

VMWORLD 2007



HANDS-ON LABS

Using VMware Virtual Desktop Infrastructure for Hosted Computing

September 10-13, 2007

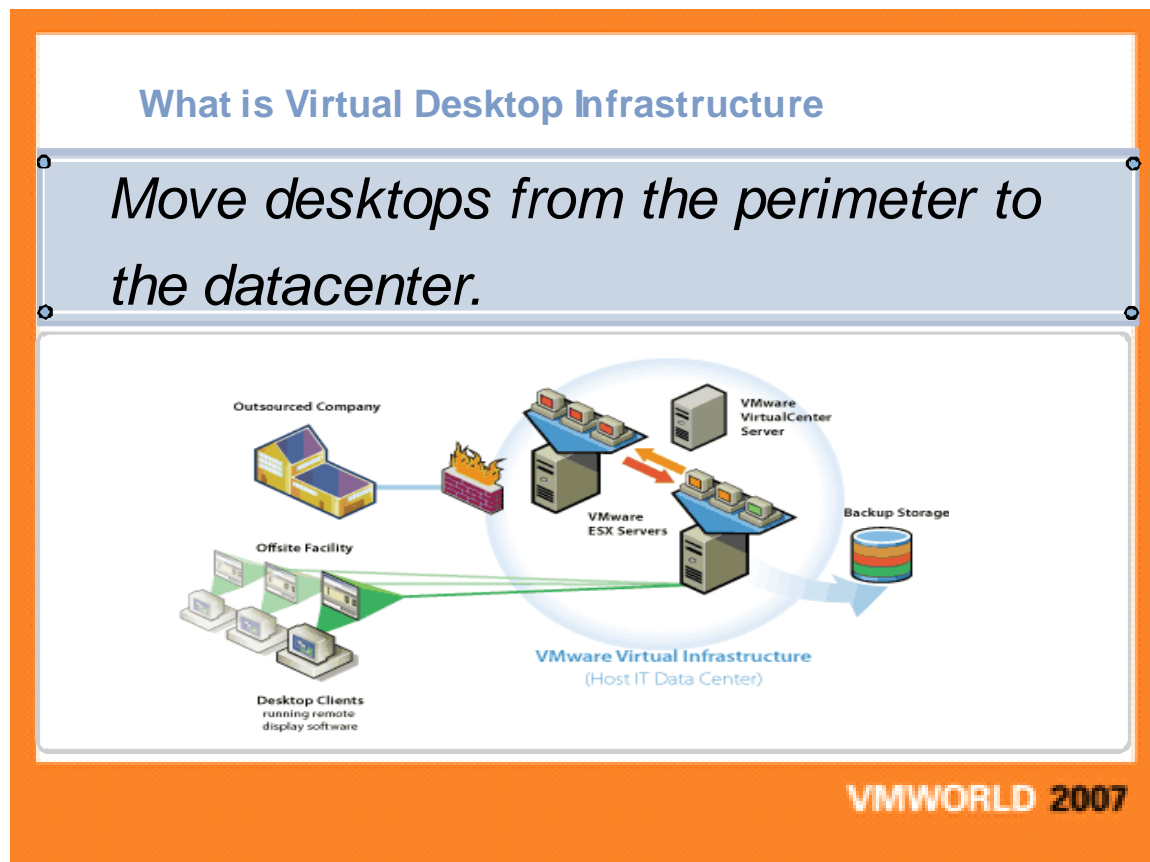
Contents

VMware VDI: Practical Applications.....	1
So why do it?	3
Simple Brokering - the process of simple connection brokering:.....	6
Tunneled Brokering:	7
The Citrix broker is similar to tunneled brokering.	8
Multi-monitor Support:	9
Printing solutions	10
Hardware based redirection.....	11
Software based redirection	12
TCO calculation	19
VMware VDM 2.0 Installation Procedure	22
The VDM 2.0 Administration Interface	30
Global Settings	35
Administrators.....	36
VDM Servers	37
Adding A Static Desktop	38
Non-persistent pools.....	48
Persistent pools	59
Installing the VDM 2.0 client	70
Connecting to a Desktop.....	74
The VMware VDM 2.0 Architecture.....	76
Using Entitlements within VDM 2.0 Connection Broker	81
Appendix.....	89
Miscellaneous Information	95

Instructors:

- Arvind Rayasam, Technical Alliance Manager
- Alexander Thoma, Sr. Consultant
- Chris Duffy, Sr. Consultant
- Michael Burnett, Staff Systems Engineer
- Nicholas Gibson, Consulting Architect
- Ian Gibbs, MTS, Platforms
- Tommy Armstrong, Product Marketing Manager

VMware VDI: Practical Applications

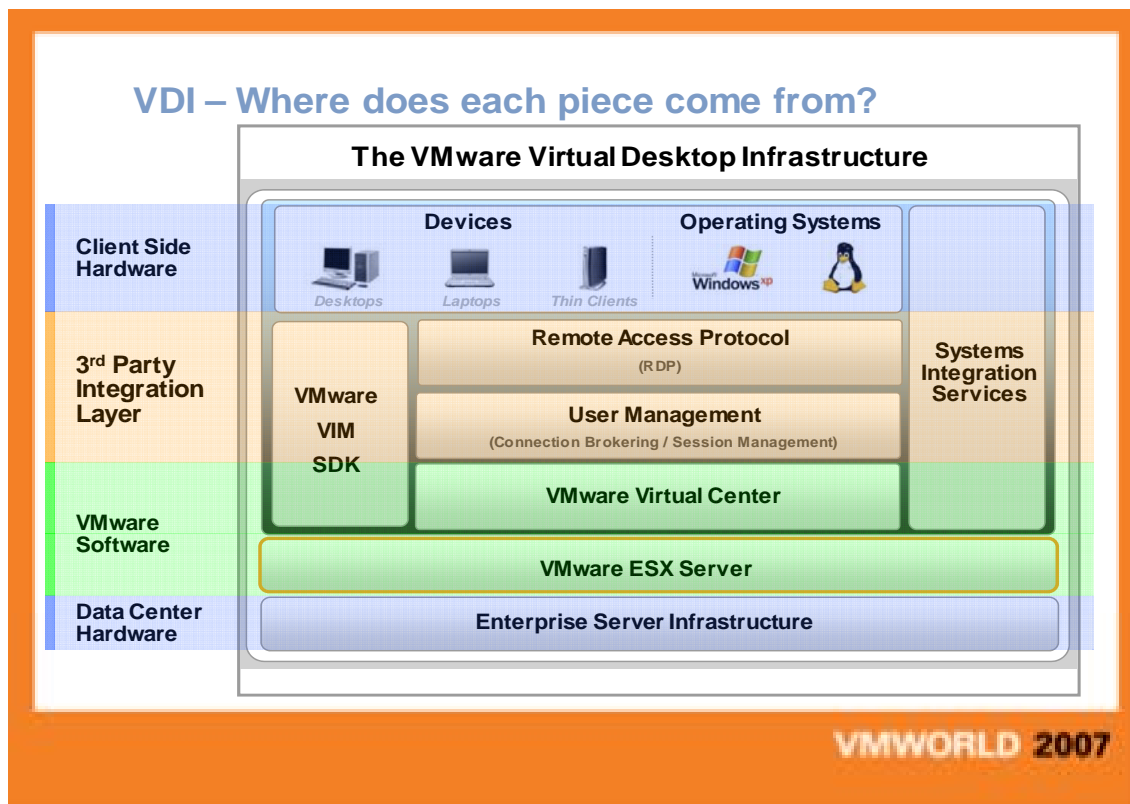


VDI is an extension of a very old concept in computing, centralization. The primary objective of VDI is to reduce complexity and gain better control over corporate desktops. This is principally achieved by moving desktops from the corporate perimeter to a controlled environment such as a datacenter.

Let's take a look at the challenges of a modern end user device, such as a dual-core desktop used mainly to perform data entry.

1. They break and are hard (and time consuming) to fix
2. Require considerable support time and advanced training
3. Need to be left on and connected to the corporation to be patched (OS, virus DAT files, software updates, etc) and backed up
4. Need to be secured against IP theft (physical device theft is cheap compared to the cost to the organization of data theft).

