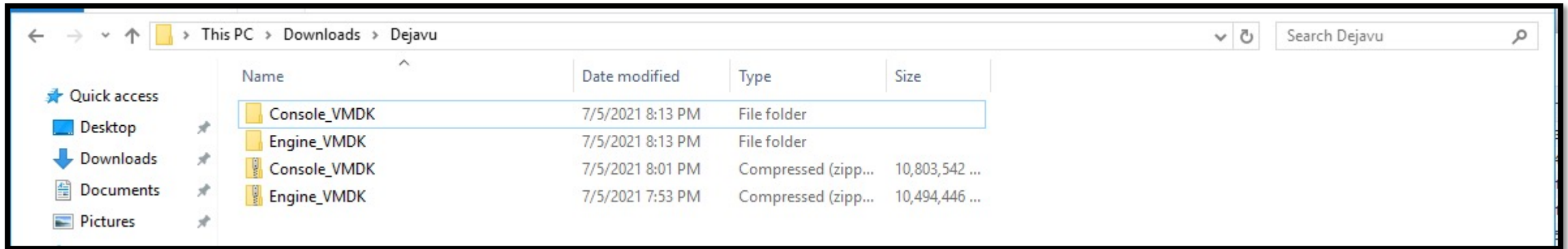
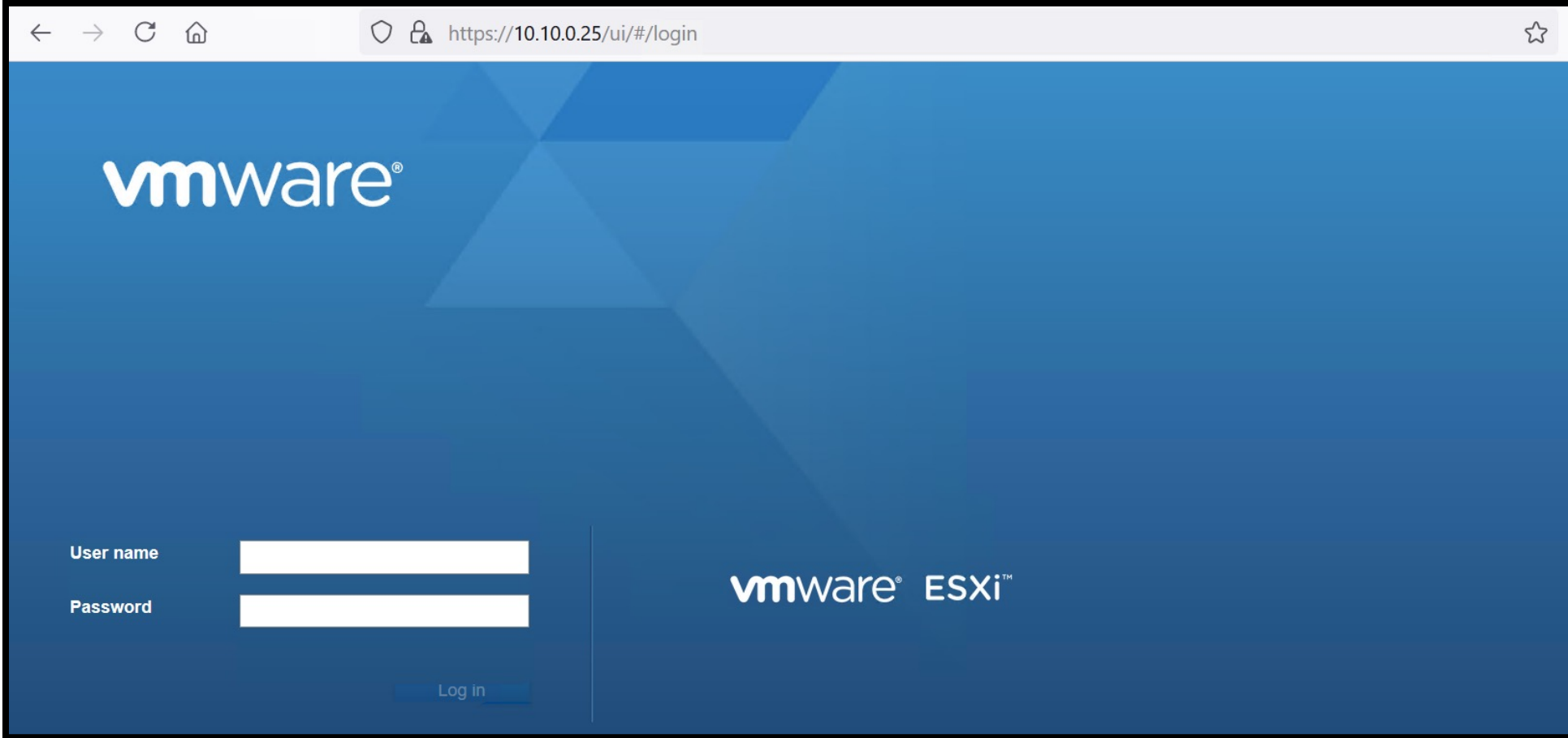


Dejavu Engine Installation Guide - VMware ESXi

Once download is Completed , extract both the files (“Console_VMDK.zip” & “Engine_VMDK.zip”)



Now Open VMware ESXi Web UI with “root” login Credentials to upload DeJaVu console and DeJaVu engine VMDK files into Data Store



The screenshot shows a web browser window with the address bar displaying `https://10.10.0.25/ui/#/login`. The page has a blue background with the VMware logo in the top left. In the bottom left, there are two white input fields labeled "User name" and "Password". A blue "Log in" button is positioned below the "Password" field. On the right side of the page, the text "vmware ESXi™" is displayed.

