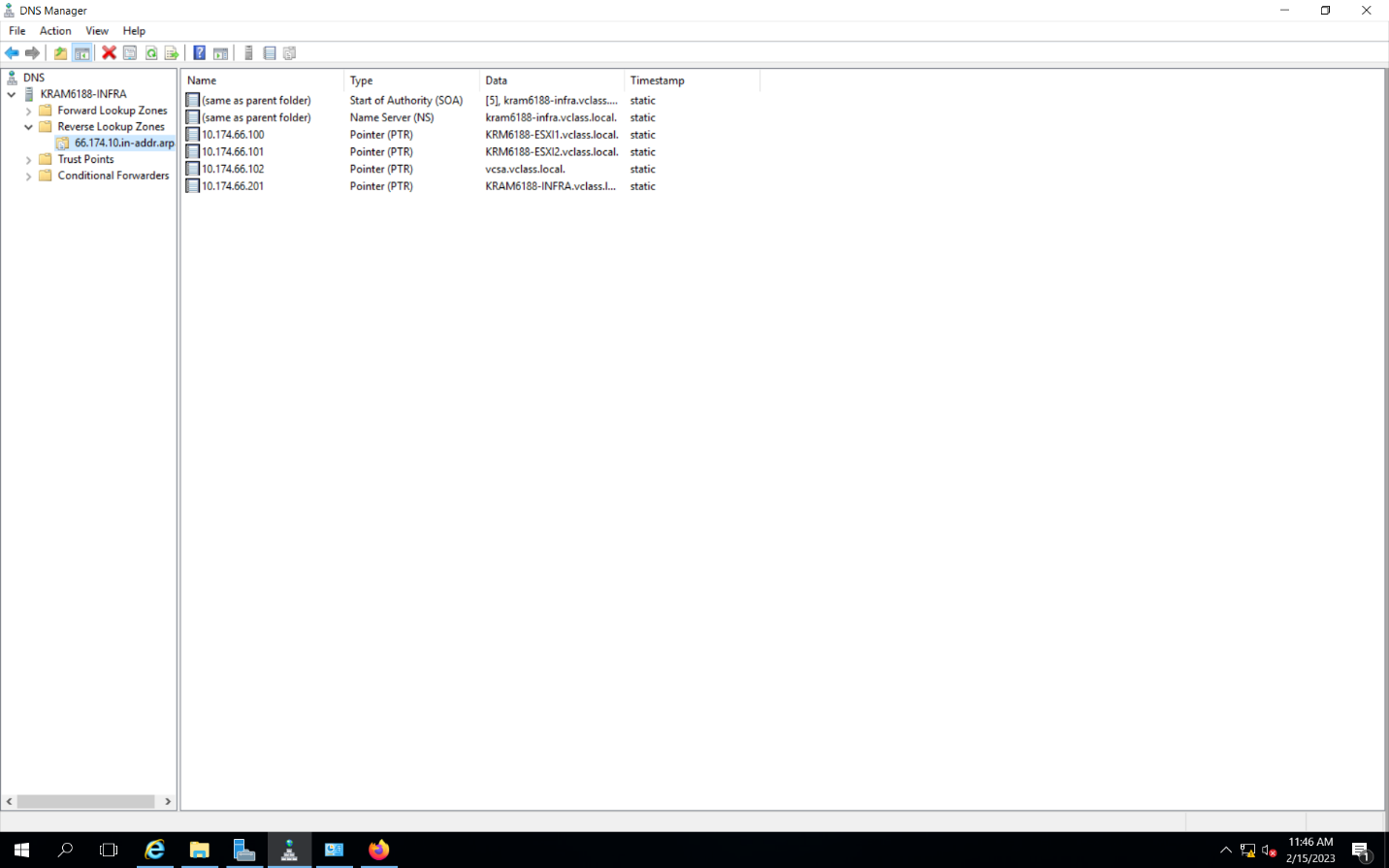
"The importance of time synchronization": <https://www.cisco.com/c/en/us/about/security-center/importance-time-synchronization.html>

