GETTING STARTED IN INSECLAB SYSTEM

Contents

I. SETTING UP AND CONFIGURATION

1.1. Introduce the system

For research and studying purposes of researchers and students in UIT, this system is built. You can create virtual machines, network topologies, etc for our research.

The system includes a local domain: *inseclab.local*. We will use this domain and its subdomain to access resources of the system. You use some hosts below to access the system.

- vCenter: *vcenter.inseclab.local* (10.102.0.3)
- VMware host 1: *vmware162.inseclab.local* (10.102.0.251)

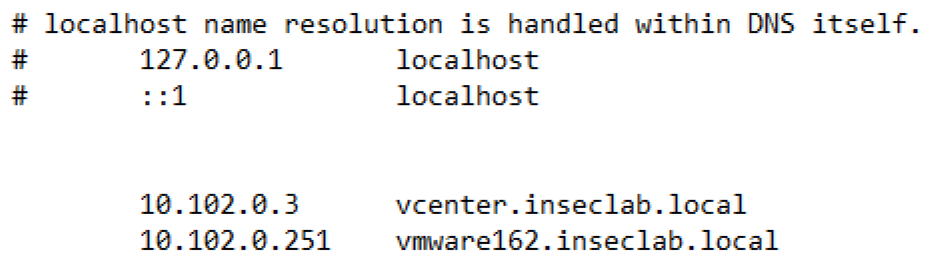
1.2. Configure hosts file

To access the system, you have to edit the *hosts* file in your computer instead of changing DNS.

In Windows system, run notepad as Administrator and open hosts file at path:
C:\Windows\System32\drivers\etc\hosts

Add new lines into *hosts* file.

```
10.102.0.3      vcenter.inseclab.local

10.102.0.251    vmware162.inseclab.local
```



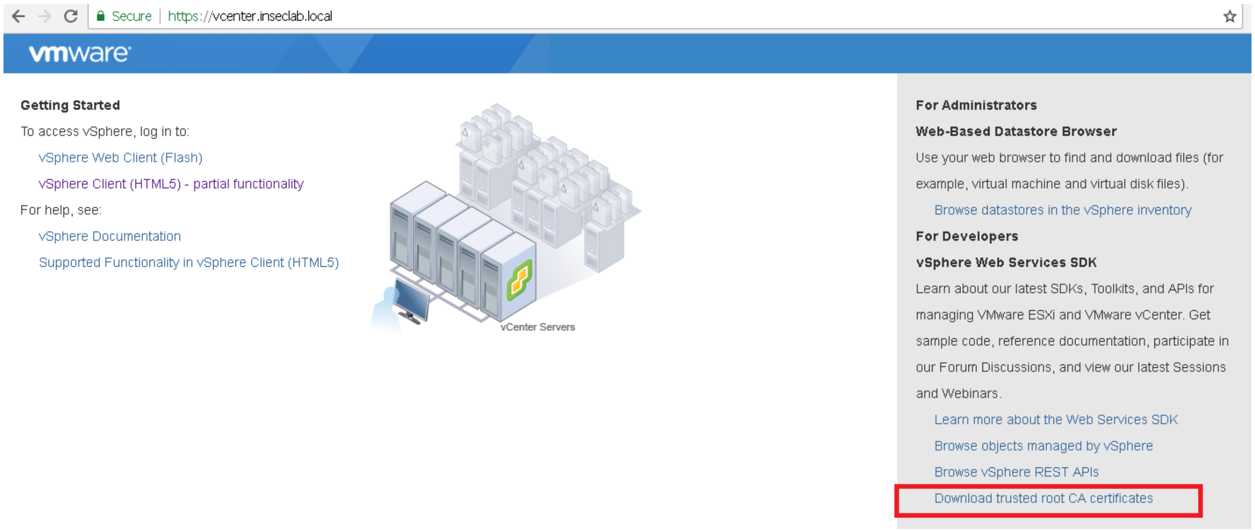
```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


        10.102.0.3      vcenter.inseclab.local
        10.102.0.251    vmware162.inseclab.local
```

Save and close *hosts* file.

1.3. Import vCenter certifites

Open your web browser and enter: https://vcenter.inseclab.local

At the first time, your will see a alert for untrusted web site because vcenter use a self-signed certificates. So you need to download and inport this certificates to your system.