vmware®

User name

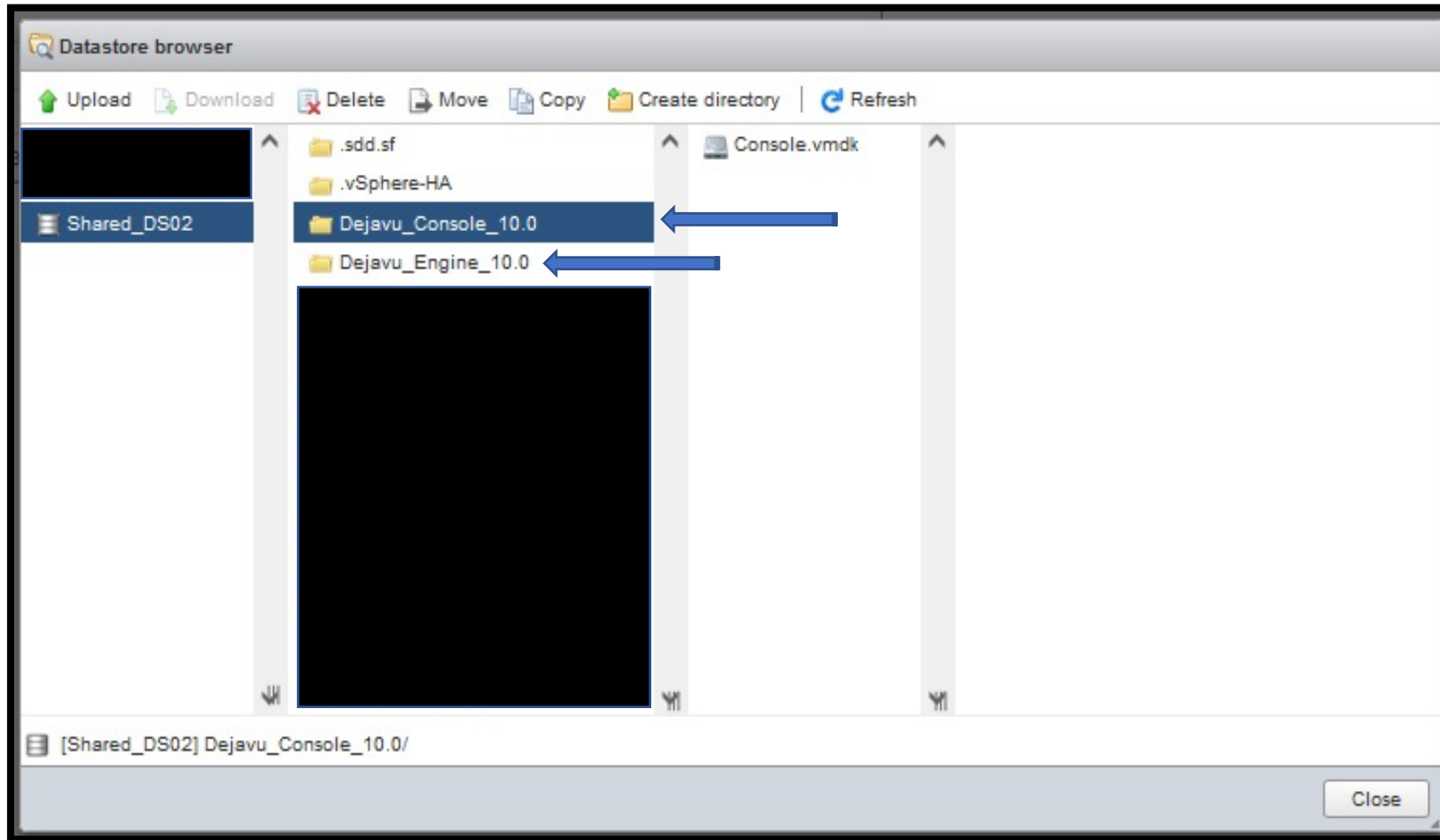
Password

Log in

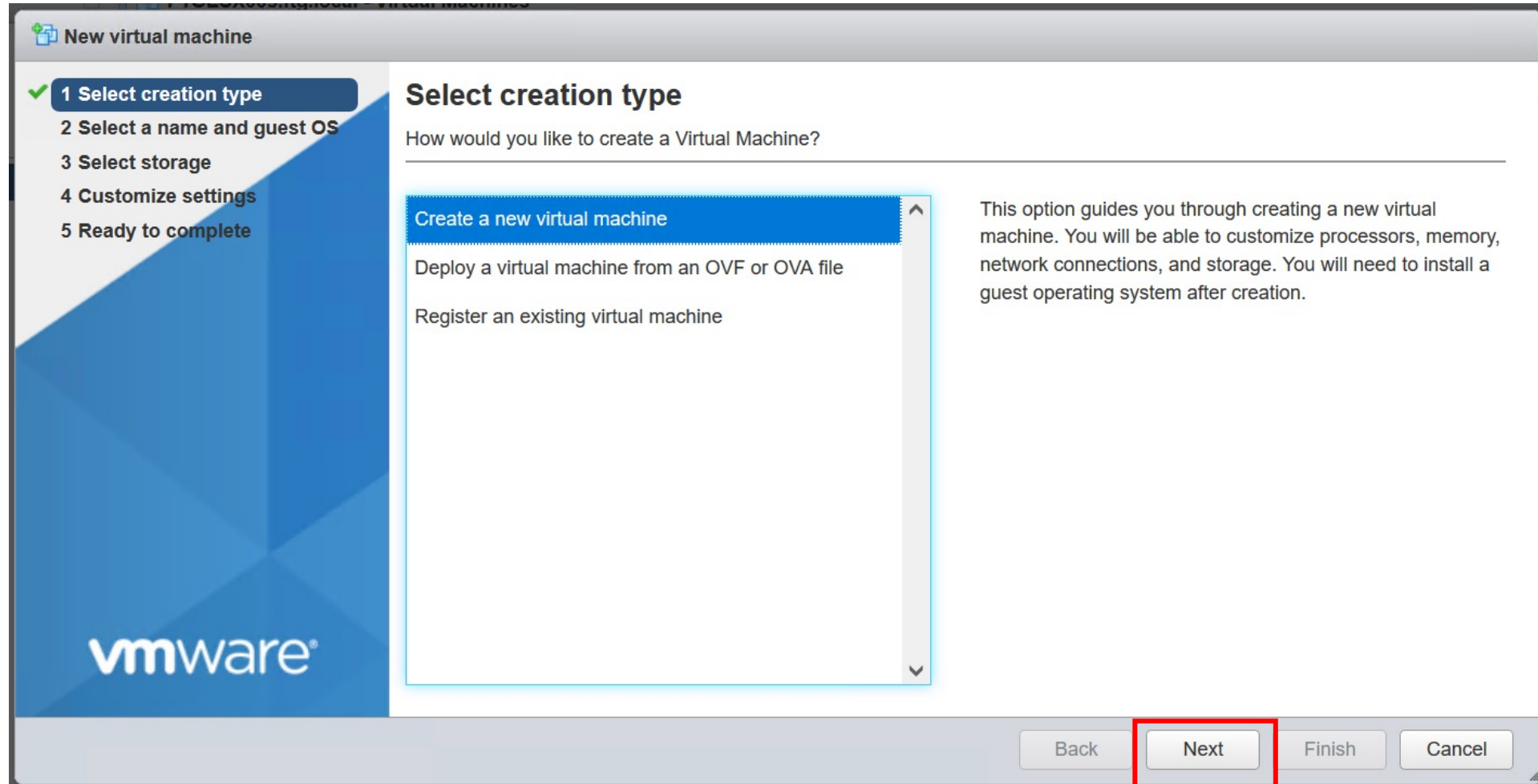
vmware® ESXi™

Create two directories:

1. DejaVu Console 2.0 – Upload Extracted DejaVu Console_VMDK_2.0.vmdk File in Dejavu_Console
2. DejaVu Engine 2.0 - Upload Extracted DejaVu Engine2.0.vmdk File in Dejavu_Engine



Now create the new virtual machine



Set desired name - I have set it as “Dejavu_Console_Server”

The screenshot shows the 'New virtual machine' wizard in VMware vSphere. The title bar reads 'New virtual machine - Dejavu_Engine_Server (ESXi 6.5 virtual machine)'. On the left, a progress bar shows five steps: 1. Select creation type, 2. Select a name and guest OS (highlighted), 3. Select storage, 4. Customize settings, and 5. Ready to complete. The main area is titled 'Select a name and guest OS' with the instruction 'Specify a unique name and OS'. A text box for 'Name' contains 'Dejavu_Engine_Server'. Below this, a note states: 'Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.' Another note says: 'Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.' There are three dropdown menus: 'Compatibility' set to 'ESXi 6.5 virtual machine', 'Guest OS family' set to 'Other', and 'Guest OS version' set to 'Other (64-bit)'. At the bottom right, there are four buttons: 'Back', 'Next' (highlighted with a red rectangle), 'Finish', and 'Cancel'. The VMware logo is in the bottom left corner.

New virtual machine - Dejavu_Engine_Server (ESXi 6.5 virtual machine)

1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select a name and guest OS
Specify a unique name and OS

Name
Dejavu_Engine_Server

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility → ESXi 6.5 virtual machine ▼

Guest OS family → Other ▼

Guest OS version → Other (64-bit) ▼

vmware

Back Next Finish Cancel

Select your data store to DejaVu VMDK file

New virtual machine - DejaVu_Engine_Server (ESXi 6.5 virtual machine)

- ✓ 1 Select creation type
- ✓ 2 Select a name and guest OS
- ✓ 3 Select storage
- 4 Customize settings
- 5 Ready to complete

Select storage

Select the storage type and datastore

☒ Standard ☐ Persistent Memory

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pr...	Access
[Redacted]					
Shared_DS02	6 TB	3.94 TB	VMFS5	Supported	Single