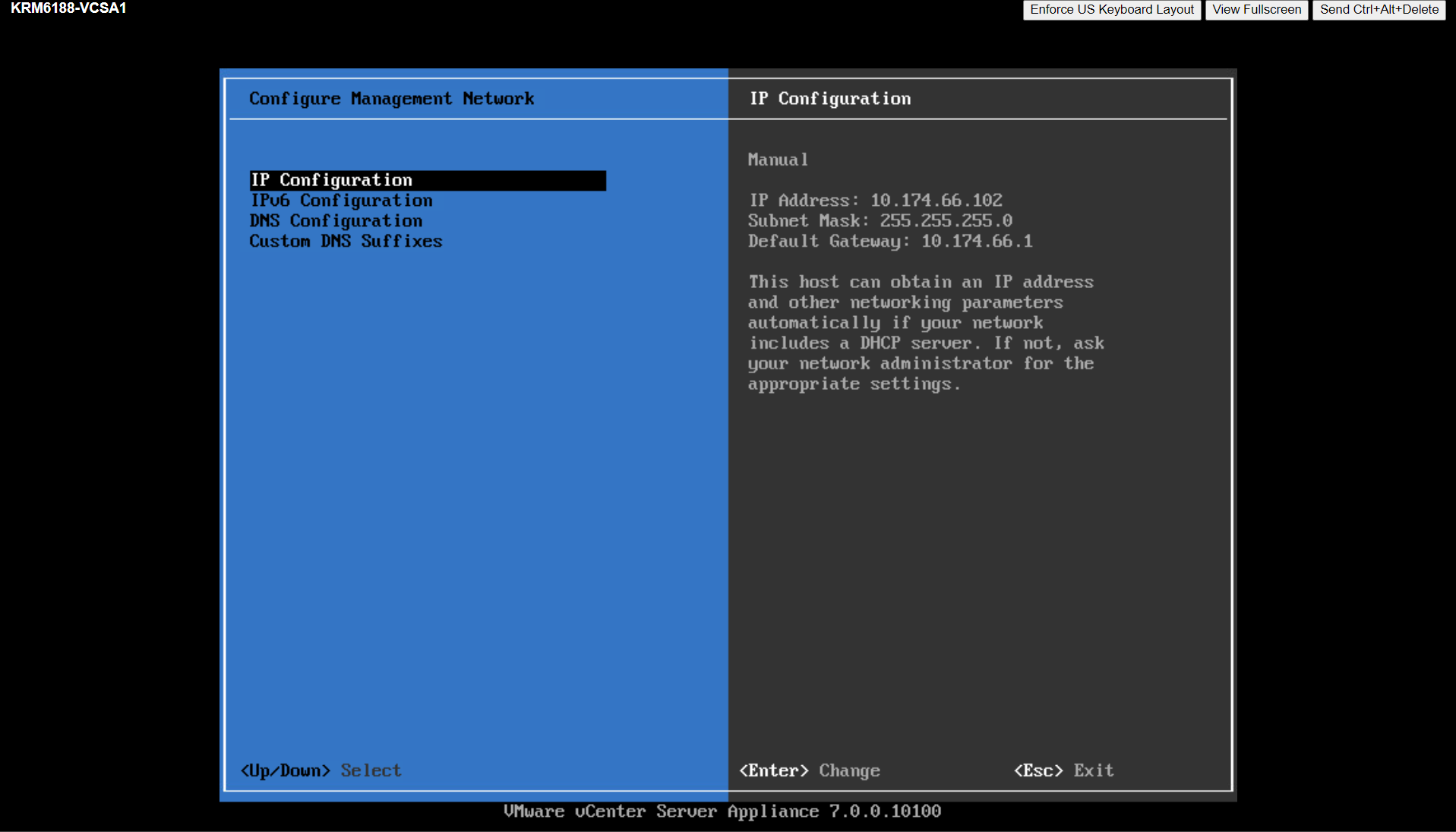
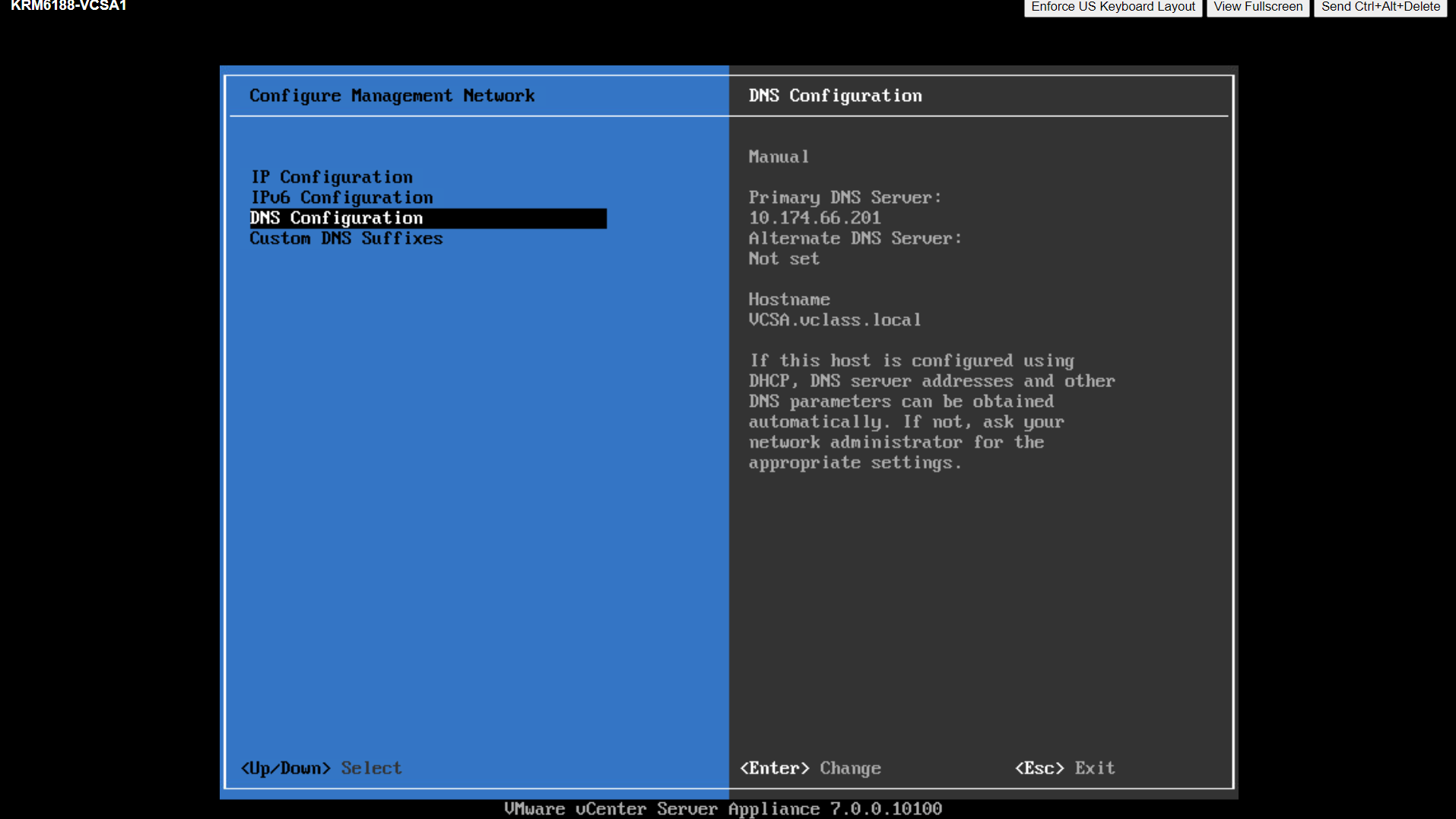
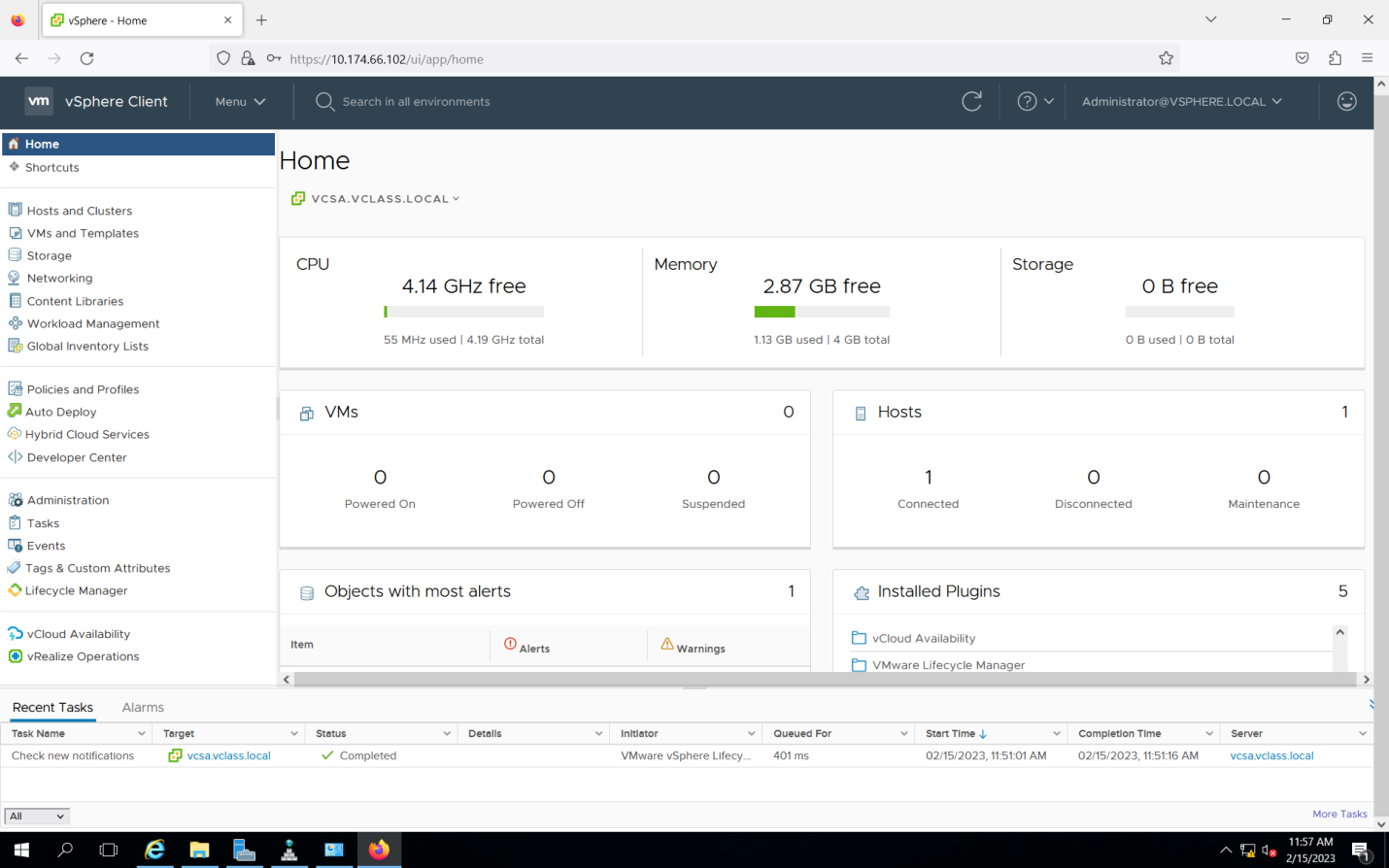
Task 2 – Secure vCenter Authentication  
  