Getting Started

To access vSphere, log in to:

- vSphere Web Client (Flash)
- vSphere Client (HTML5) - partial functionality

For help, see:

- vSphere Documentation
- Supported Functionality in vSphere Client (HTML5)

For Administrators

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- Browse datastores in the vSphere inventory

For Developers

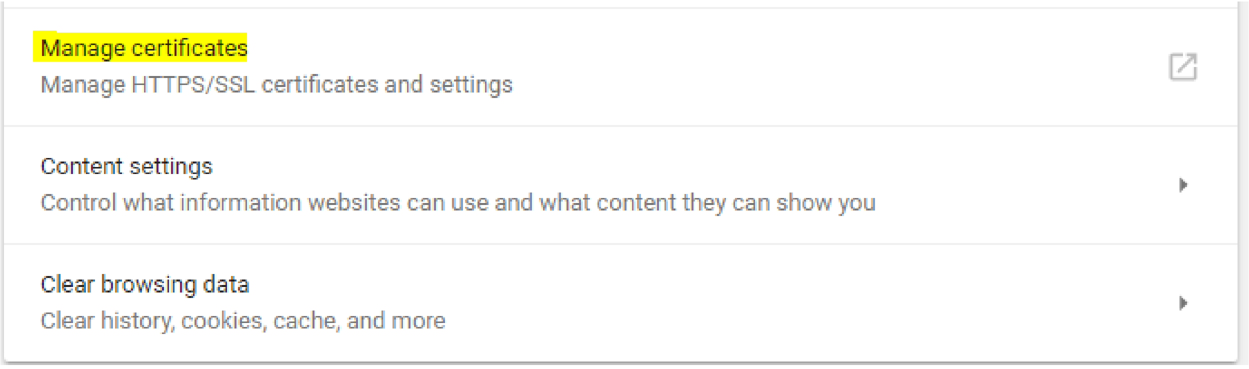
vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESXi and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- Learn more about the Web Services SDK
- Browse objects managed by vSphere
- Browse vSphere REST APIs
- Download trusted root CA certificates

Click *Download trusted root CA certificates* to download the certificates. After completing download, extract file and import to the browser.

In Google Chrome, go to *Settings* and click *Advanced*. And find *Manage certificates*.