3 items

vmware

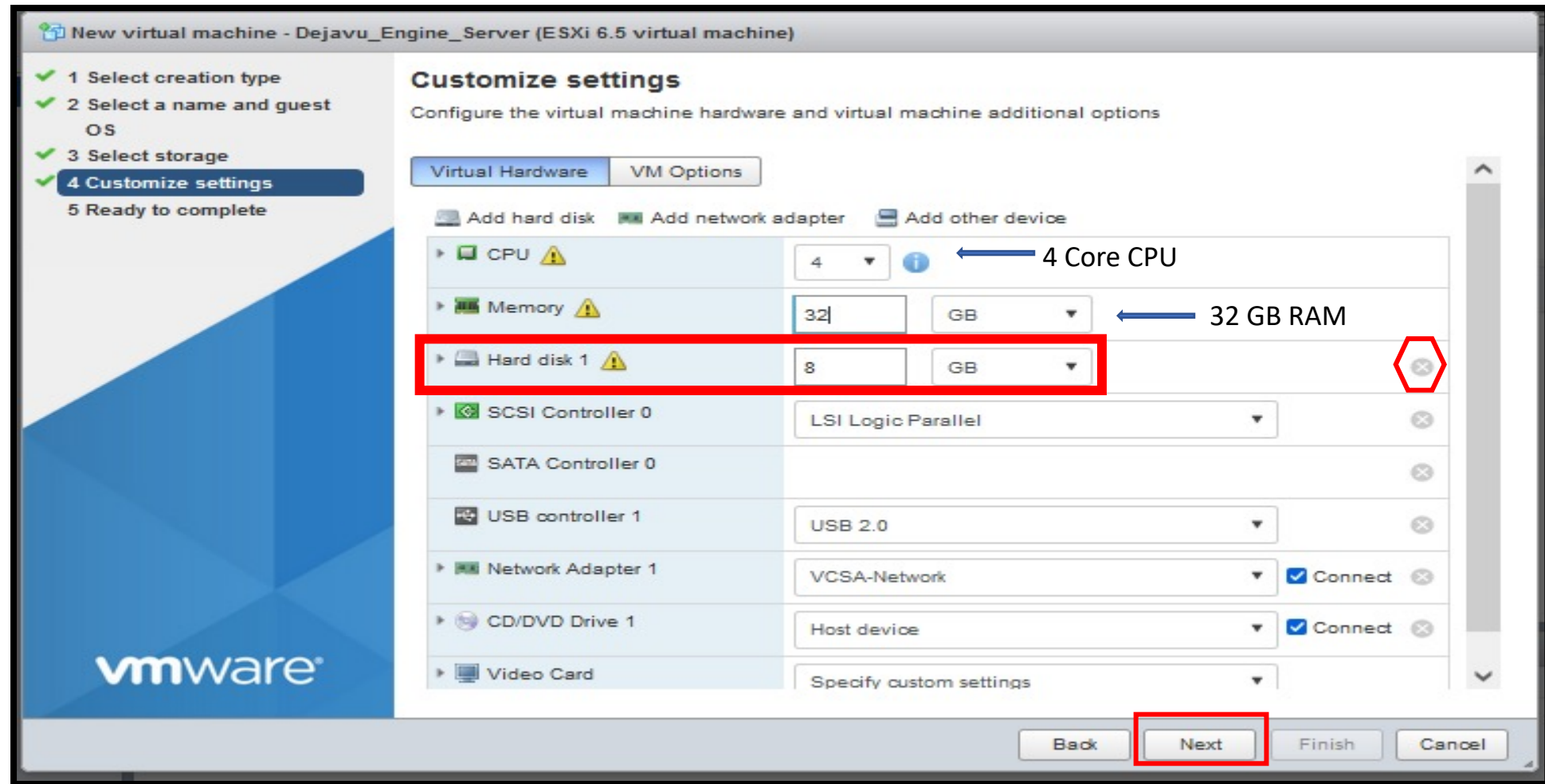
Back Next Finish Cancel

Datastore

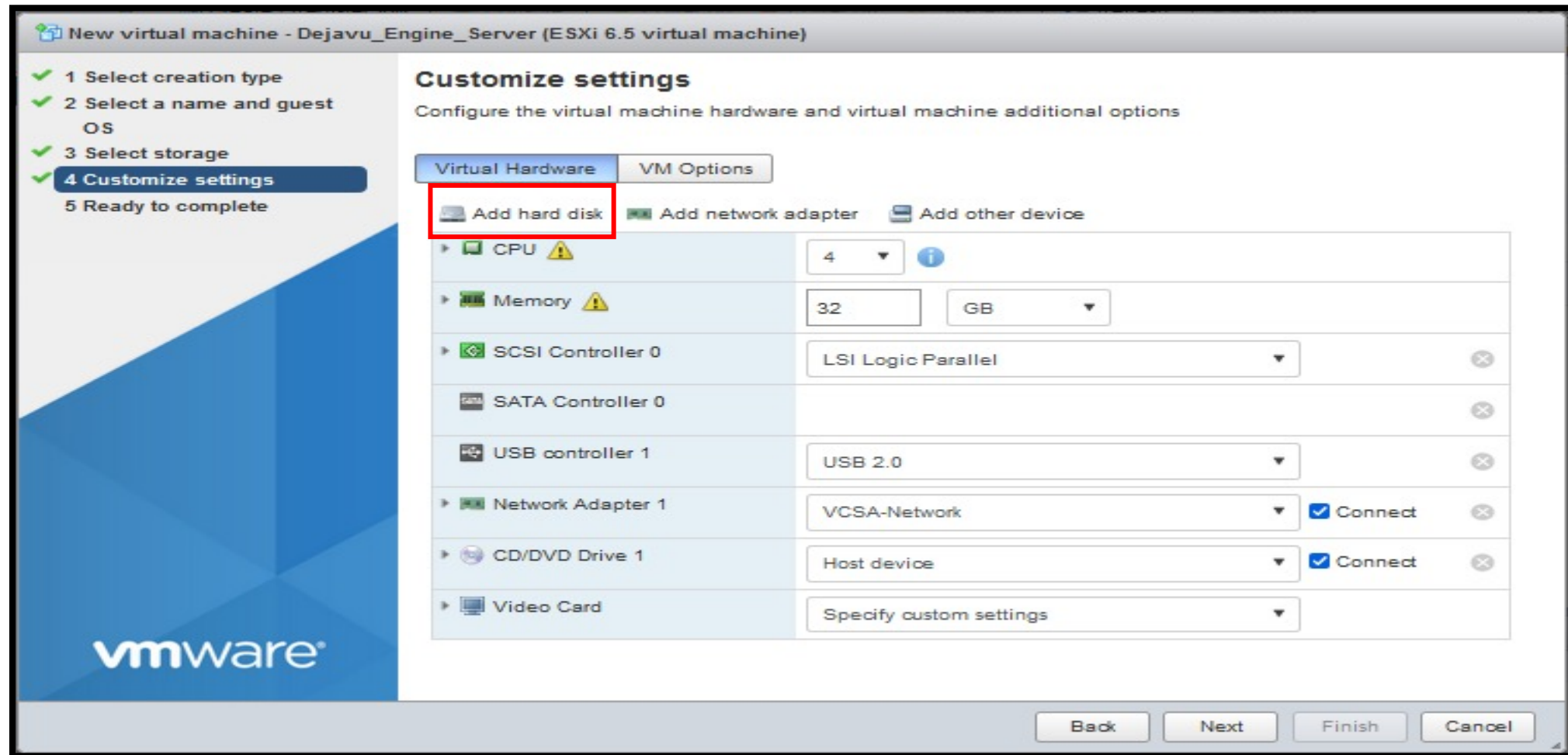
Virtual Machine hardware Configuration for DejaVu engine server