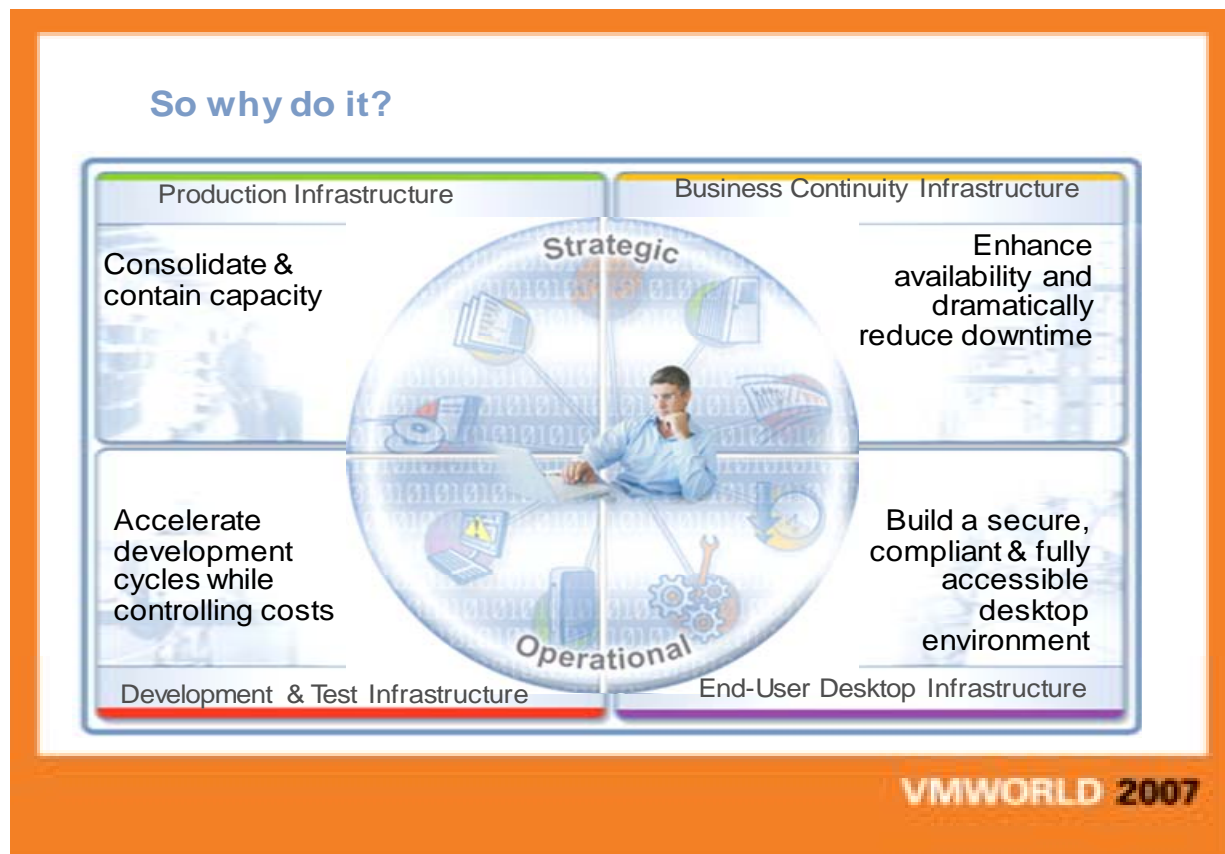
These challenges result in increased costs, and therefore an increased total cost of ownership.



As just mentioned VDI is not a product it's actually a solution. This solution consists of multiple layers that work together to provide an end user with a desktop like experience. The above slide lists all of the various segments that make up an end-to-end VDI solution.

When looking at the overall VDI stack there is a very important fact to keep in mind. The end goal of VDI is to implement a simple, cost-effective solution that mimics a standard desktop environment. It is very possible to add so many elements to the VDI stack that the solution is no longer cost-effective and actually increases the support burden on IT. As customers and partners explore the options surrounding the overall VDI solution they must keep in mind:

- What type of experience their end users will be satisfied with?
- What type of cost and support burden will this experience levy on the IT staff?



So why do it?

In addition to all the benefits achieved by VMware Virtual Infrastructure (see above slide), the implementation of VMware as VDI solution offers some very interesting value propositions to organizations of any size.

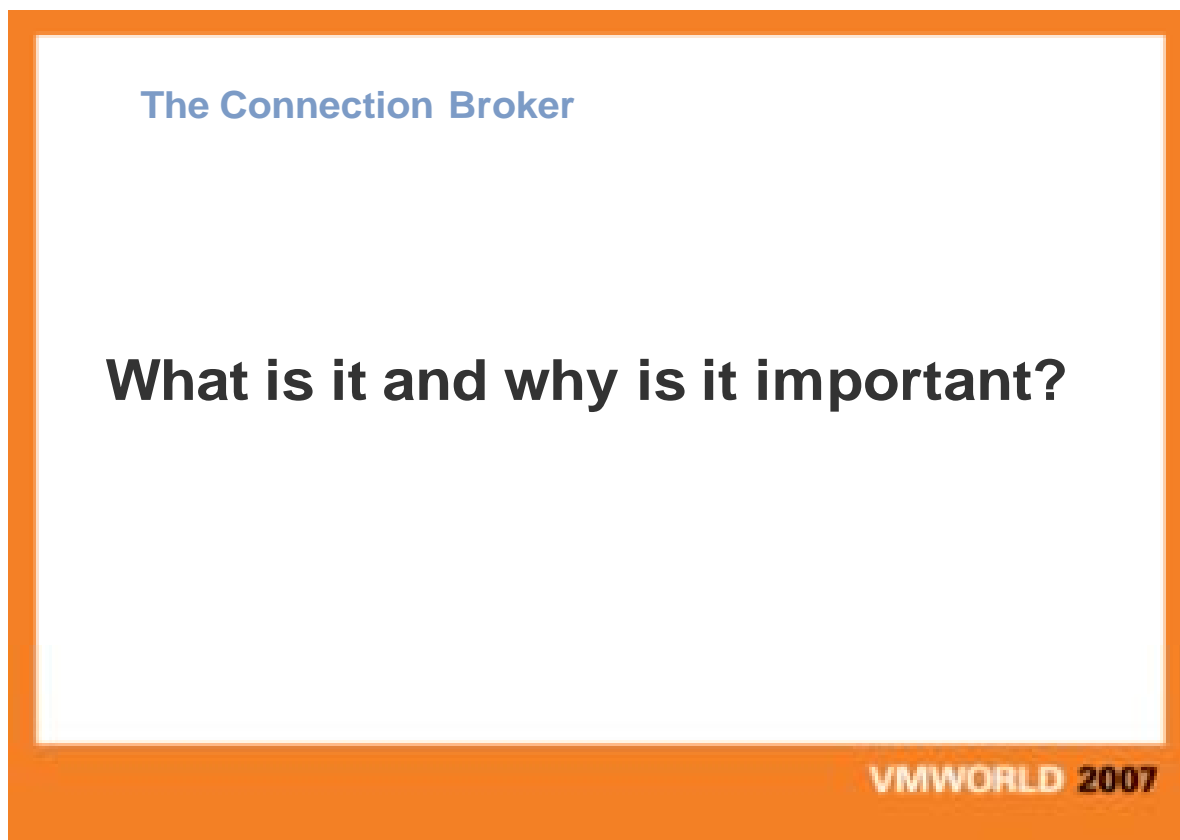
Hardware independent desktop environments. Software developers can accelerate development by concentrating on features and functionality rather than having to worry about supporting an almost infinite variety of hardware devices

Better resource utilization. By leveraging ESX technology, large consolidation ratios of virtual machines are achieved reducing both cost and complexity

Performance and availability. End user operating environments are no longer on physical machines which are subject to downtime. Operating environments will be more available and more flexible, greatly reducing machine and productivity unavailability

Streamlined deployments. It is now possible for IT administrators to rapidly clone and provision new virtual machines in a fraction of the time it takes to provision of physical machines

Improved data protection. Operating systems, applications, and more importantly data are no longer located in insecure locations. Thereby allowing use desktops to have the ability to operate under the same stringent rules and regulations as server based operating environments



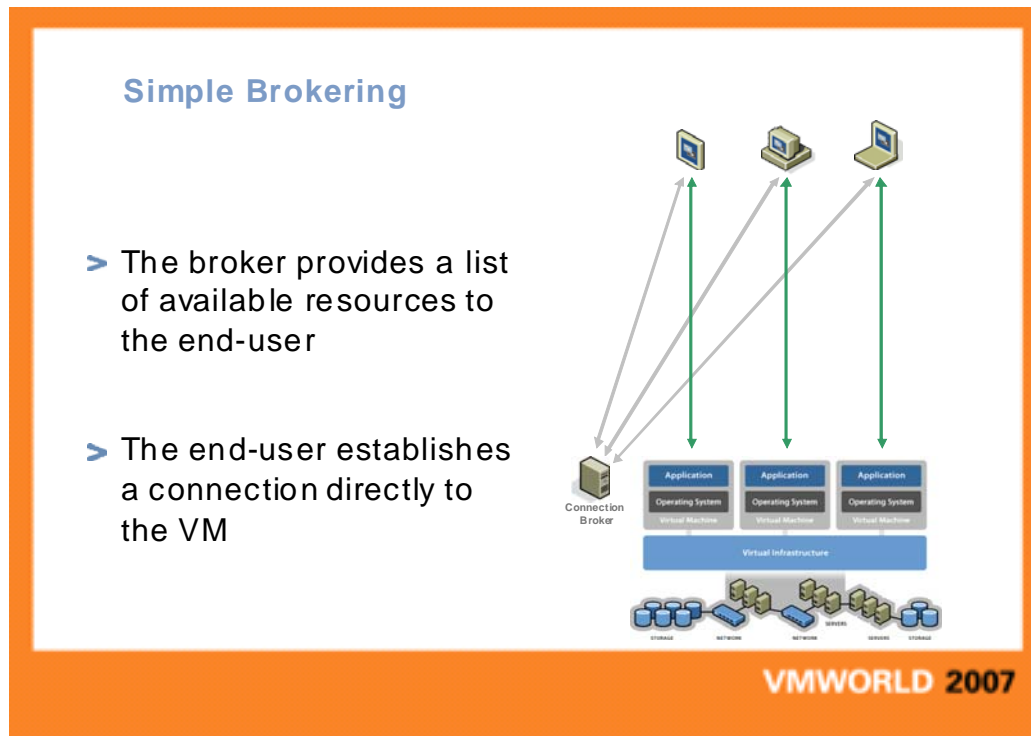
The connection broker is arguably the most critical piece in any VDI solution. Why? Let's suppose we're at a small customer environment. During our initial conversations with this customer we find out he has approximately 10 employees that are concentrated in one geographic location. With this simple type of setup it can be very easy for IT administrators to individually assigning each employee a virtual machine and have that employee access that virtual machine through an IP address or machine name. Although cumbersome the operation can be easily managed by one IT administrator.