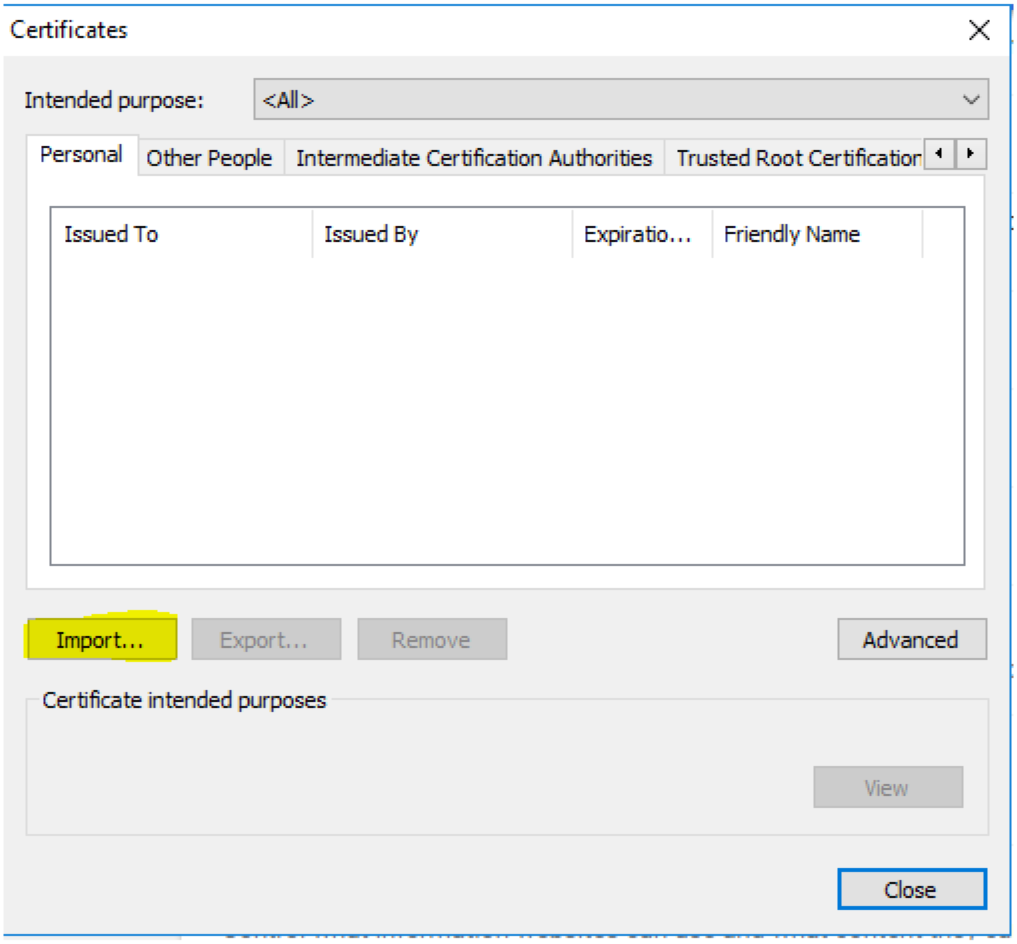


Manage certificates
Manage HTTPS/SSL certificates and settings

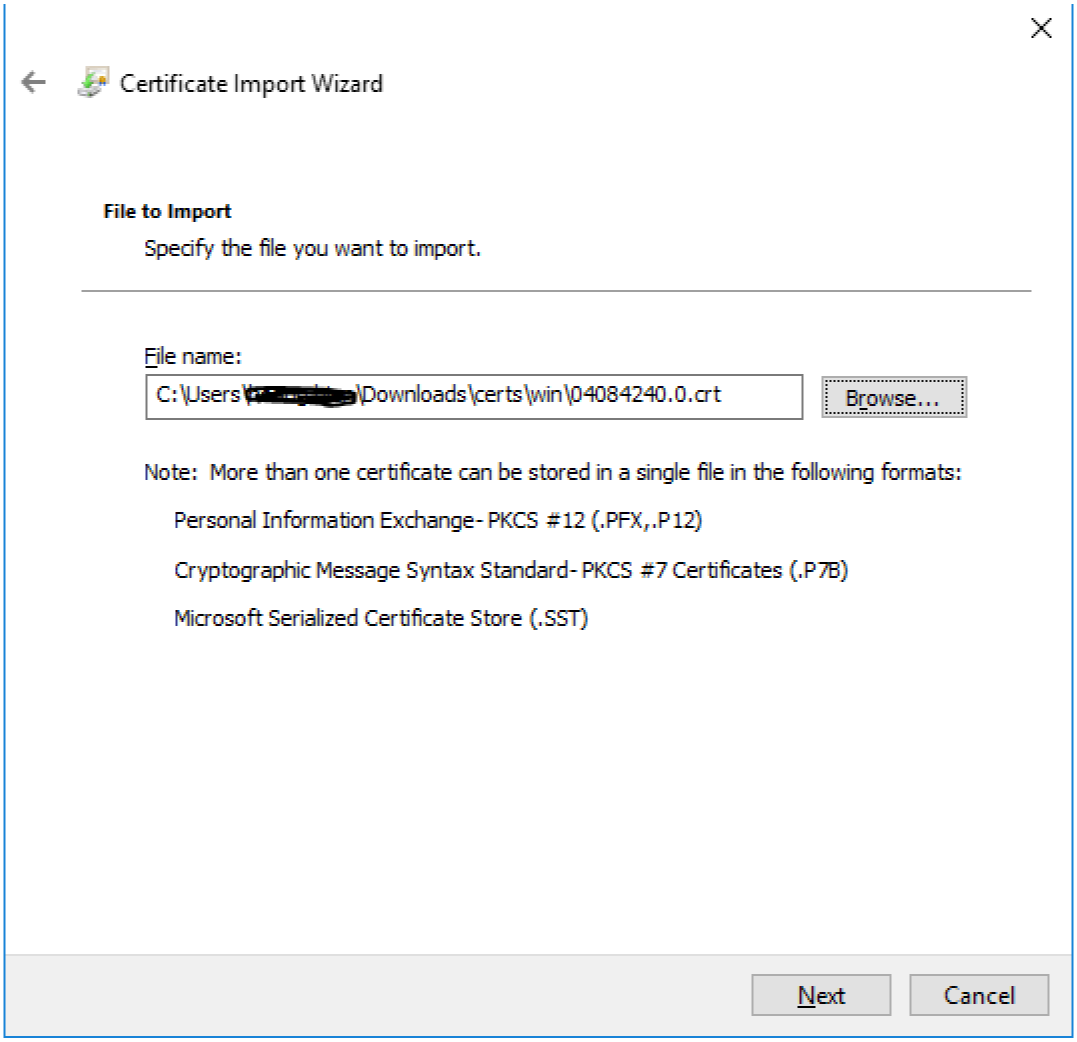
Content settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

In Certificates dialog, click Import and browse to cert file.