- . 4 Core CPU
- . 32 GB RAM

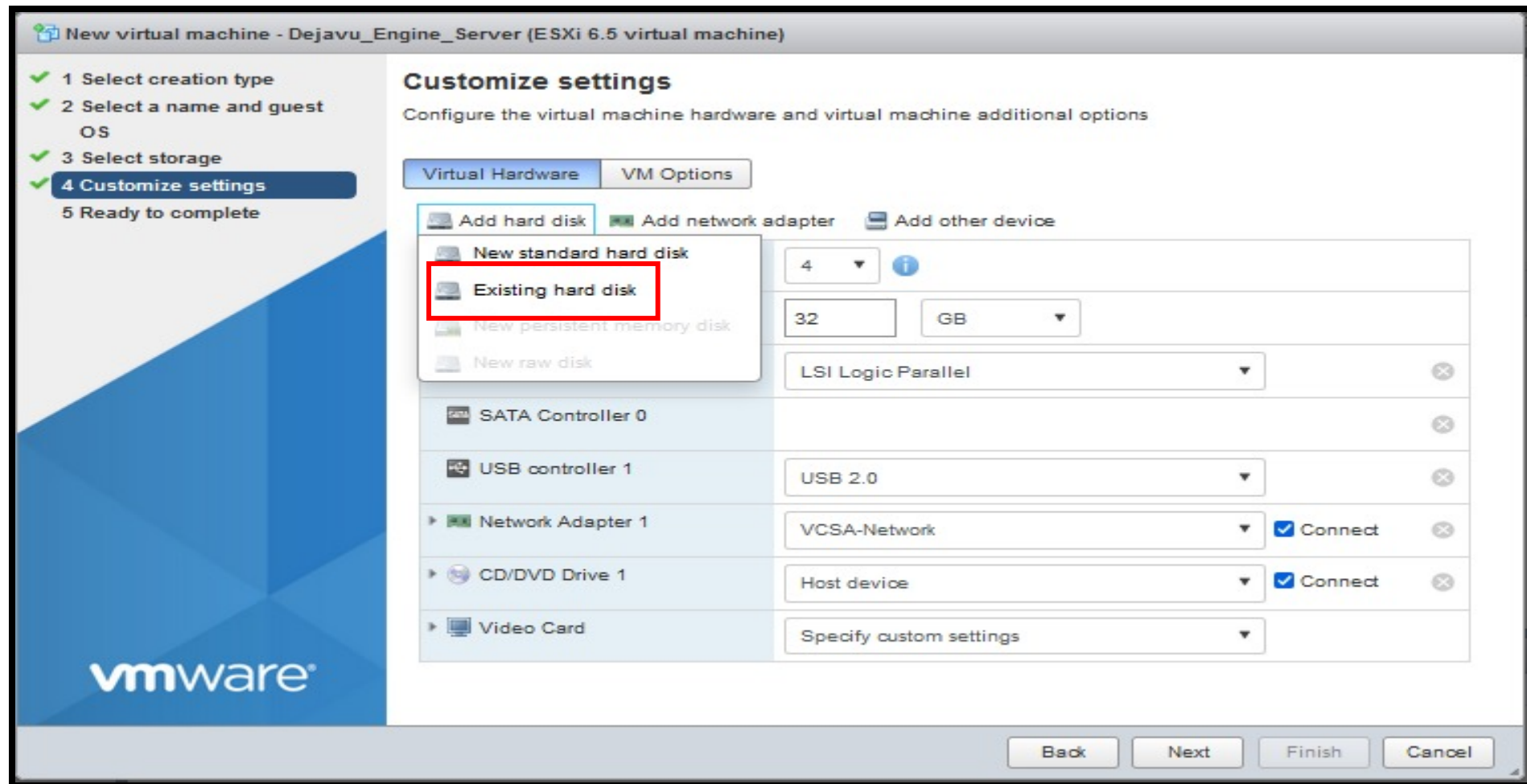
Note : Delete the exiting hard disk and attach that VMDK as a hard disk



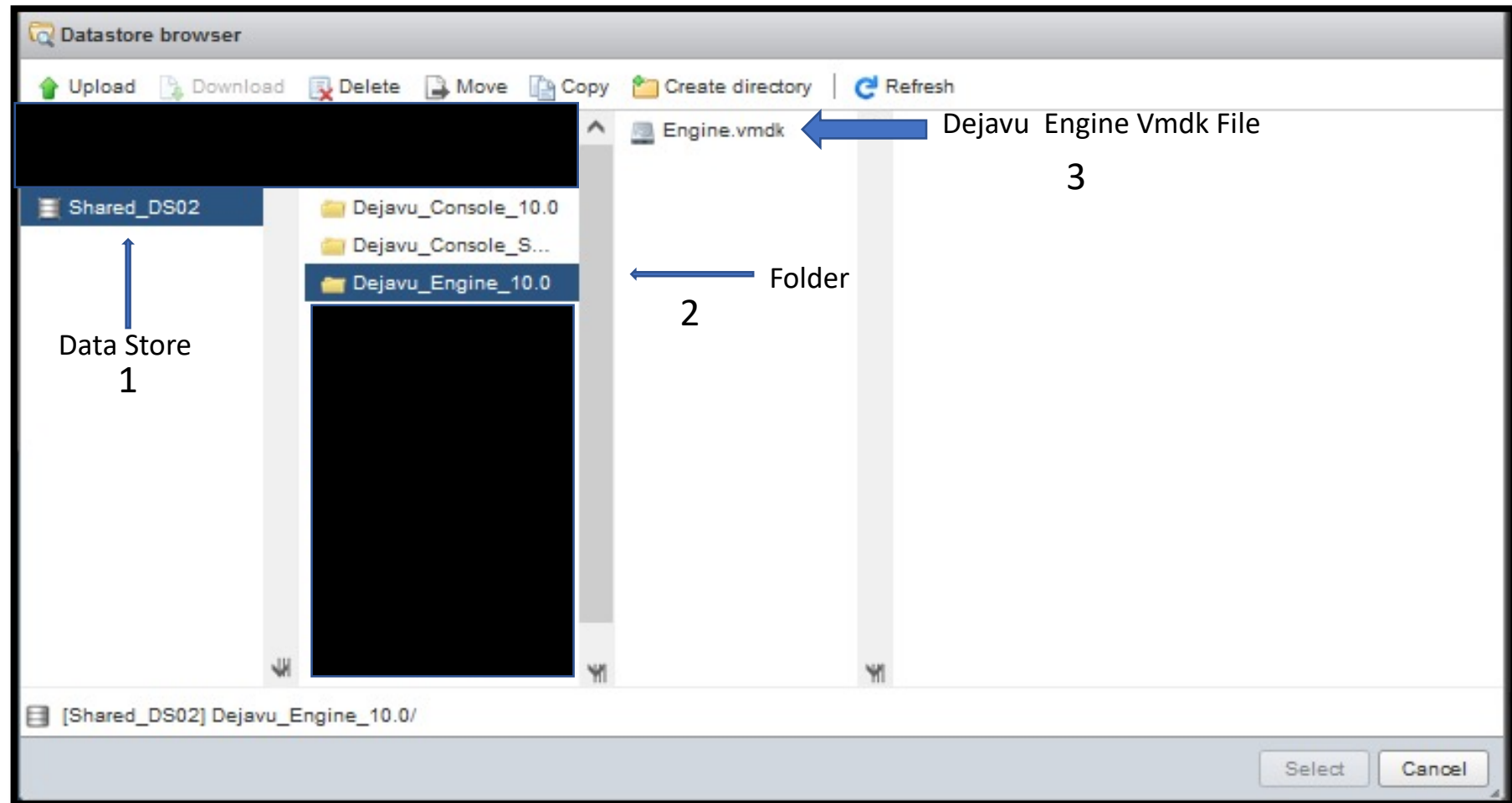
To add hard Disk, click on **“Add hard disk”**