Now suppose we visit a customer who has 5000 employees scattered all across the globe. In this scenario it becomes impractical to hand each employee and IP address for machine name to access their virtual machine. Doing so could result in problems such as machine conflicts, individuals attempting to contact machines that are down, dropped connections, resource constraints, etc. In this scenario a connection broker would fill the gap and manage all of the inbound connections to the virtual machine infrastructure on

the back end. If a connection was dropped the connection broker would re-establish it. If virtual machines were unavailable the connection broker would automatically clone one.



Brokering a connection is not easy. Because of this different connection broker vendors have taken different routes to address the challenges. While the features of different vendor's brokers will vary, the overall process is the same.

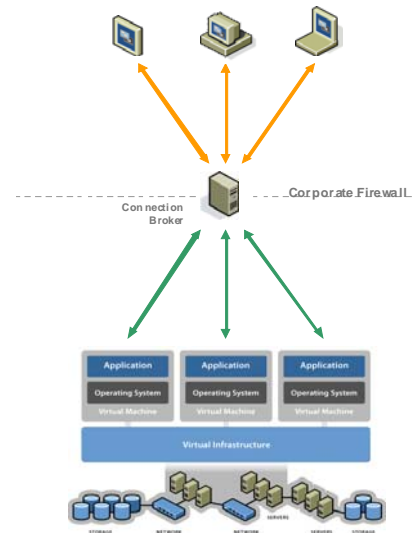


Simple Brokering - the process of simple connection brokering:

- An end user contacts the connection broker through a URL given to him by his IT administrators
- This URL forces the end user to log in and checks that user's credentials against a back end authentication mechanism such as active directory
- Once the user's credentials and role has been verified and he is brought to a page which lists all of the virtual machines to which she has access
- The end user clicks on the link, the broker establishes the connection with the virtual machine, and then the broker steps out of the way
- The broker will on occasion check the connection between the end client and the backend virtual machine to make sure that everything is working as expected

Tunneled Brokering

- The connection broker links the end-user via an encrypted tunnel to the VM
- > The encrypted tunnel is a mini-VPN component designed to route only RDP traffic



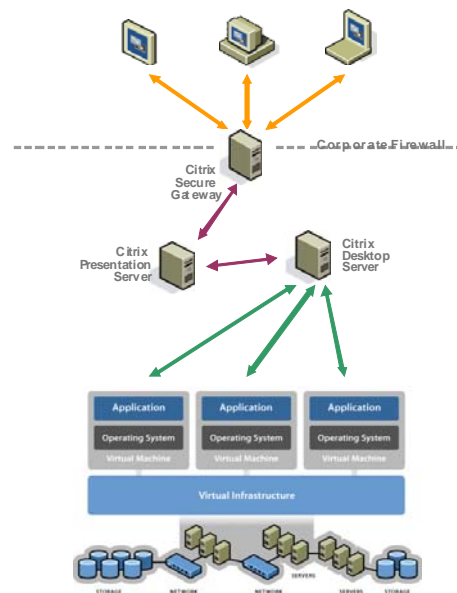
VMWORLD 2007

Tunneled Brokering:

Tunneled brokering is similar, except the broker acts as a proxy for all connections. All traffic from the end users to their respective virtual machines goes through the broker. Picture it like an SSL gateway. The broker and the proxy piece would mostly likely be on separate machines so as to not have the broker in an untrusted network.

Joint Citrix Implementation

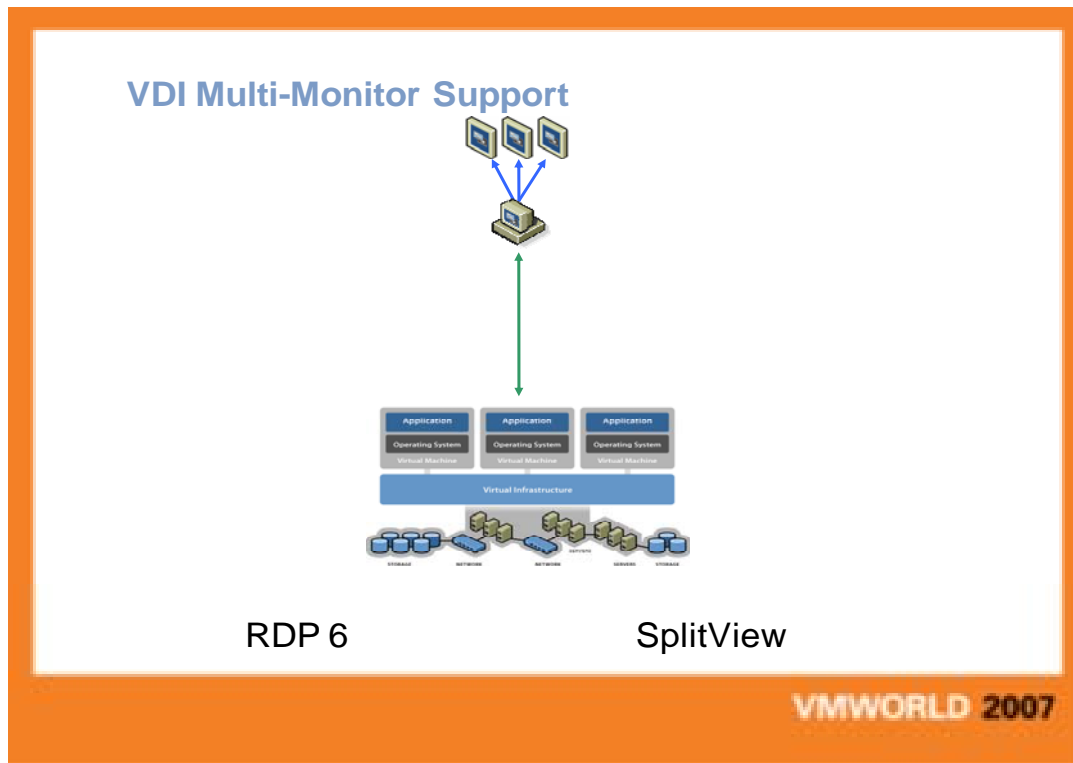
- > Remote desktops are treated the same as published applications
- > Citrix talks to VMware over RDP
- > Citrix talks to the end clients over ICA



VMWORLD 2007

The Citrix broker is similar to tunneled brokering.

- The Citrix Secure Gateway acts as the proxy to encrypt/decrypt the connection
- Clients use Citrix ICA Protocol to talk to the Citrix Presentation Server
- The Citrix Desktop Server acts as a Connection Broker
- The Citrix Presentation Server talks to VMware over RDP

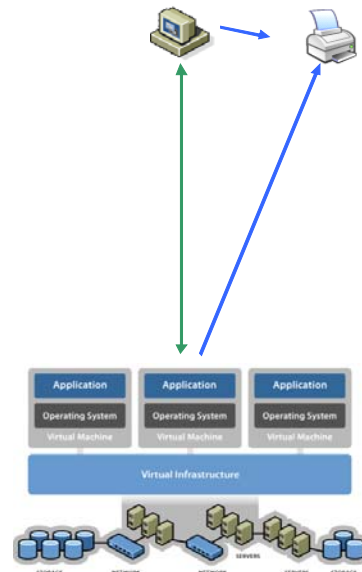


Multi-monitor Support:

One of the most requested features for a "true" desktop experience is the ability to span multiple monitors. VDI addresses this requirement by working with various partners to fill the gap. Connection broker vendors paired with other third party vendors such as [SplitView](#) address the requirement of multiple monitors. Each solution provides a different type of experience at a different cost.

VDI Printing

- > Network Printers
- > Local Printers via RDP
- > Local Printers via local client software
- > PDF Printing