Intended purpose: <All>



File to Import

Specify the file you want to import.

File name:

C:\Users\[redacted]\Downloads\certs\win\04084240.0.crt

Note: More than one certificate can be stored in a single file in the following formats:

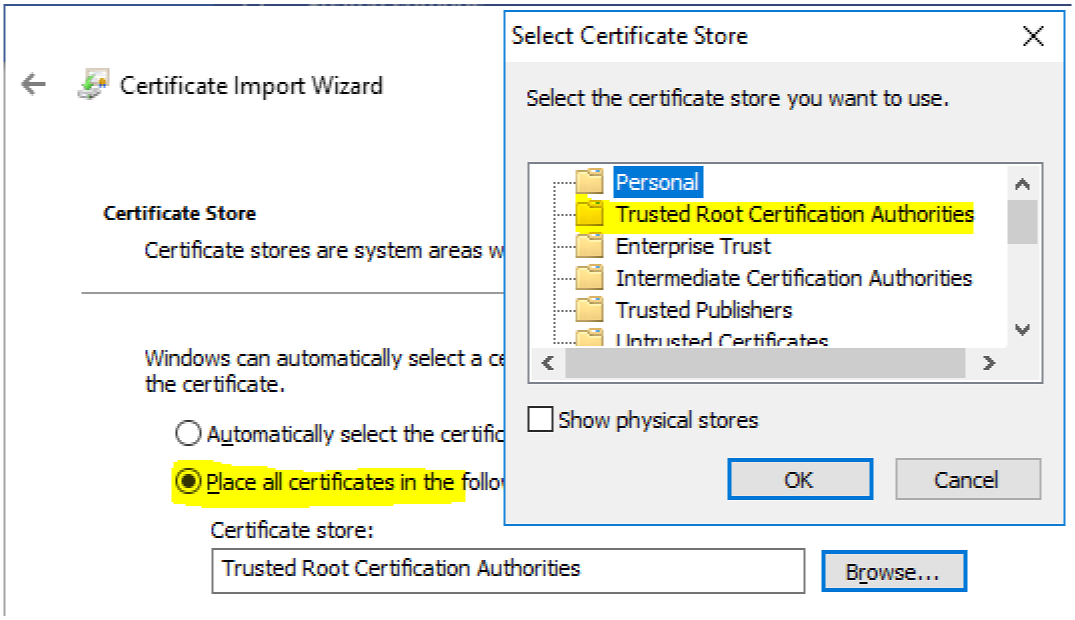
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Click Next to continue.

In this dialog, click *Browse* button, and select *Trusted Root Certification Authorities* and click OK.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas w

Windows can automatically select a ce
the certificate.

○ Automatically select the certific

● Place all certificates in the follo

Certificate store:

Trusted Root Certification Authorities

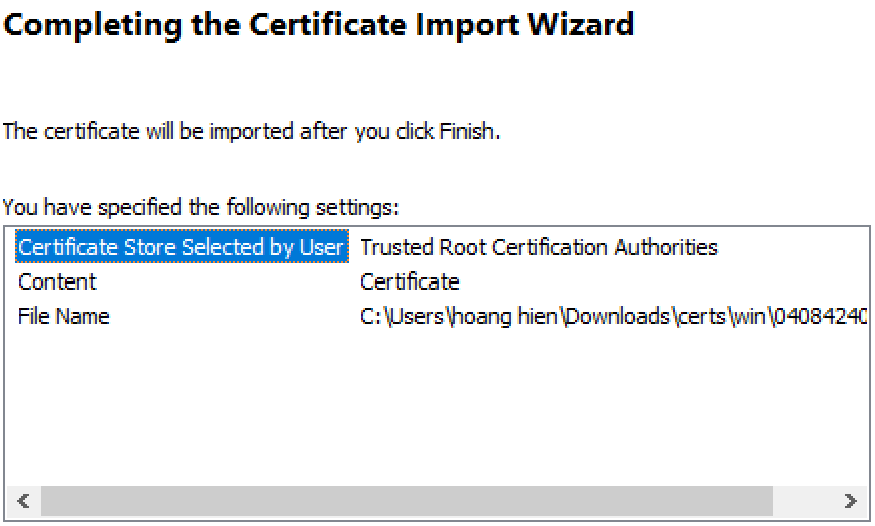
Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates

□ Show physical stores

Click Next and Finish.