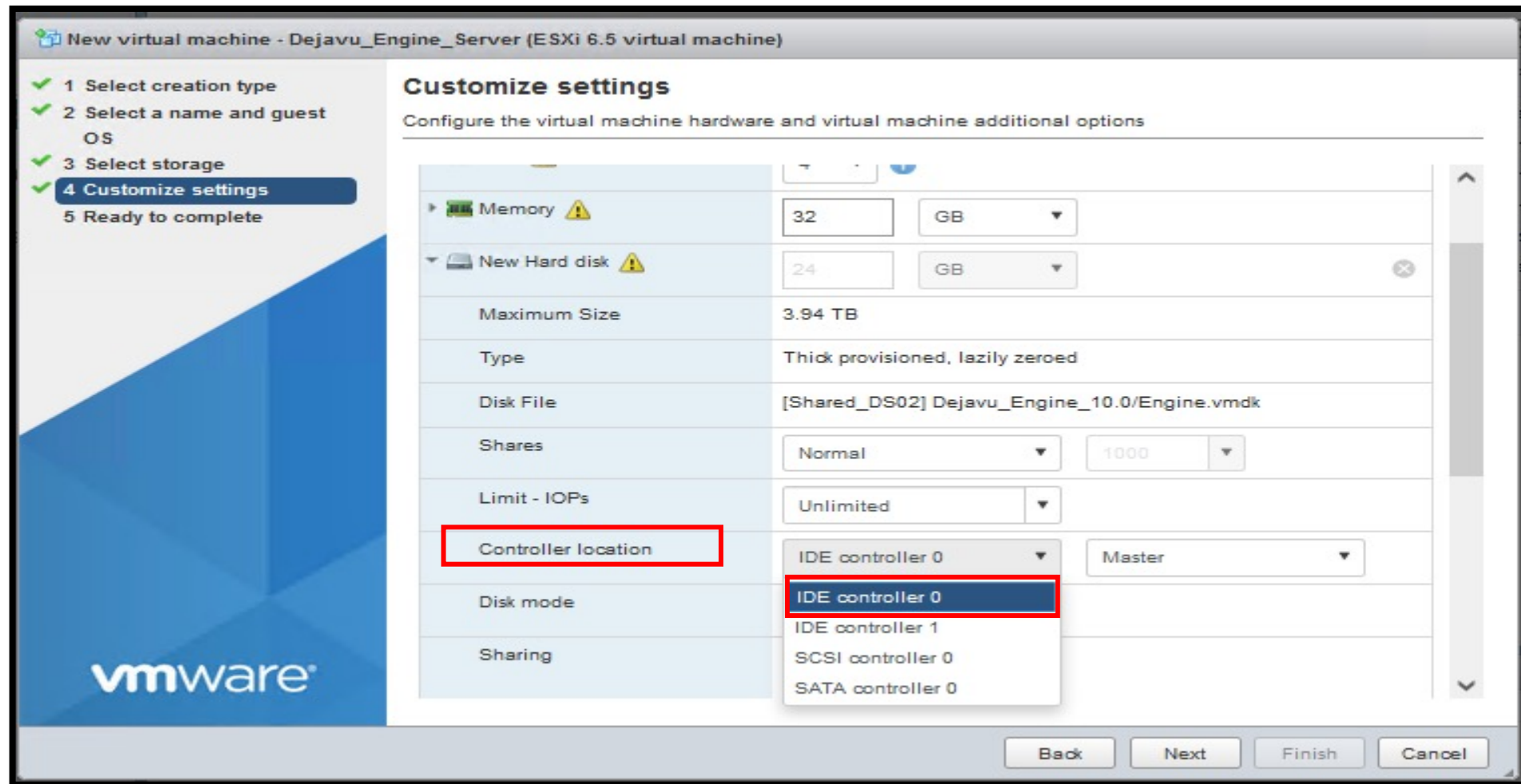
After you click on Add hard disk, select **“Existing hard disk”**



Once you Click on **Existing hard disk**, go to the datastore where you have uploaded that **DejaVu Engine** VMDK file & select the VMDK File