Overview  
In this task, we will configure VCSA to use an Active Directory domain as an identity source. Also Configuring vCenter Server Appliance to use Active Directory domain as a Single Sign-On (SSO) identity source.  
  
Description

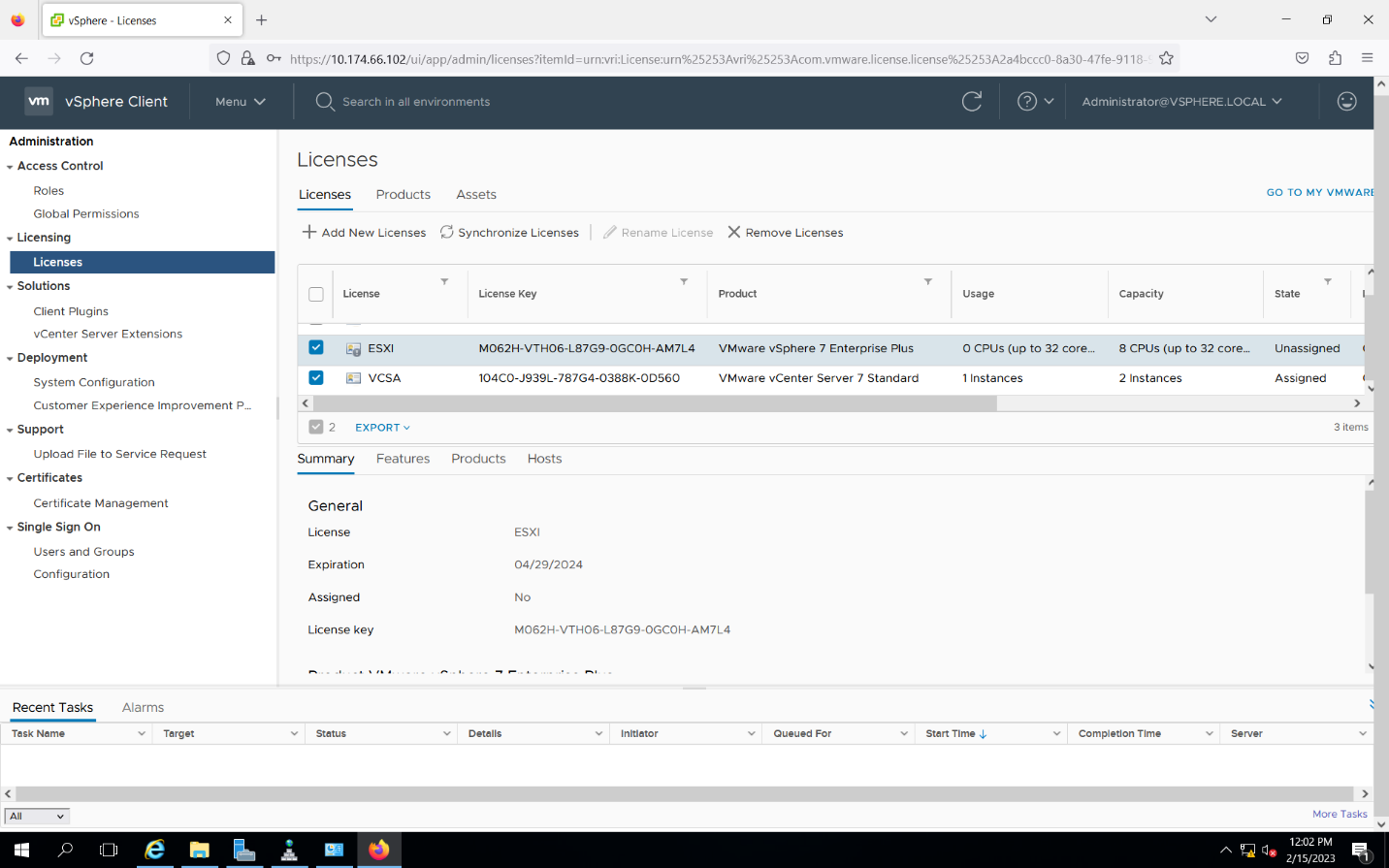
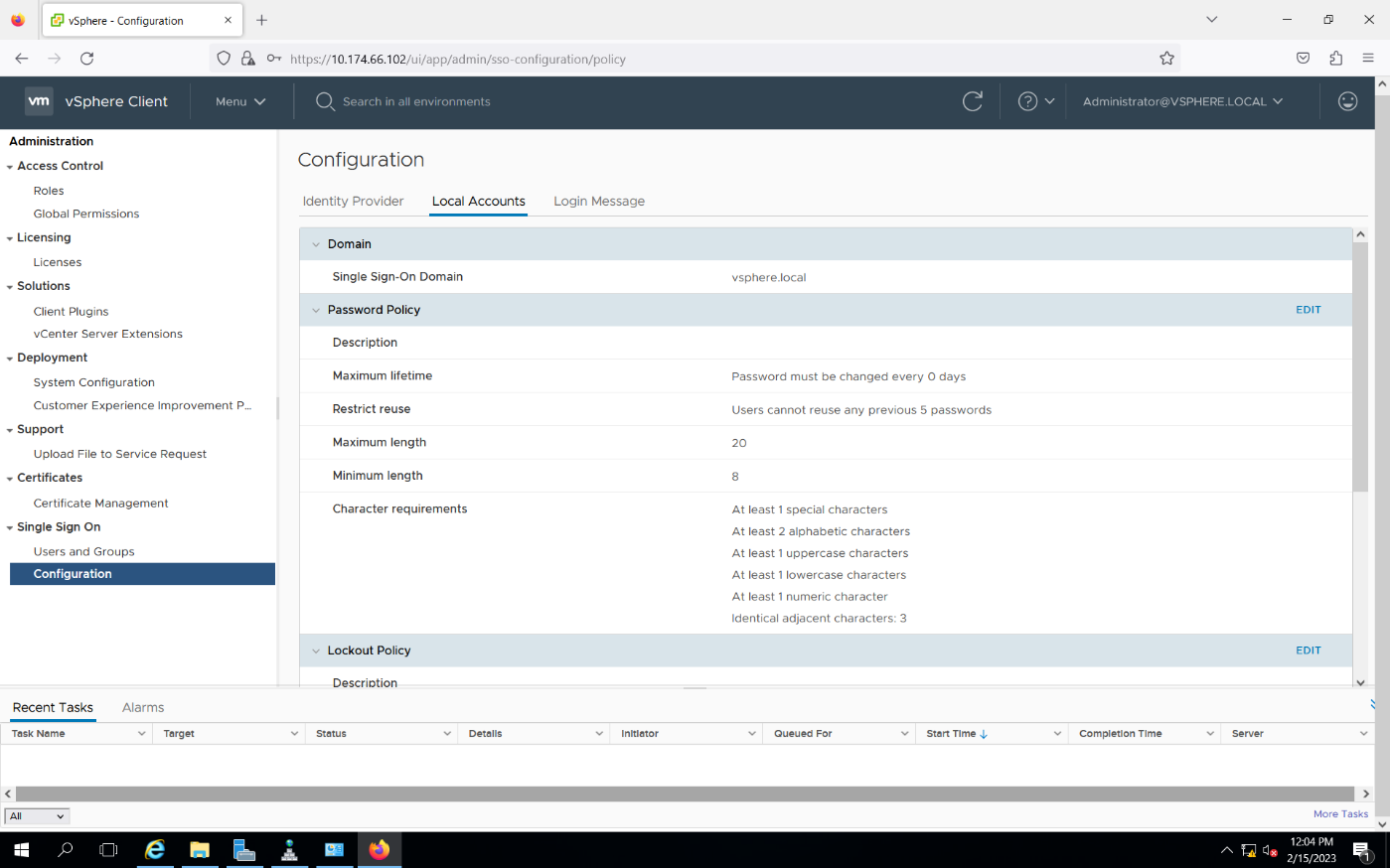
* Connected the Windows server using Remote Desktop connection.
* Ensured that it is connected to the internet after connecting to the RDC.
* Installed Active Domain Service from the Tools taskbar.
* After installing promoted the Infra VM to the Domain Controller in the vclass.local
* Reboot will happen after the previous step.
* Opened the DNS manager from the Tool after rebooting.
* Created a Reverse lookup zone to the subnet.
* Deployed a New VCSA VM.
* Configured the VCSA VM by entering IP and Default Gateway.
* Ensured that the DNS is same as IP of the Windows Infra VM.
* Opened the RDP and connected the vSphere using the VSCA Ip in the Firefox browser.
* Successful connected the VSCA in windows infra vm.
* On the VM center login page entered the given credentials r administrator@vsphere.local as the username,  
  enter Vclass123$ as the password and click Login.
* Selected Administration from the Menu Icon.
* Selected Licenses from the navigator panel.
* Added the new license one for ESXI and one for VCSA.
* Assigned the license for the vcsa.vclass.local

Screenshot

Fig 2.1 Installed AD DS and promoted to DNS

  
Fig 2.2 Created Reverse lookup zone also created host and point records.