Completing the Certificate Import Wizard

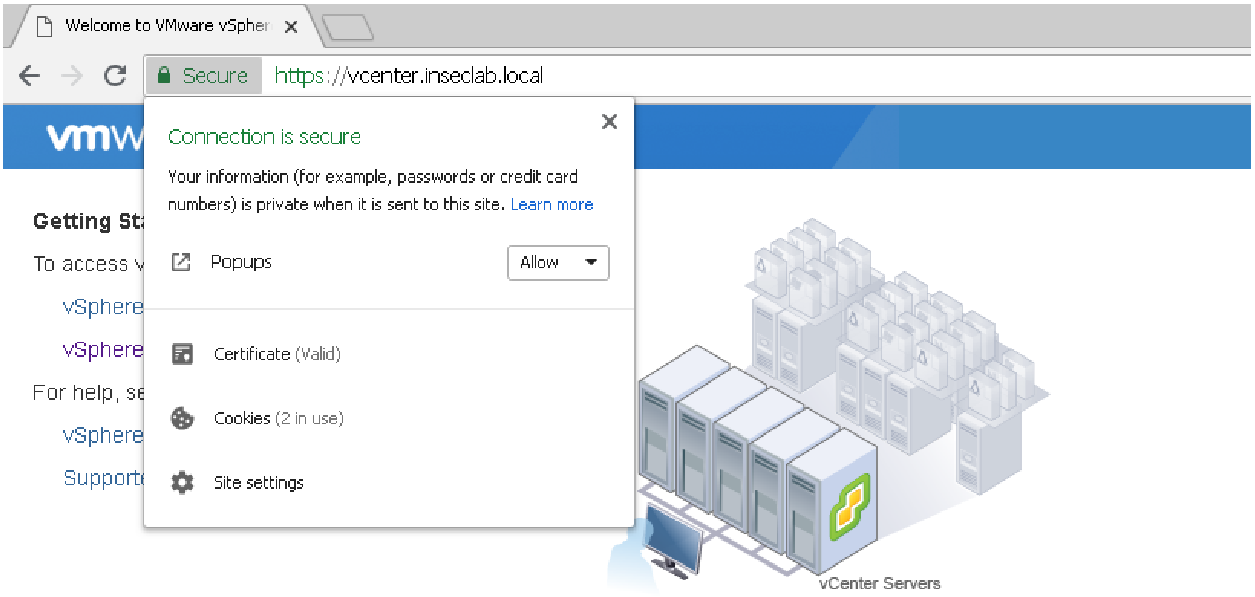
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\hoang hien\Downloads\certs\win\0408424

You finished to import the certificates. Close your web browser, reopen it and access https://vcenter.inseclab.local. In some cases, you need to clear history, cache of browser after importing certificates.

Now, you can see the web site connect is secure.