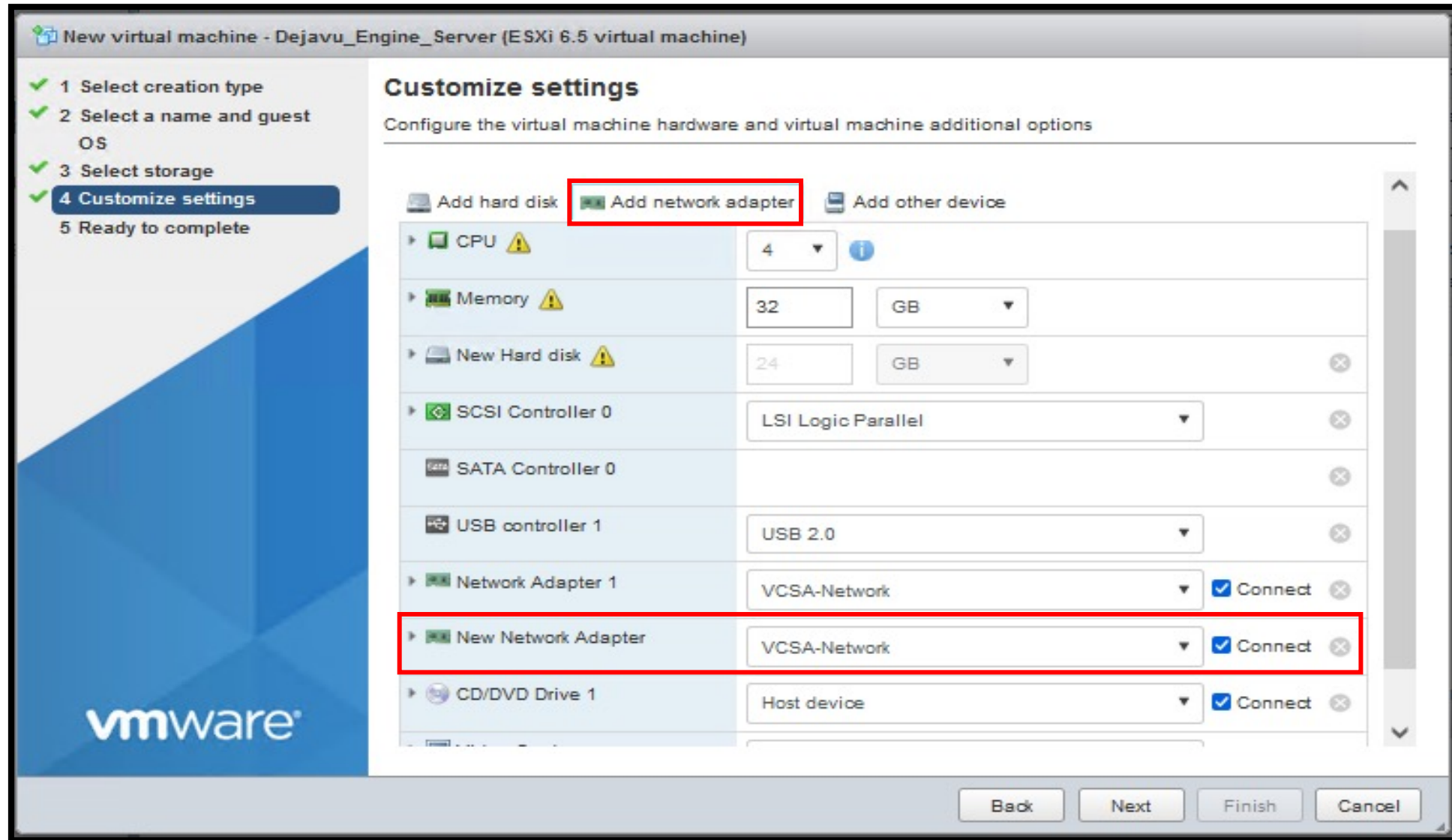


Now, go to the controller location and select the “IDE Controller 0” instead of “SCSI controller 0”



Two network cards are required for the Dejavu Engine. As shown in the screenshot below, click Add Network Adapter and then add another Network Adapter.

Note : Network Adapter 1 is the default, while Network Adapter 1 is a new one that we've added.



After configuring RAM, CPU and Hard disk Settings, click on **Next**

Note : Remove CD/DVD Drive 1 From Virtual Machine Configuration

New virtual machine - Dejavu_Engine_Server (ESXi 6.5 virtual machine)

- 1 Select creation type
- 2 Select a name and guest OS
- 3 Select storage
- 4 Customize settings**
- 5 Ready to complete

Customize settings

Configure the virtual machine hardware and virtual machine additional options

Add hard disk

Add network adapter

Add other device

CPU	4		
Memory	32	GB	
New Hard disk	24	GB	
SCSI Controller 0	LSI Logic Parallel		
SATA Controller 0			
USB controller 1	USB 2.0		
Network Adapter 1	VCSA-Network	<input checked="" type="checkbox"/> Connect	
New Network Adapter	VCSA-Network	<input checked="" type="checkbox"/> Connect	
Video Card	Specify custom settings		

Back

Next

Finish

Cancel

Virtual machine Configuration is done, click Finish. Power on the Virtual machine and DejaVu Engine should be running.

New virtual machine - Dejavu_Engine_Server (ESXi 6.5 virtual machine)

- ✓ 1 Select creation type
- ✓ 2 Select a name and guest OS
- ✓ 3 Select storage
- ✓ 4 Customize settings
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Name	Dejavu_Engine_Server
Datastore	Shared_DS02
Guest OS name	Other (64-bit)
Compatibility	ESXi 6.5 virtual machine
vCPUs	4
Memory	32 GB
Network adapters	2
Network adapter 1 network	VCSA-Network
Network adapter 1 type	E1000e
Network adapter 2 network	VCSA-Network
Network adapter 2 type	E1000e
IDE controller 0	IDE 0
IDE controller 1	IDE 1
SCSI controller 0	LSI Logic Parallel
SATA controller 0	New SATA controller
Hard disk 1	