Fig 2.3 Deployed VCSA VM and Configuring Ipv4.  
  
  
Fig 2.4 Deployed VCSA VM and Configuring DNS.  
  
  
Fig 2.5 Successfully logged in to vSphere client

  
Fig 2.6 Added Two license one for ESXI and VCSA and assigned the license  
  
  
Fig 2.7 Single sign on configuration page

Reflection  
  
I recently had the chance to configure a Single Sign-On (SSO) solution for a web application utilizing Active Directory (AD) as the identity provider as part of a lab exercise. Overall, I had a real experience, and I think there are several benefits to using AD as an SSO identity provider. The unified management of user accounts and access control is one of the main benefits of utilizing AD as an SSO identity provider. The challenge of managing identity and access across the business is made simpler by AD's ability to let administrators manage users, groups, and computers from a single location. In big or complicated environments where numerous applications and systems need to be secured, this is especially crucial. An further advantage of using AD as an SSO identity provider is the ability to enforce stringent password policies and other security measures. Administrators in AD can define password complexity requirements, account lockout policies, and other security settings to help prevent unauthorized access and protect against password-related attacks. This may be especially important for web applications that must adhere to regulations or hold sensitive data. Using AD as an SSO identity provider can also help to enhance the user experience by allowing users to log in just once and access several applications without having to enter their credentials again. This can reduce user workload, boost output, and diminish the likelihood of password-related security incidents.  
  
Reference  
**Centralized management of user accounts and access control:**

"Benefits of Active Directory": <https://www.microsoft.com/en-us/security/business/identity-and-access-management/benefits-of-active-directory>

"Why Use Active Directory?": <https://www.techrepublic.com/article/why-use-active-directory/>

"Active Directory - Centralized Identity and Access Management": <https://www.manageengine.com/products/ad-manager/active-directory-identity-access-management.html>