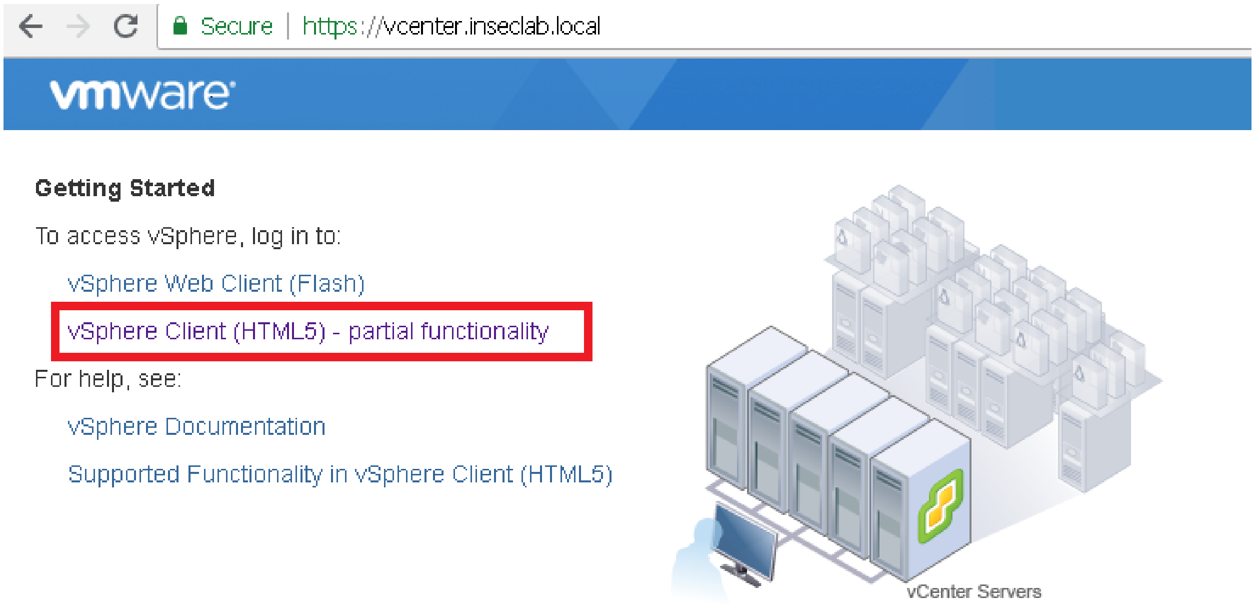


Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

1.4. Access vCenter

In your browser, enter https://vcenter.inseclab.local ,and click *vSphere Client (HTML5) - partial functionality*



Getting Started

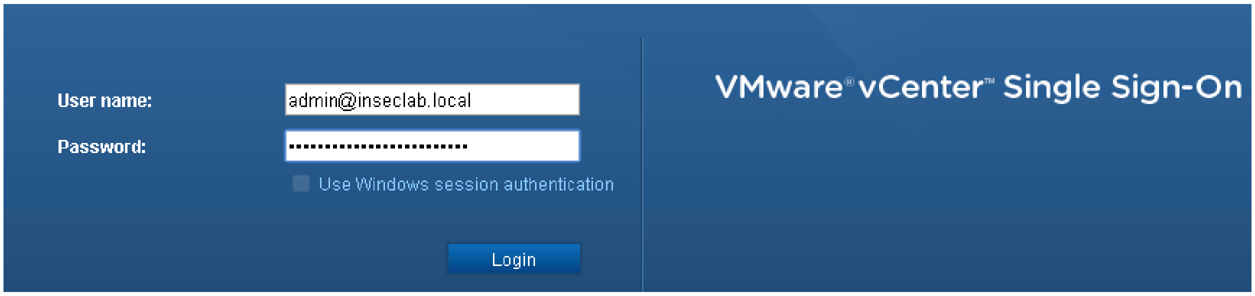
To access vSphere, log in to:

- vSphere Web Client (Flash)
- vSphere Client (HTML5) - partial functionality

For help, see:

- vSphere Documentation
- Supported Functionality in vSphere Client (HTML5)

Use your account to login vCenter.



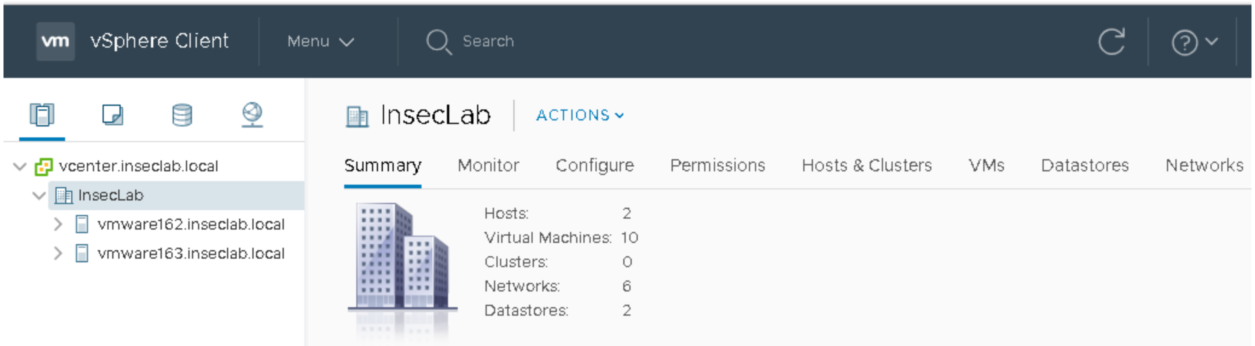
VMware® vCenter™ Single Sign-On

User name: admin@inseclab.local

Password: ••••••••••••••••••••••••••

□ Use Windows session authentication

After you login in successfully, you can see vCenter interface like this.



Hosts:	2
Virtual Machines:	10
Clusters:	0
Networks:	6
Datastores:	2

1.5. Install Vmware Remote Console

VMware Remote Console provides console access and client device connection to VMs on a remote host.