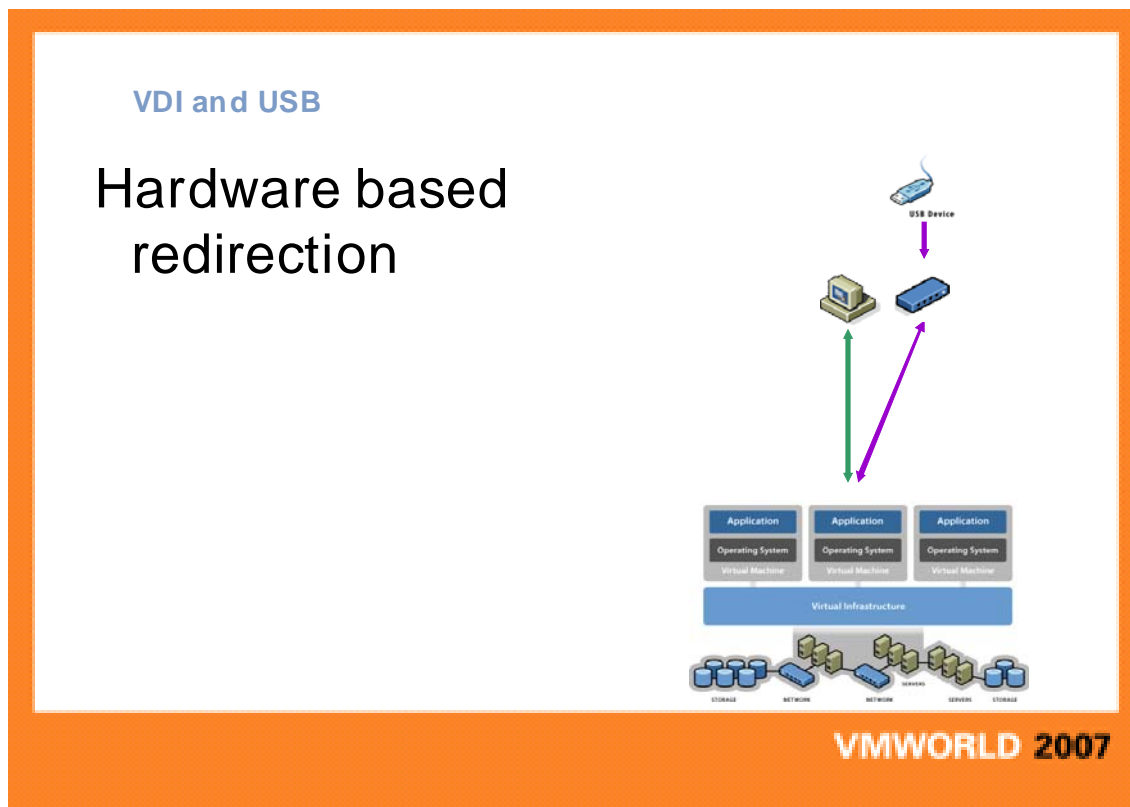


VMWORLD 2007

Printing solutions

Another important requirement for VDI on the endpoint is “endpoint printing”. There are numerous solutions available in the market place that will allow IT departments to enable remote printing.

- The simplest solution is to put virtual machines on a domain and use network attached printers (works with thin clients)
- You can also use local printers via the features inherent in your RDP client (works with thin clients)
- Universal print drivers that communicate back to locally installed client software (may not work with thin clients)
- Users can print to a pdf that they can later access via web browser for final printing

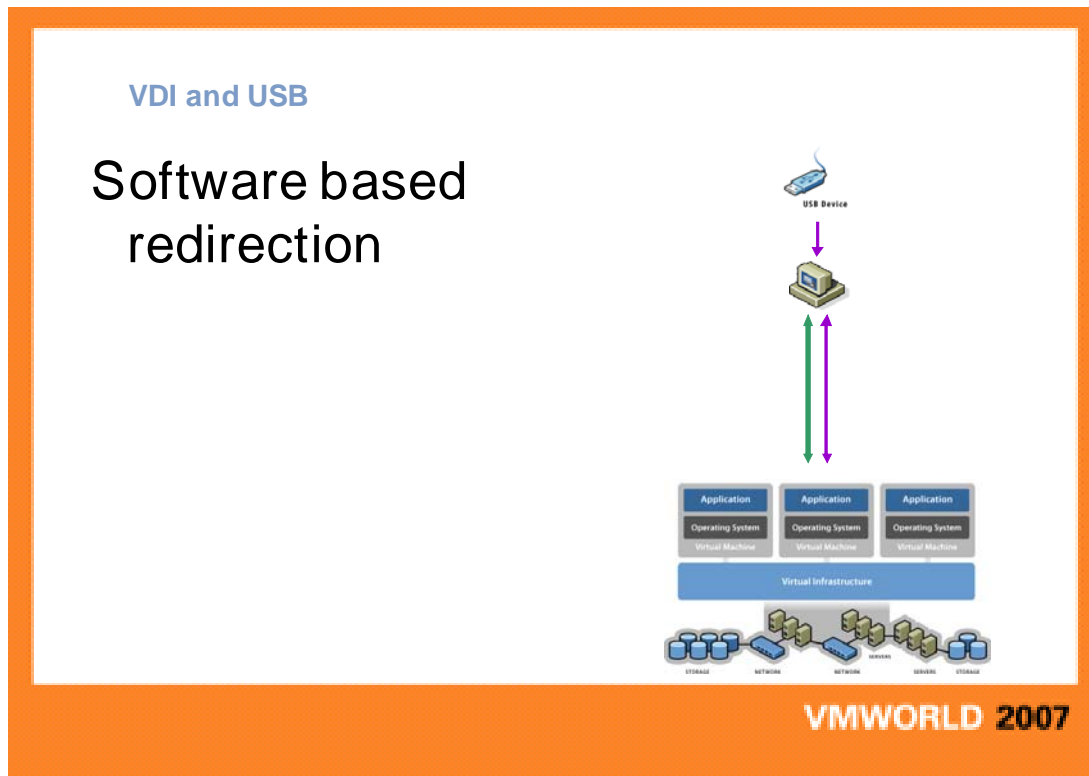


Hardware based redirection

Two methods of USB are available – Hardware and software.

Let's look at hardware based redirection first:

- A hardware USB-over-Ethernet device is located near the endpoint
- Users attach USB devices to the hardware device for redirection
- A client component is installed inside the Virtual Machine
- The client connects a port on the hardware device to the VM which makes it appear to be directly connected



Software based redirection

Next we have software based redirection:

- The connection between the client and the server looks like a direct attached device
- The client initiates the connection to the server component on the thin terminal or client device. A software server component is installed on the end-point and a client component is installed inside the Virtual Machine. Users attach USB devices to the local machine for redirection. The client/server components connect the VM to the user's terminal.

Systems Management

- ☐ Patching?
- ☐ Inventory?
- ☐ Provisioning?
- ☐ ITIL ?
- ☐ Security?
- ☐ Backup?



VMWORLD 2007

So even though VDI does not remove the requirement for systems management. Customers who pursue a VDI strategy will still need to patch, keep track of software inventories, provision, and just basically care for their virtual machines in the same way they did for physical machines. VDI simply makes the process much easier and much faster. It does this by taking those machines from the perimeter and moving them into a controlled data center. Instead of deploying patches and software across a wide area network to an end user that might or might not be on a high speed connection IT administrators can now deploy patches or software across high speed networks to virtual machines.



Unfortunately there's no right answer when a customer asks "what is right for me". Because VDI is a solution and not the product its implementation will vary from one customer to another based on that customers needs, infrastructure, resources, and budget.

Define your business

- **Small Environment (1 ~ 20 clients)**
- **Medium Environments (20 ~ 250 clients)**
- **Large Environments (250+ clients)**

VMWORLD 2007

To get you started there are several key questions that can help point you in the right direction when considering a VDI implementation.

One key question that needs to be answered is: " What is the size of the organization that will be serviced by in this VDI implementation? "

The answer to this question can help determine what type of back and infrastructure is needed. If there are only 15 or 20 employees then having an ESX backend makes no sense. The infrastructure would be far too complicated and costly for this particular use case. In these types of small and medium environments products such as VM server can work just fine. Remember, the ultimate goal of VDI is to provide a solution that removes complexity and cost. VDI's main objective is to simplify and streamline.

As environments and deployments get a larger the value of proposition of ESX becomes more tangible. It is now possible for customers to take full advantage of functions such as a vMotion, DRS, HA, etc. Larger environments also have the necessary resources to implement and maintain an ESX based backend infrastructure.



Another major question that needs to be answered is: "What exactly do you need -- based on available resources, requirements, and future growth?"

In most complex sales it is very difficult to fully understand what an organization may need. In many cases the complexity of the solution, lack of knowledge about all the pieces of your own environment, and sheer scale of the implementation adds a layer of confusion. In these cases it is sometimes helpful to have an outside group come in and help access what you need to get the most value out of a VDI implementation.

A sales team from a partner or VMware is a great resource to help plan a complete solution.

Some questions to ask yourself

- ☐ **Current state of my environment?**
- ☐ **Resources?**
- ☐ **Citrix?**
- ☐ **3rd party solutions?**
- ☐ **Operating systems?**

VMWORLD 2007

Some other key questions to answer before moving forward with a recommended VDI architecture.

- What is the current state of the environment?
- What are the resources at your disposal to implement and maintain this environment?
- What is the role of Citrix in this environment?
- Why is this important? Many customers looking into a VDI solution have tried or are already using Citrix. In case they have implemented Citrix they get free access to the Citrix connection broker. This broker will allow end users to connect to VMware virtual machines through their standard Citrix interface. There is no learning curve and the broker plugs into Presentation Server with minimal work.
- What type of third party solutions are needed to get the end user experience you are looking for? What operating systems do you expect to use now and in the future?

TCO/ROI

TCO/ROI

VMWORLD 2007

VDI TCO Whiteboard

→ 40 users per 2 socket server

➤ ESX Enterprise ~ \$6000/40 users	\$150
➤ Server HW \$8000 to \$12000	\$250
➤ Client HW (if any)	\$200
➤ Microsoft XP or Vista	\$250
➤ Storage per User 10GB \$50 to \$150	<u>\$100</u>
➤ Total Costs per User desktop	\$750 to \$1000 per

VMWORLD 2007

TCO calculation

Rough whiteboard TCO. These numbers are going to differ with each customer but these are typical of what is being seen in the customer base.

Breaking out the fixed costs for a VDI solution we need to look at ESX, the server HW, client HW for a thin client or repurposed PC, Microsoft licensing costs and then backend storage.