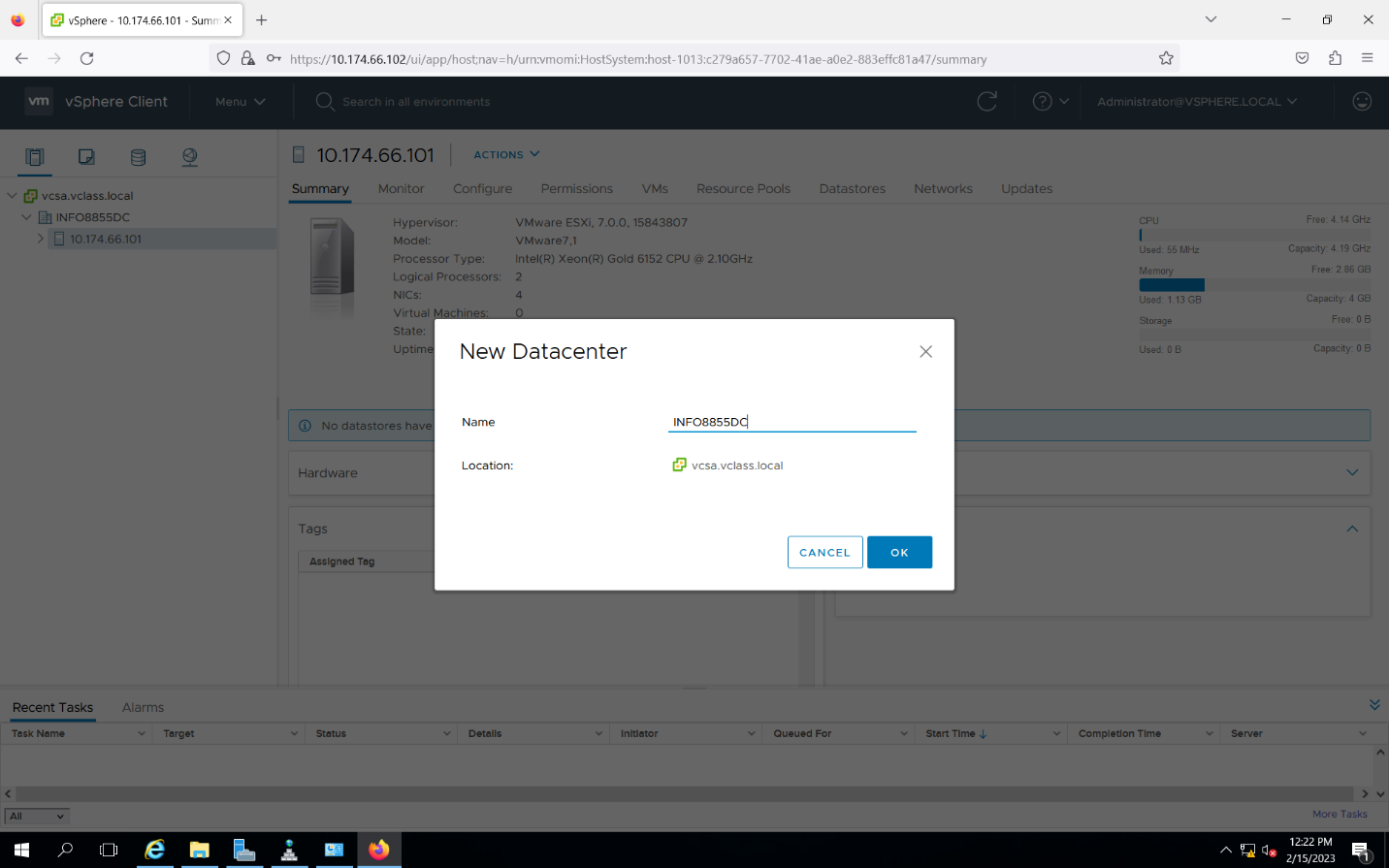
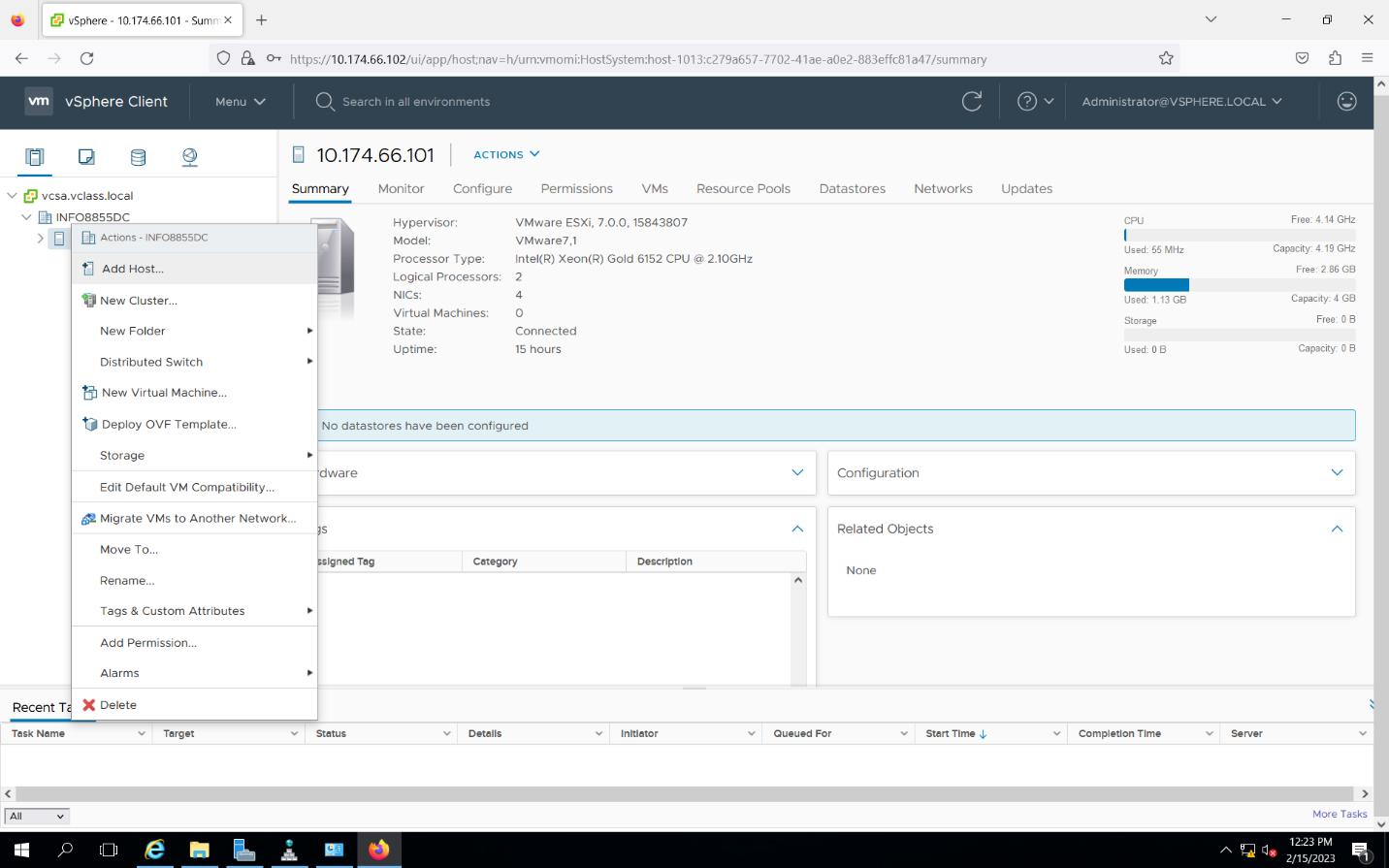
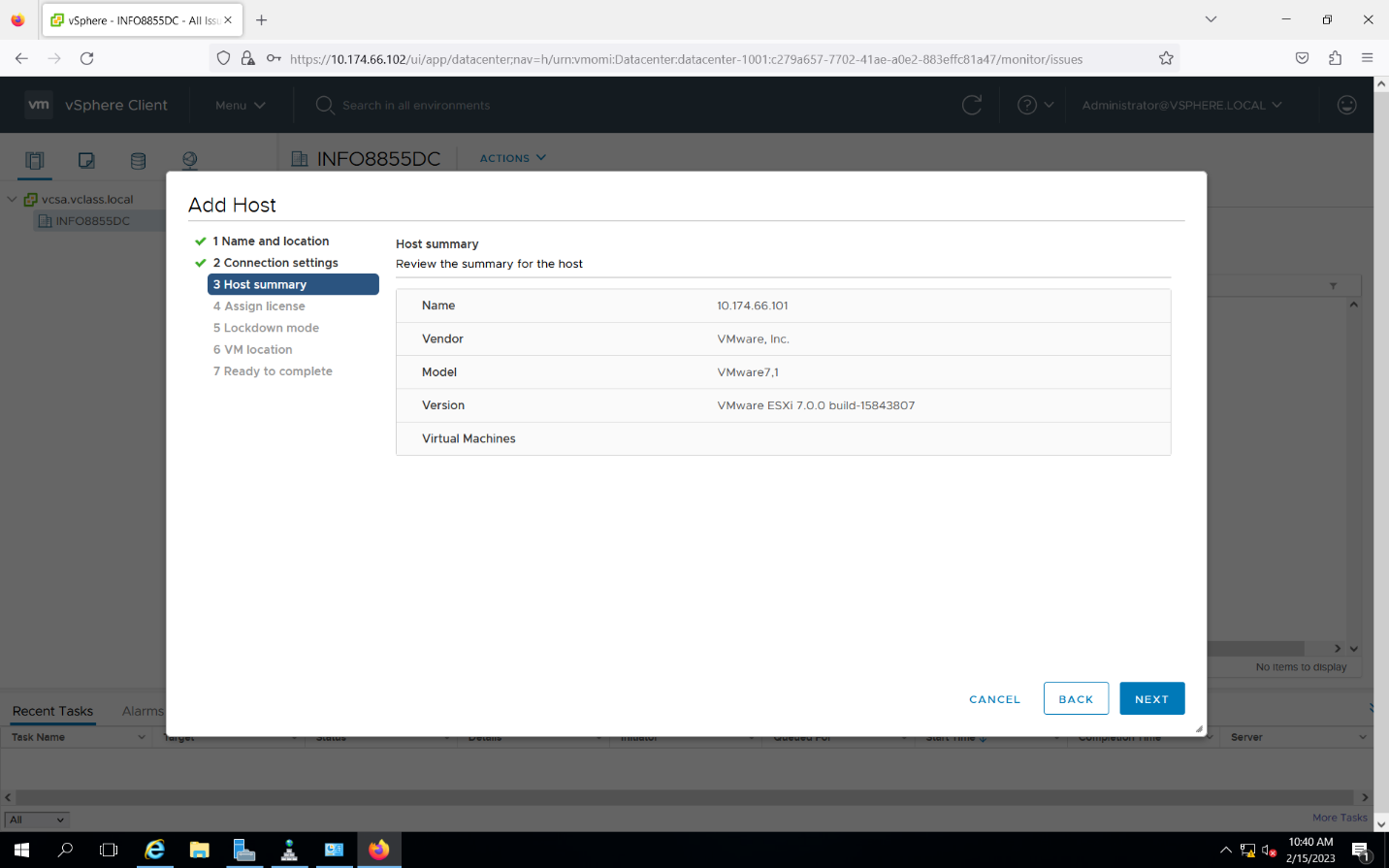
"Active Directory Password Policies: Best Practices, Tips and Tricks": <https://www.netwrix.com/active_directory_password_policies.html>