Back Next **Finish** Cancel

DejaVu Engine is booting.



```
Dejavu_Engine_Server
[ 1.116597] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
/dev/sda1: clean, 424560/32006144 files, 4863880/127999744 blocks
[ 1.993504] ata31.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x0
[ 1.993799] ata31.00: BMDMA stat 0x24
[ 1.993930] ata31.00: failed command: WRITE DMA
[ 1.994084] ata31.00: cmd ca/00:08:00:08:44/00:00:00:00:00/e0 tag 0 dma 4096
out
[ 1.994084]          res 41/10:08:00:08:44/00:00:00:00:00/e0 Emask 0x81 (inva
lid argument)
[ 1.994444] ata31.00: status: { DRDY ERR }
[ 1.994578] ata31.00: error: { IDNF }
```

If you see this, then we are good.
DejaVu Engine is up.



```
Dejavu_Engine_Server
Debian GNU/Linux 9 DejavuEngine tty1
DejavuEngine login:
```


Dejavu Engine Default IP Address is : 192.168.56.102

Access URL : <https://192.168.56.102>

Default username : Set your username here

Default password is : Set your password here

← → ↻ 🏠 🔒 https://192.168.56.102/Decoify/setupView.php ☆ 📧 📶 ☰

DejaVu | Engine Initial Setup

User Information

🔒

🔒

Configure Management Interface Submit

NOTE: System will reboot to reflect the changes.

Once you enter the credentials, click on “ **Configure Management Interface**” Tab and set up the IP Address reachable by Dejavu Console Server

Don't Click on **Submit** With Out Apply IP Address Settings

DejaVu | Engine Initial Setup

User Information

adimin

••••••••

Configure Management Interface **Submit**

NOTE: System will reboot to reflect the changes.

Server will reboot to reflect the Changes after submitting the information.

Note : DejaVu Engine and Console management IP should be reachable by each other.

Example Of IP address settings

Vyuha Console Server IP Address is: 10.10.0.X

Then, Vyuha Engine Server IP Address should be: 10.10.0.X

DejaVu | Engine Initial Setup

User Information

adimin

.....

Management Interface (vboxnet0/eth0)

10.10.0.251

255.255.252.0

10.10.0.254

Configure Management Interface Submit

NOTE: System will reboot to reflect the changes.

You should be able to access the Engine on the new IP



If you get to this page, Vyuha engine installation is task is completed

DejaVu | Engine

Console Connection

DejaVu Console ()

Sign Out

Admin

Online

MAIN NAVIGATION

Decoy Management

Manage Decoys

Add Server Decoy

Add Client Decoy

N/W and File Managment

Breadbcrumbs

Settings

New Server Decoy

Home > Decoy Management > Add Server Decoys

New Decoy

Physical Interface

eth1

Decoy Name

DecoyName

Network Location

IT

Decoy Type

Internal Decoy

For Engine to authenticate Console, copy the Auth Key from the **Console** and use this key in Engine to establish connection.

The screenshot shows the DejaVu Console interface. The browser address bar displays `https://10.10.0.250/Decoify/list-key.php`. The page header includes the DejaVu logo, a hamburger menu, and links for 'Active Attacks (0)' and 'Sign Out'. The left sidebar shows the user 'admin' as 'Online' and a 'MAIN NAVIGATION' menu with 'Key Management', 'Threat Analysis', and 'Settings'. The 'Key Management' menu item is highlighted with a red box. The main content area is titled 'Key Management' and 'Key List', with a breadcrumb trail 'Home > Key Management > Auth key'. It contains a table with one row for the 'Auth Key'.

Name	Value	Update Date	Reset key
Auth Key	95ba37ae5e12ce2c6882f5c38100f2f42e724703dac7aedaa2	2021-07-06 12:11:18	

On Engine, enter “DejaVu Console Server IP”, “Auth Key”

The screenshot shows a web browser window with the URL `https://10.10.0.251/Decoify/cloudSettings.php#api-connection-check`. The interface has a sidebar on the left with a 'MAIN NAVIGATION' menu. The 'Settings' option is selected, and its sub-menu 'Connection & Logging' is highlighted with a red rectangle. The main content area is titled 'API Connection Check' and displays a red error message: 'API Connection Failed! Check API KEY and ensure connection to DejaVu Console!'. Below this message is a 'Test Connection' button. The next section is 'Update API Key', which contains a text input field with the value '95ba37ae5e12ce2c6882f5c38100f2f42e724' and an 'Update' button. The final section is 'Update DejaVu Console IP', which is highlighted with a red rectangle. It contains a text input field with the value '10.10.0.250' and an 'Update' button. A blue double-headed arrow points from the text 'IP Address OF DejaVu Console Server' to the 'Update' button in this section.

MAIN NAVIGATION

- Decoy Management
- N/W and File Managment
- Breadbcrumbs
- Settings**
 - Device Settings
 - Connection & Logging**
 - Backup & Upgrade

API Connection Check

API Connection Failed! Check API KEY and ensure connection to DejaVu Console!

Test Connection

Update API Key

95ba37ae5e12ce2c6882f5c38100f2f42e724

Update

Update DejaVu Console IP

10.10.0.250

Update

IP Address OF DejaVu Console Server

If you added correct IP Address and Auth key, then connection will be established.

Click on “ **Test Connection**” and you will Get "**API Connection Successful**"

The screenshot displays the DejaVu | Engine web interface. The browser's address bar shows the URL `https://10.10.0.251/Decoify/cloudSettings.php?key=success`. The top navigation bar includes a hamburger menu, a status indicator for 'Console Connection' (a green dot), 'DejaVu Console (0)', and a 'Sign Out' link. The left sidebar, under the 'Admin' profile (Online), lists navigation options: Decoy Management, N/W and File Management, Breadbcrumbs, and Settings (selected). The main content area is titled 'Dashboard Connection & Logging'. It features three sections: 1. 'API Connection Check' with a green status message 'API Connection Successful' and a blue 'Test Connection' button. 2. 'Update API Key' with a text input field containing 'DejaVu Console API Key' and an 'Update' button. 3. 'Update DejaVu Console IP' with a text input field containing '10.10.0.250' and an 'Update' button. Red dashed boxes highlight the 'Console Connection' status and the 'API Connection Successful' message with its 'Test Connection' button.