Go to https://drive.google.com/drive/folders/1lLCqMTNrGa39QMs7A5Qe4thCuXA5zfWd and download VMware Remote Console and install it. Vmware supports Linux, MacOS and Windows.

II. ACCESS YOUR LAB

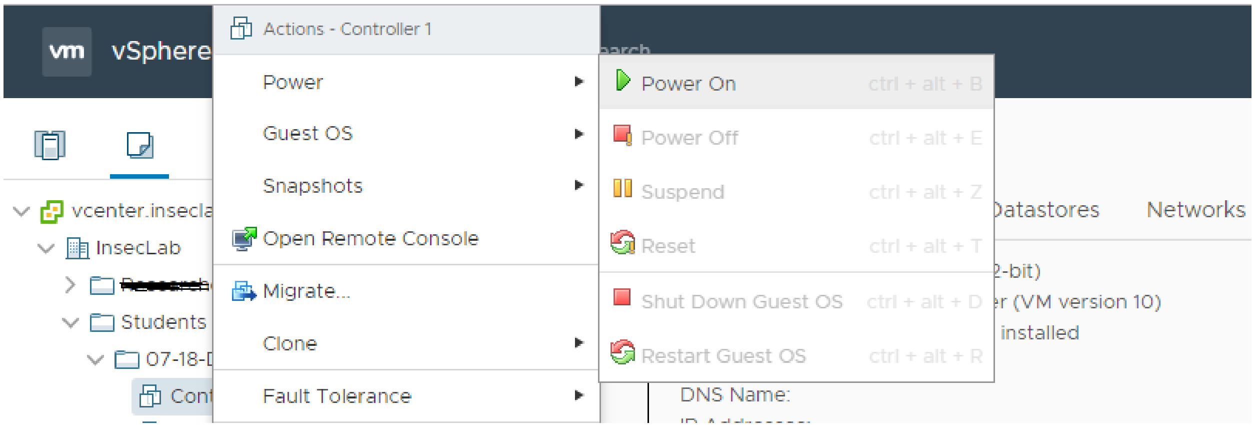
2.1 Access console for control

VMware vCenter supports 2 interface for controlling VMs: Web Console and Remote Console.

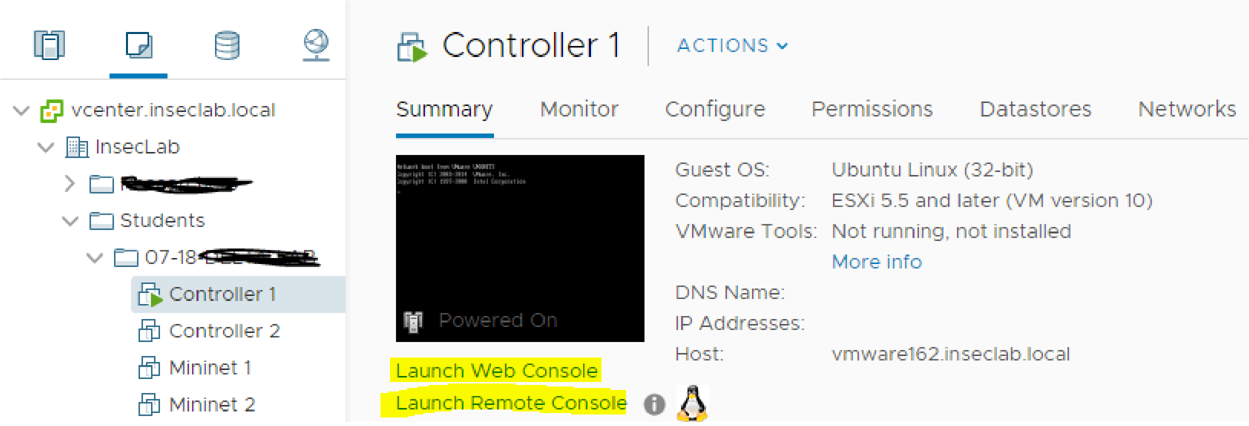
With the Web Console, you can access a virtual machine's desktop by launching a console to the virtual machine. From the console, you can perform activities in the virtual machine such as configure operating system settings, run applications, monitor performance, and so on.

VMware Remote Console provides access to virtual machines on remote hosts and performs console and device operations such as configuring operating system settings and monitoring the VM console for VMware vSphere. VMware Remote Console can also modify virtual machine settings such as RAM, CPU cores, and disks.