We are looking at a collapse ratio of 40 users per 2 socket server. The server HW looks at a 2 socket server with 16GB to 32GB based on the footprint of the virtual desktop to achieve a 40 to 1 consolidation. We have customers who have optimized XP and are running 60 users on a server with 16GB of memory. Once again this will be based on your own individual desktops. I want to take a minute and talk about memory “right sizing”. Yes I think that is a made up term, but what it means is sizing your memory footprint at the correct size based upon need and not building in a large buffer. Start your virtual machine, launch your typical applications, use them for a period of time and look at your memory utilization. You can add in around a 100Mb buffer, but this is typically a correctly sized memory environment instead of saying I need a 1GB memory footprint. If your applications require this you might, but most environments are much smaller. Now we can take a look at the client, your options are to reuse your existing PC or to replace with a thin client or some other device. Thin clients are getting very inexpensive and we have many options around \$200. The Microsoft client license needs to be looked at and if it needs to be purchased should be around 250. The final component is the cost for shared storage. This can range from quite low to relatively high based upon their current SAN architecture. We can look at alternate storage tiers to reduce this component. The numbers above can be tailored above based upon your own infrastructure and costs.

OPEX Savings		
→ Desktop Management	PC	VDI
> User Administration	\$11	\$2
> Hardware Configuration	\$26	\$33
> Hardware Deployment	\$7	\$5
> Software Deployment	\$121	\$6
> Application Management	\$32	\$21
> Backup, Archiving, Recovery	\$7	\$2
> Service Desk	\$239	\$92
> End User Downtime	<u>\$143</u>	<u>\$37</u>
> Total per desktop	\$586	\$196

...provided by Gartner.

Thin client savings			
→	PC	Thin client	Server
➤ Devices	1000	1000	28
➤ Power Rating	~170	~92	~450
➤ Hours per Day	12	12	24
➤ Days per Week	5	5	7
➤ Total Power	10200000	5520000	2116800
➤ Cost per Kwh	<u>.0813</u>	<u>.0813</u>	<u>.0813</u>
➤ Total	\$829260	\$448776 +	\$172095
		=\$620871	
Savings	\$829260 - \$620871 = \$208389		

VMWORLD 2007

This slide takes a look at replacing PCs with thin clients and the power consumption savings even building in the server back end.

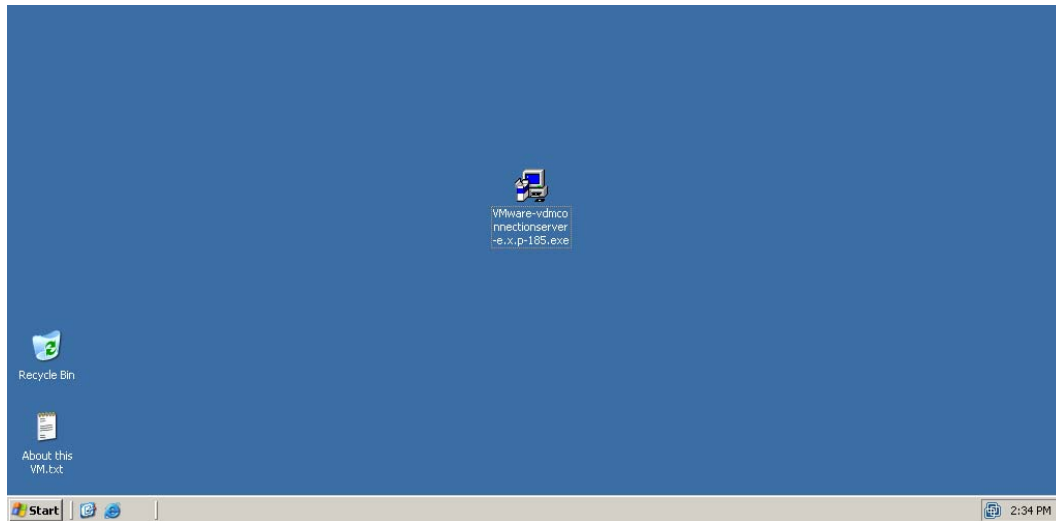
We are looking at 1000 personal computers versus 1000 thin client devices. The power rating we are using includes a standard monitor and can be adjusted per your devices. We are looking at the total time the devices are used and if you use a 24 x 7 number the savings are even more substantial. We calculate the total power used and then the industry average for power. For the VDI solution we also add power for the servers with redundancy built in. We have not captured cooling and storage, but these do not impact the numbers that much more. Add the thin client number plus the server number and you come up with the total cost. Comparing this to the PC only cost you can see substantial savings.

VMware VDM 2.0 Installation Procedure

The following section of the guide will walk you through an installation of the VDM 2.0 connection broker. You will not be carrying out these steps in this lab session.

Step 1:

Log in to the computer which will become the VDM connection server using an account with administrative privileges.



Step 2:

Launch the VDM Connection Broker installer.



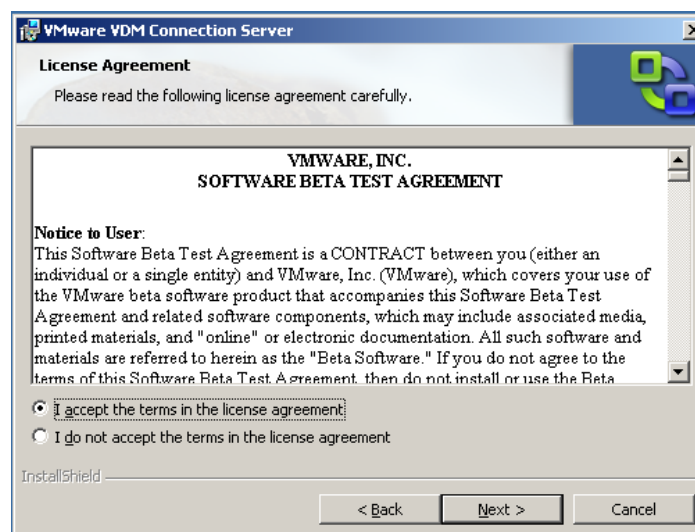
Step 3:

After instructing Windows to run the installer, follow the on-screen prompts, accepting the default settings.



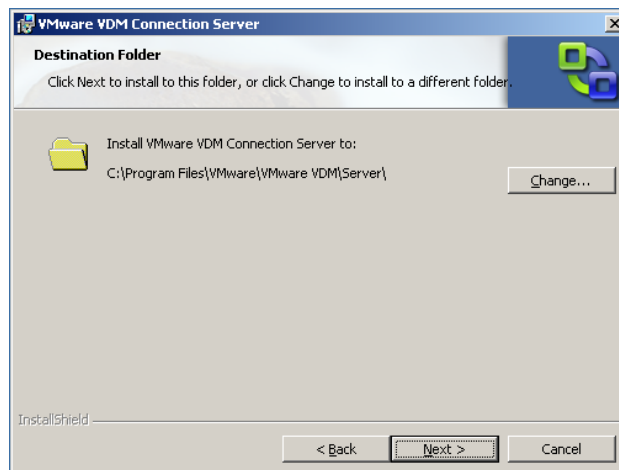
Step 4:

Read and accept the license agreements for VDM and ADAM (see below for further information on ADAM).



Step 5:

Leave the destination folder as the default of *C:\Program Files\VMware\VMware VDM\Server* and continue the install.



Step 6:

Once you select next you will be presented with three installation options; **Standard**, **Replica**, and **Security Server**.

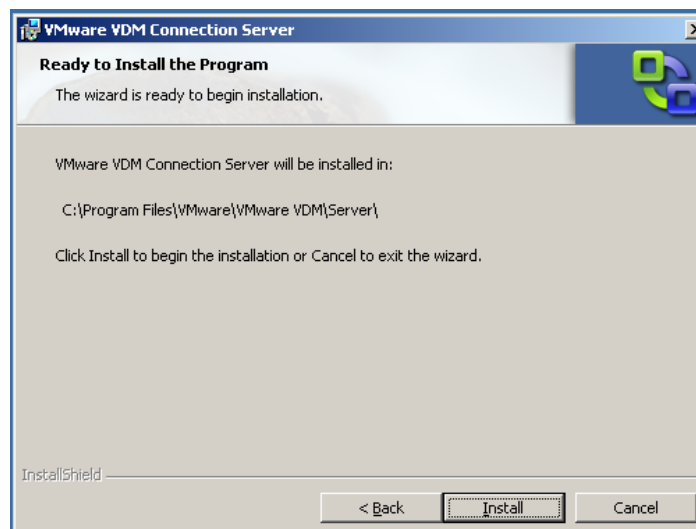
- **Standard:** Performs a full install of a standalone instance of VDM Connection Server or the first instance of a group of VDM Connection Servers.
- **Replica:** This election installs a replica broker that will go on to join another group of VDM servers that all share a common configuration.
- **Security Server:** Performs an install of just the security server components. A security server is located in a DMZ and used to make a VDM installation internet-accessible.

For the purposes of this lab we will be performing a Standard installation of the VDM connection broker.