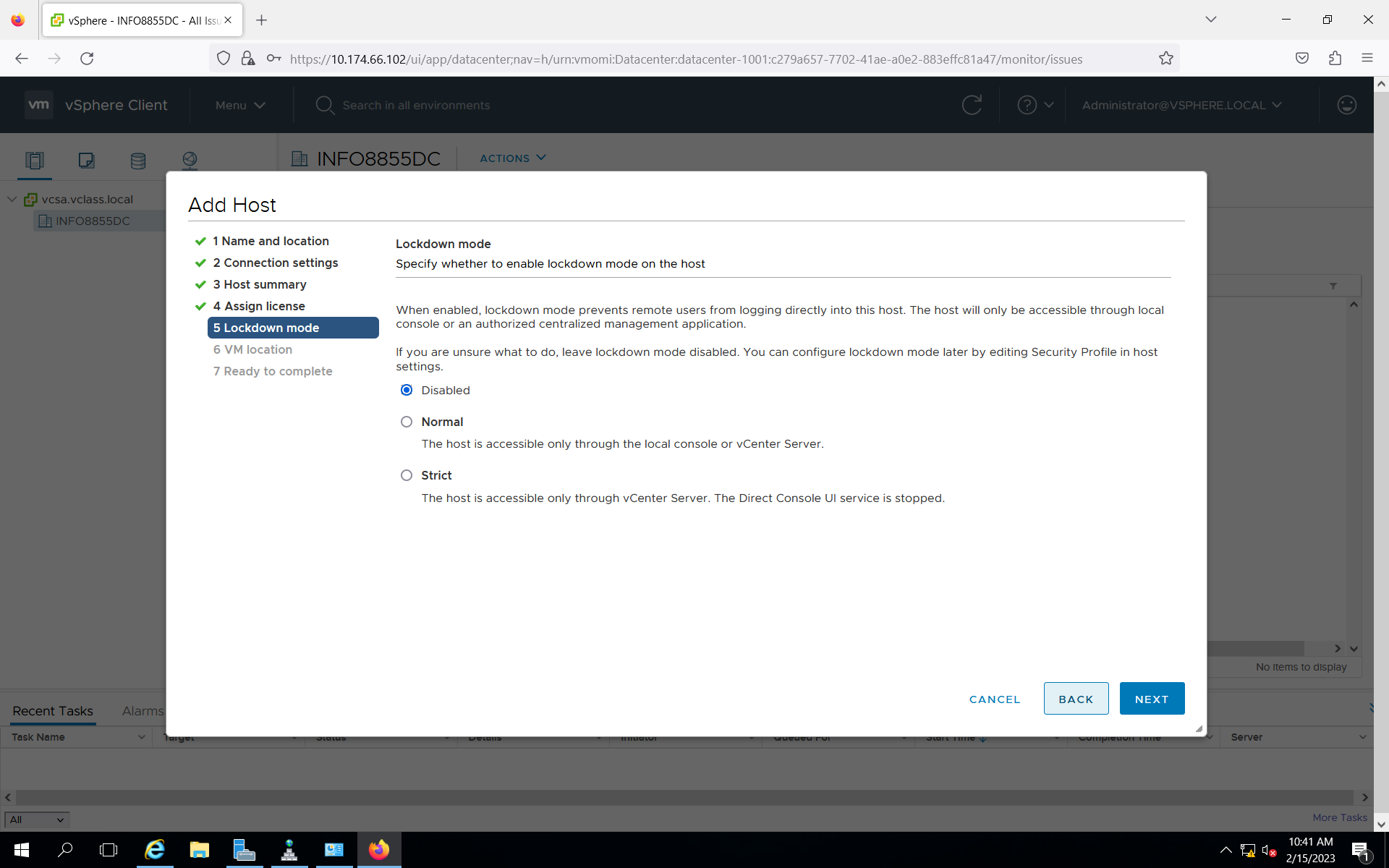
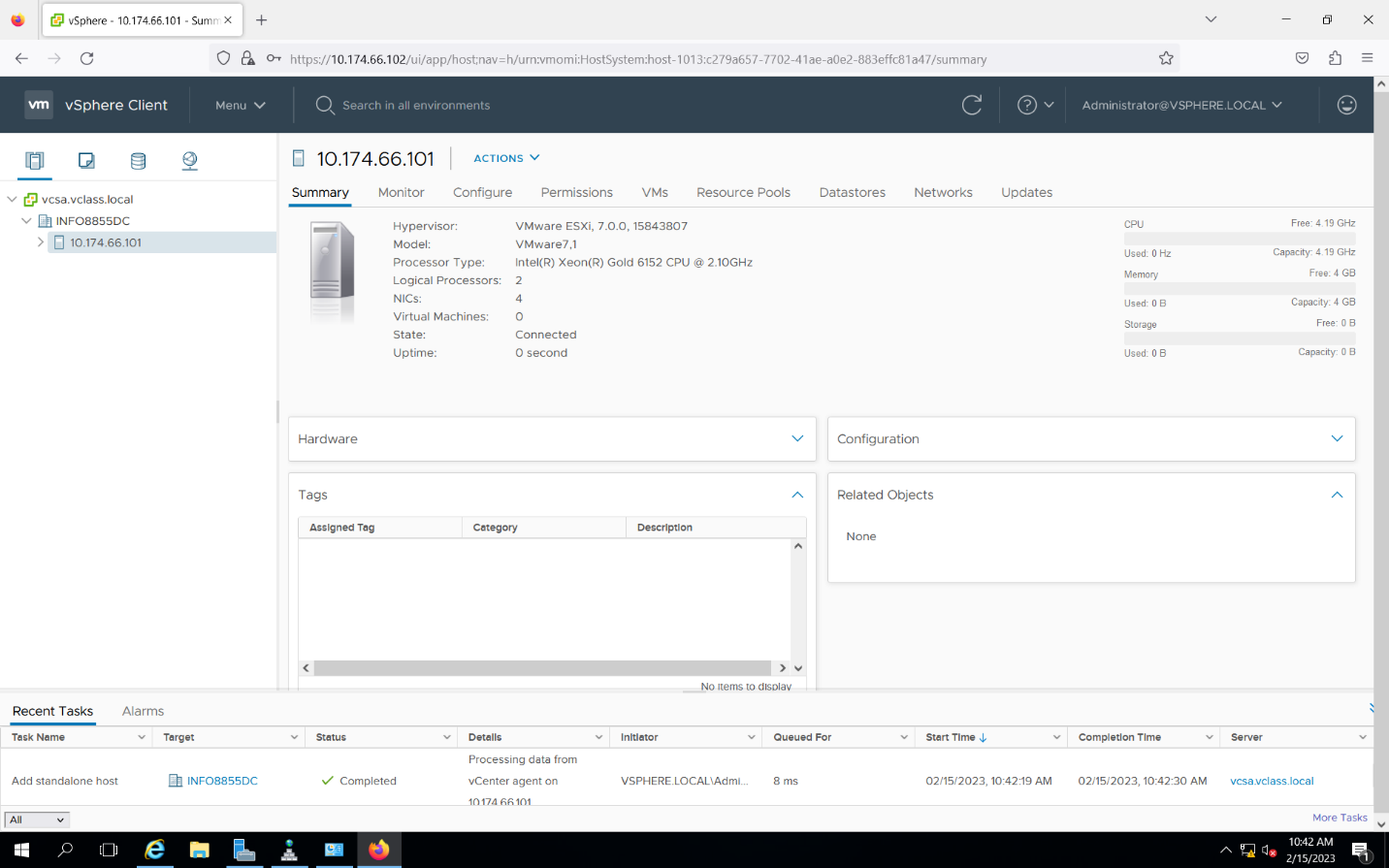
**Streamlining the user experience:**