In vCenter, select a VM and press *Power On*.

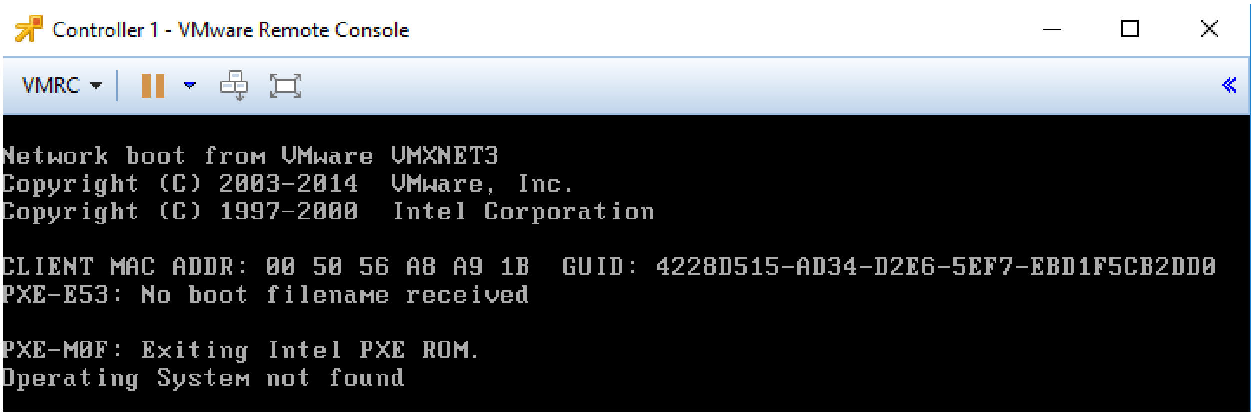


Select *Lanch Web Console* or *Lanch Remote Console*.

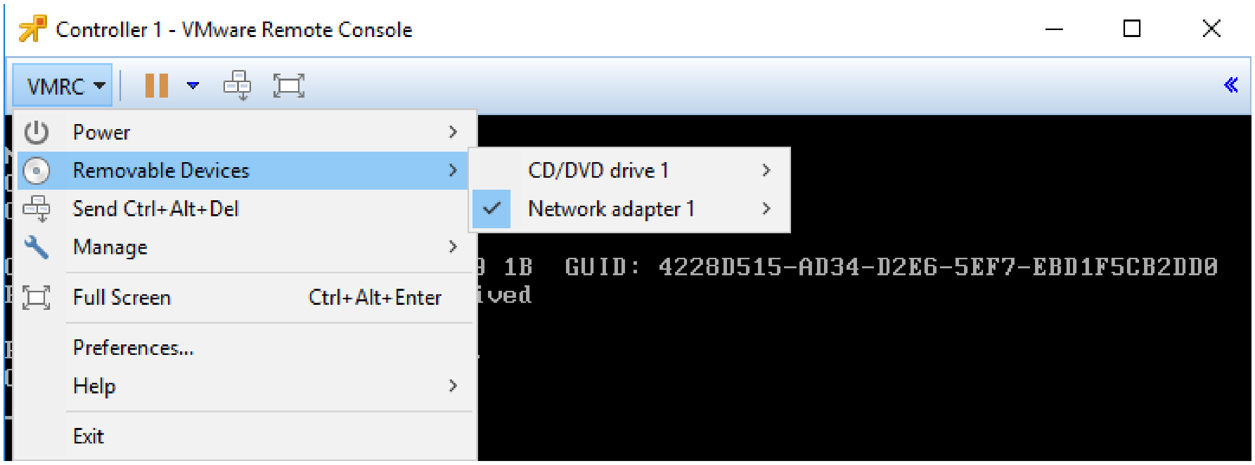


Guest OS: Ubuntu Linux (32-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Not running, not installed
DNS Name:
IP Addresses:
Host: vmware162.inseclab.local

In Remote Console, you can control some remote devices.



```
Network boot from VMware VMXNET3
Copyright (C) 2003-2014  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 50 56 A8 A9 1B  GUID: 4228D515-AD34-D2E6-5EF7-EBD1F5CB2DD0
PXE-E53: No boot filename received

PXE-M0F: Exiting Intel PXE ROM.
Operating System not found
```



```
9 1B  GUID: 4228D515-AD34-D2E6-5EF7-EBD1F5CB2DD0
ived
```