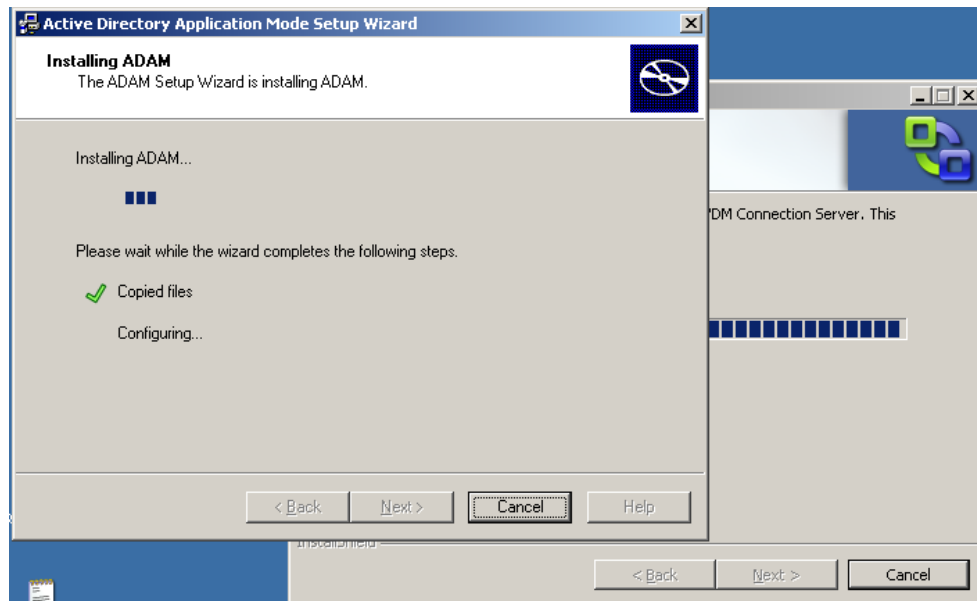
Step 7

Review the summary information presented and select **Install** to begin the installation process. If you would like to make any changes simply hit the **Back** button.



Using VMware Virtual Desktop Infrastructure for Hosted Computing

ADAM will be installed automatically by the VDM installer (see below for further information on ADAM).



The installation of VMware VDM Connection Server has successfully completed. You are now able to click Finish to exit the installation wizard.



ADAM is installed with the Connection Server. ADAM is a freely-distributed LDAP-compatible service released by Microsoft that is a requirement for proper functionality of VDM. For more information on how ADAM is used by VDM, refer to the “architecture and design” section of the lab manual.

ADAM can be configured through a standard set of tools installed on the server. For more information about ADAM including information on how to configure the ADAM server visit the links below.

<http://redmondmag.com/columns/article.asp?EditorialID=592>

<http://www.microsoft.com/windowsserver2003/adam/default.mspx>

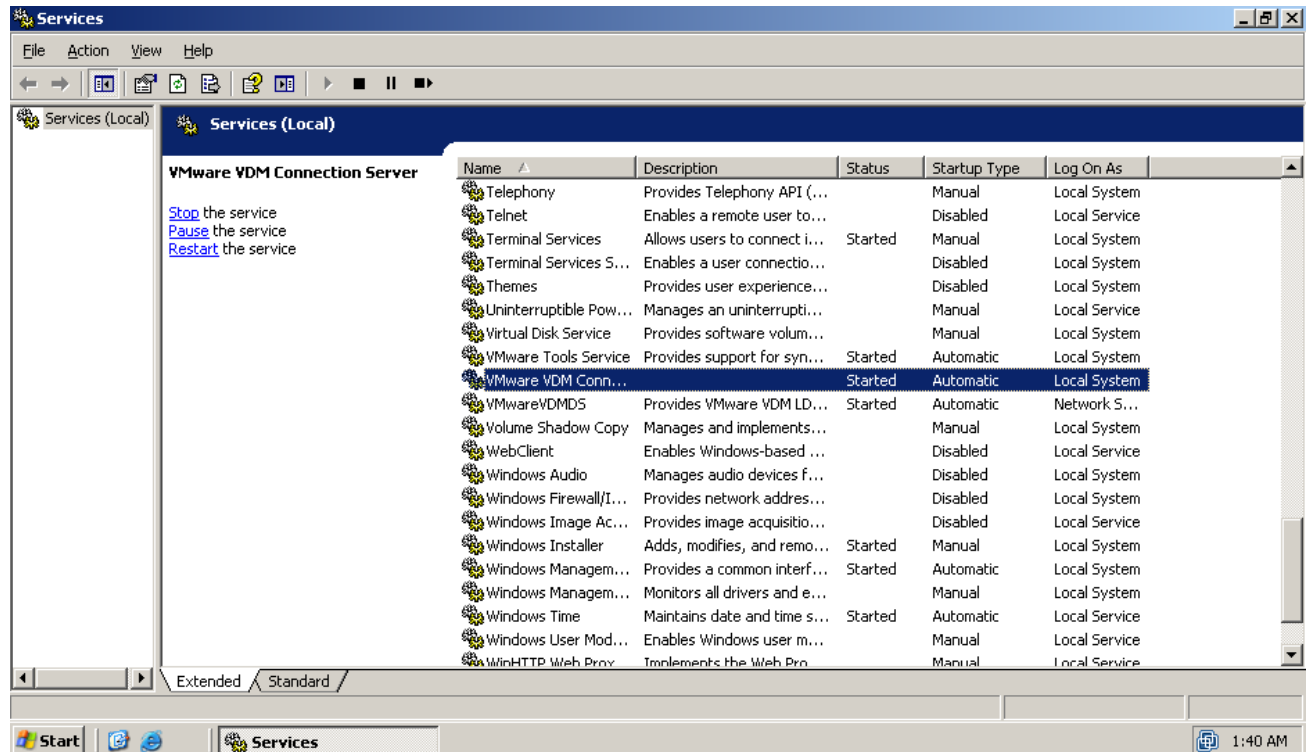


Using VMware Virtual Desktop Infrastructure for Hosted Computing

To confirm that the VDM server installed correctly, check the service control manager for the following two services and confirm their status is as follows;

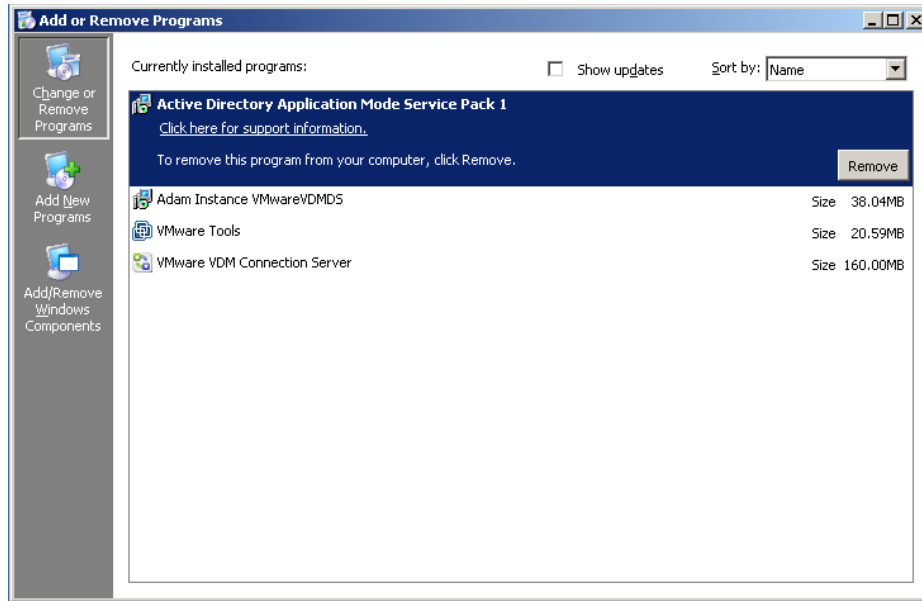
VMware VDM Connection Server
VMwareVDMDS