"Single sign-on (SSO)": <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on>

"Advantages and Disadvantages of SSO": <https://blog.capterra.com/advantages-and-disadvantages-of-sso/>  
  
  
  
Task 3 – Configure Hosts to be Managed by vCenter  
  
Overview  
In this task, we will configure ESXI hosts to be managed by VCSA. Also Adding hosts to the datacenter such that they are managed by vCenter Server Appliance.  
  
Description

* In home page Selected the New Datacenter.
* Added the Datacenter as INFO8855DC.
* Under Datacenter Added new host by clicking New Host.
* Enter the ESXI ip address and click Next.
* Under Lockdown mode selected Disabled.
* Click Finish and successfully added the Host

Screenshots  
  
Fig 3.1 Created New datacenter named INFO8855DC  
  
  
Fig 3.2 Adding New host to the datacenter  
  
Fig 3.3 Adding ESXI IP to the host

  
Fig 3.4 Under lockdown mode selected Disabled.  
  
  
Fig 3.5 Successfully added the host to the Datacenter  
  
Reflection  
  
I recently got the chance to investigate the advantages of controlling ESXI hosts with vCenter Server as opposed to stand-alone administration during a lab exercise. Overall, I discovered that managing ESXI hosts using vCenter Server offers a variety of benefits that make it a more effective and efficient way to manage virtual infrastructure. The central management of virtual infrastructure is one of the main advantages of adopting vCenter Server. Administrators can control numerous ESXI hosts and virtual machines from a single location using vCenter Server. Especially in big or complex situations where there are numerous hosts and virtual machines that need to be maintained, this makes it simpler to manage virtual infrastructure. Utilizing vCenter Server also has the benefit of allowing for the automation of routine operations and workflows. Administrators can automate resource allocation, write custom workflows, and run scripts using vCenter Server to expedite routine activities. As a result, managing virtual infrastructure may take less time and effort, and accuracy and consistency may also improve.  
  
Reference  
**Centralized management of virtual infrastructure:**

"What is VMware vCenter Server and What Are Its Advantages?": <https://www.nakivo.com/blog/vmware-vcenter-server-advantages/>

"vSphere: The Benefits of vCenter Server": <https://blog.infradata.com/vsphere-the-benefits-of-vcenter-server>

**Automation of common tasks and workflows:**

"VMware vCenter Server – Centralized Control for Your Datacenter": <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vcenter/VMware_vCenter_Server.pdf>

"Automating vSphere Tasks with PowerCLI": <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/automating-vsphere-tasks-with-powercli.pdf>