Started Automatic
Started Automatic

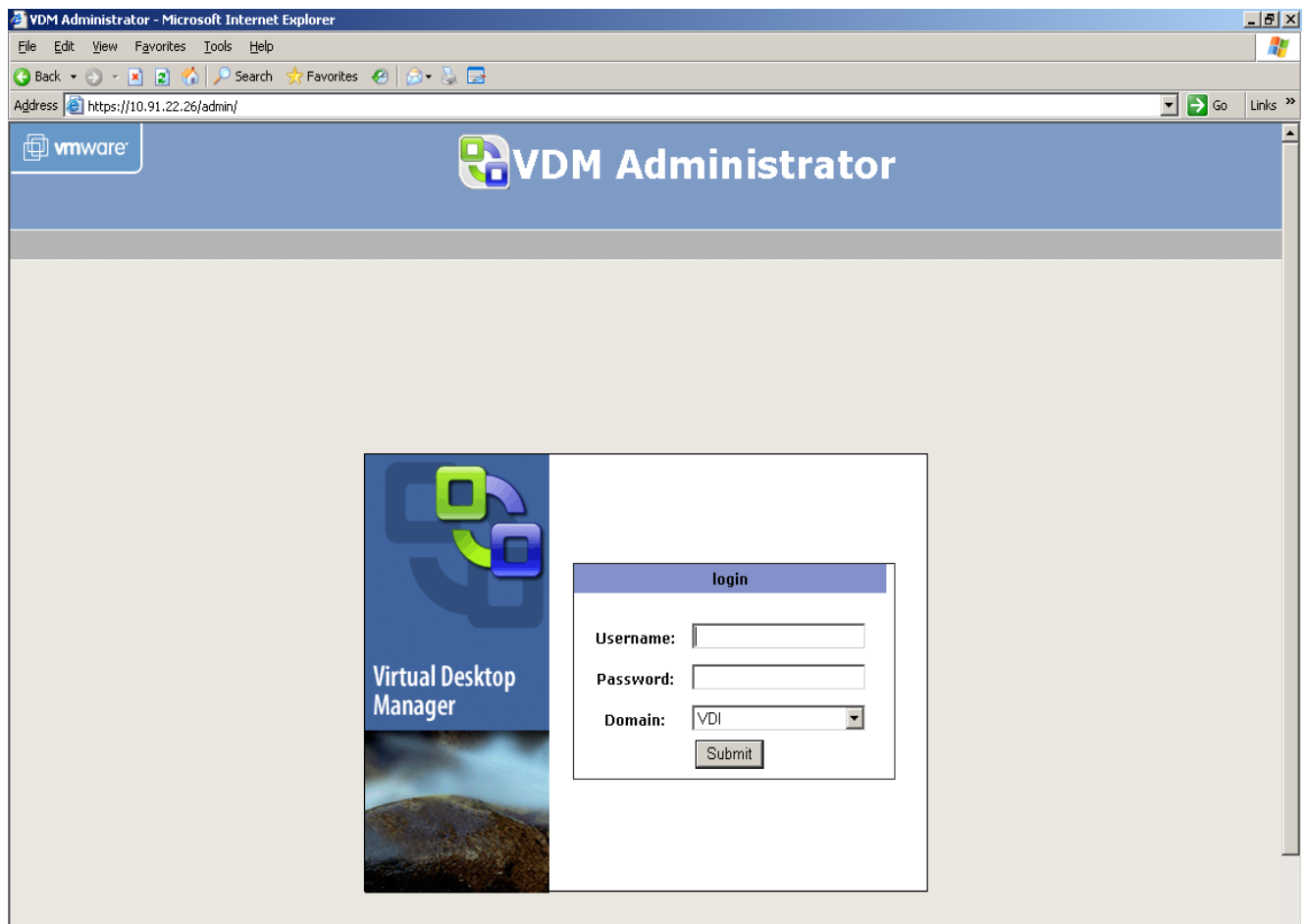


Opening the **Add or Remove Programs** applet from the Control Panel, you should see the following new entries listed:

Active Directory Application Mode Service Pack 1
Adam Instance VMware/VDMDS
VMware VDM Connection Server



The VDM 2.0 Administration Interface



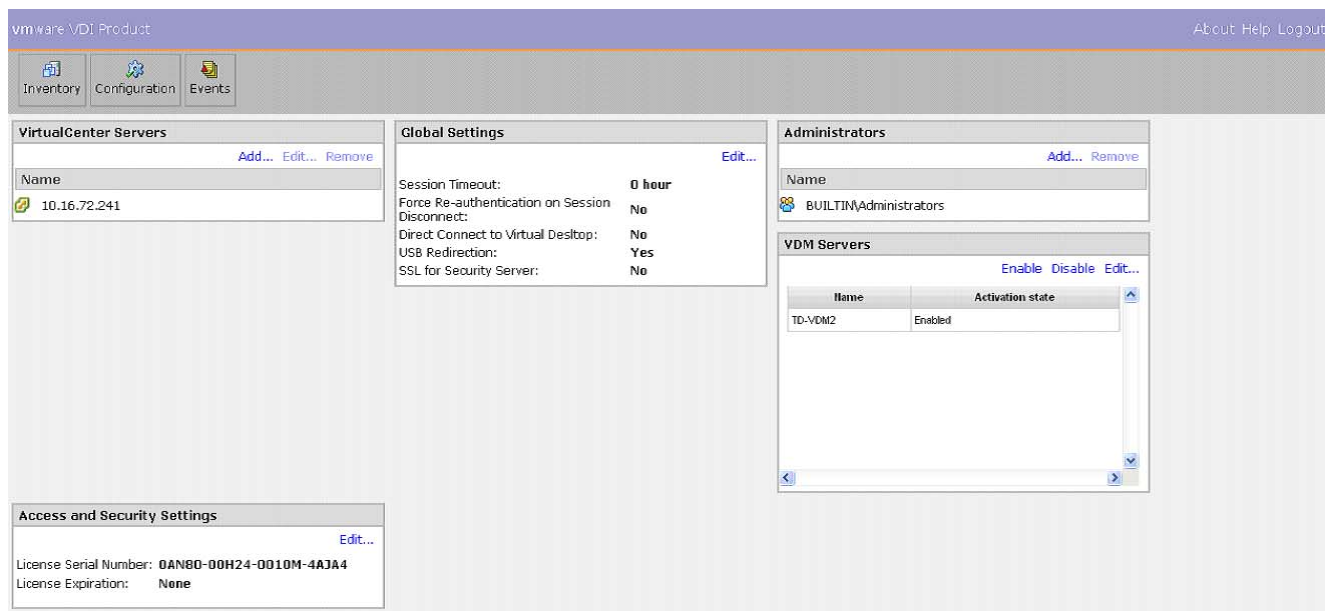
To access and login to the VDM Connection Server Administrator UI, open Internet Explorer 6 or 7, or Firefox; enter the URL

<https://<connection-server-fqdn>/admin>

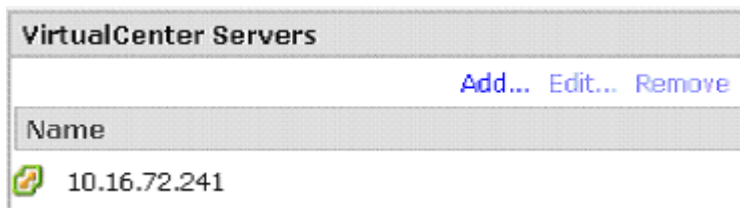
where <connection-server-fqdn> is the fully-qualified DNS name of the connection server (which you have just installed). The SSL certificate provided with the connections server is not signed by a well-known CA, so your browser will prompt you with a security warning which you should ignore. VDM gives you with the ability to provide a proper certificate matched to your server's name, which will resolve this warning. You can also connect using an IP address, but this will result in a security warning that cannot be resolved with a correct certificate.

Using VMware Virtual Desktop Infrastructure for Hosted Computing

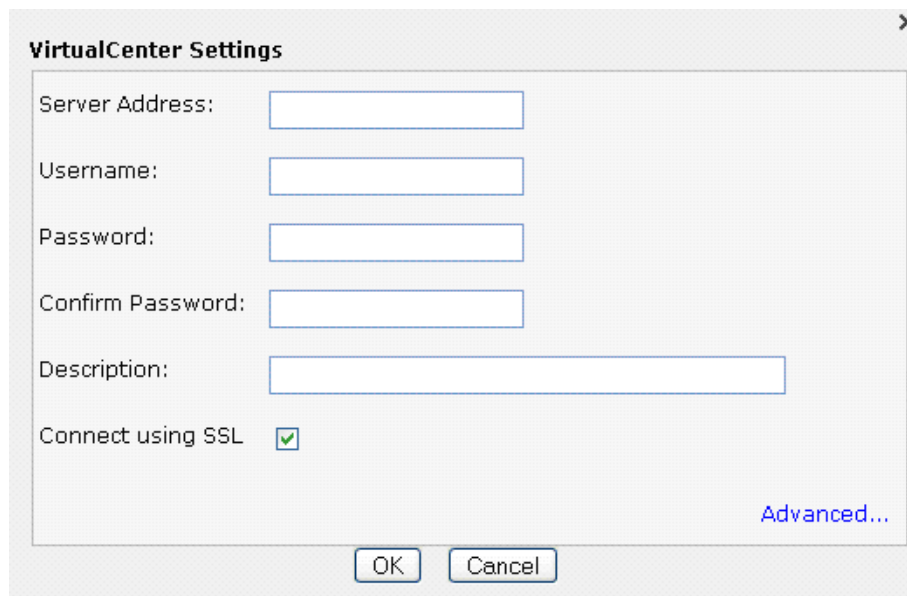
After logging in you should see a screen similar to the one shown below. Explore the screen and notice the various functions available to you.



Add a VirtualCenter Server



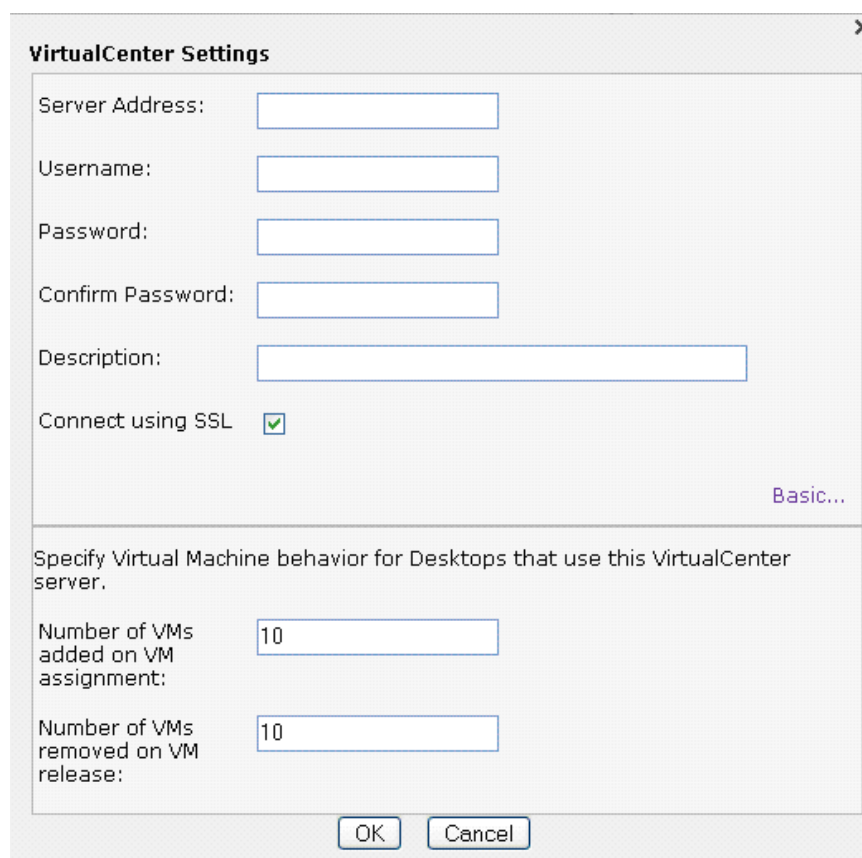
To add a VirtualCenter server click on the **Add** hyperlink to see the options for configuring VirtualCenter. You already have a VirtualCenter server assigned to your desktop manager, but the following would allow you to add additional VirtualCenter Servers to your desktop manager. The screen seen below appears.



The image shows a 'VirtualCenter Settings' dialog box. It contains the following fields and controls:

- Server Address:
- Username:
- Password:
- Confirm Password:
- Description:
- Connect using SSL: ☒
- Advanced... (hyperlink)
- OK button
- Cancel button

Click on the **Advanced** hyperlink for additional configuration options. The screen below appears.



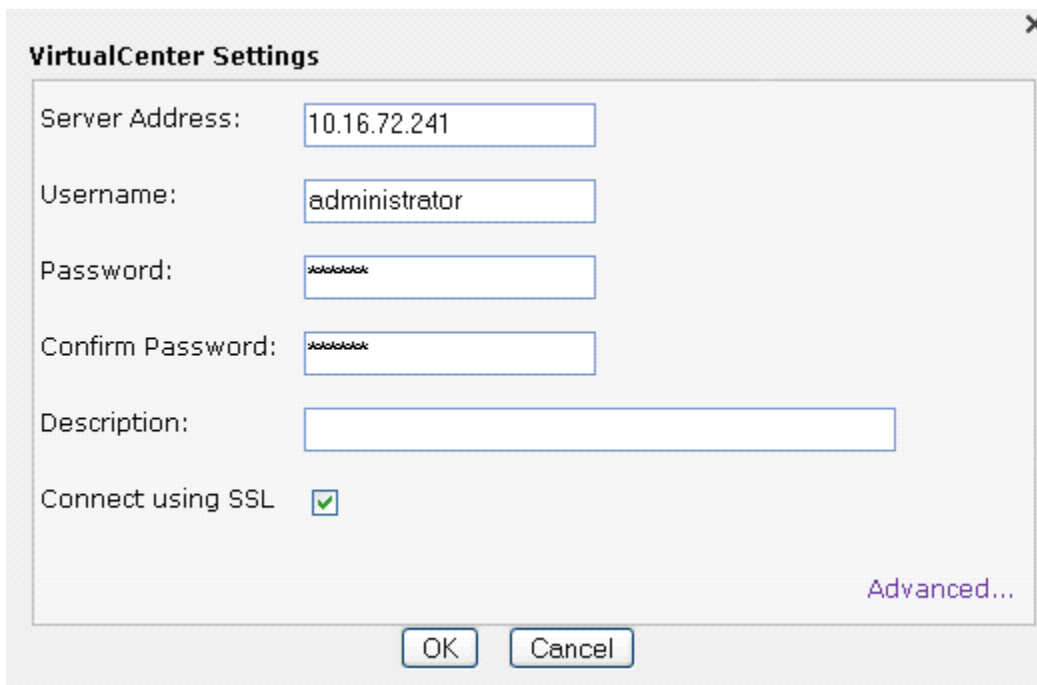
The image shows the 'VirtualCenter Settings' dialog box with the 'Advanced' tab selected. It contains the following fields and controls:

- Server Address:
- Username:
- Password:
- Confirm Password:
- Description:
- Connect using SSL: ☒
- Basic... (hyperlink)
- Specify Virtual Machine behavior for Desktops that use this VirtualCenter server.
- Number of VMs added on VM assignment:
- Number of VMs removed on VM release:
- OK button
- Cancel button

Using **Number of VMs added on VM assignment** and **Number of VMs removed on VM release** you can control how many disk-intensive operations VDM will attempt to perform at once according to your infrastructure's performance. Set these to 1 to start with.

Click **Cancel** to return to the main configuration screen.

You should now be on the main window of the administration console. Under the **VirtualCenter Servers** section of this page, click on the name of your VirtualCenter server. Doing this will bring the **Edit** and **Remove** functions into focus. Click on the **Edit** hyperlink to view the configuration of your VirtualCenter server.

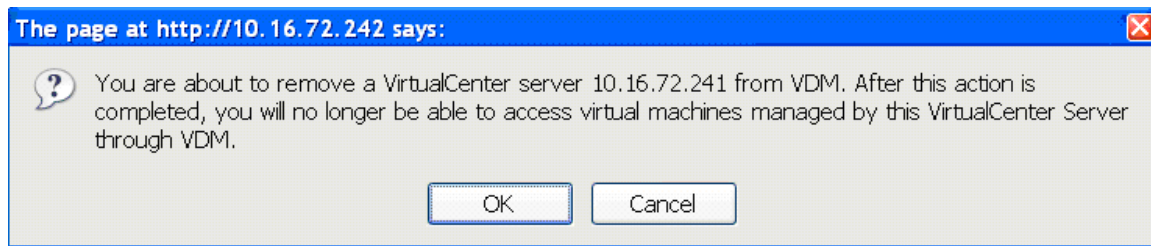


The screenshot shows a 'VirtualCenter Settings' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Server Address:** A text box containing '10.16.72.241'.
- Username:** A text box containing 'administrator'.
- Password:** A text box with masked characters 'xoxoxoxox'.
- Confirm Password:** A text box with masked characters 'xoxoxoxox'.
- Description:** An empty text box.
- Connect using SSL:** A checkbox that is checked, indicated by a green checkmark icon.
- Advanced...** A purple hyperlink located at the bottom right of the settings area.
- OK** and **Cancel** buttons are located at the bottom center of the dialog.

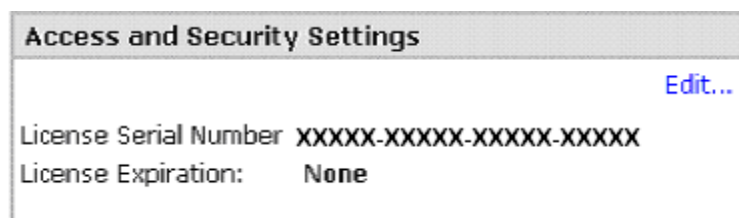
You may edit your advanced options if you like or click **Cancel** to return to the main configuration screen.

Clicking the remove hyperlink will cause the following warning screen to appear. **DO NOT CLICK REMOVE.**

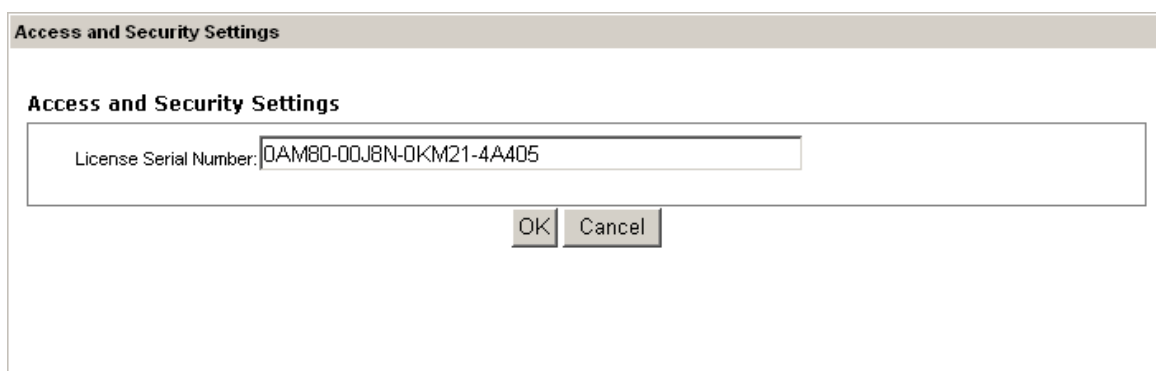


If you selected the remove function **DO NOT** click **OK**. Click **Cancel** if this message is on your screen.

Access and Security Functions



On the main configuration page of the VDM connection broker located in the **Access and Security Settings** dialog. Click the **Edit** hyperlink to add or modify your existing license.



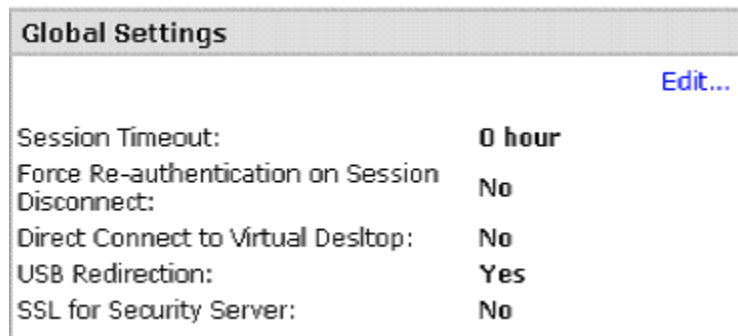
Enter your license key provided for your station and click **OK**.

The license information is stored internally on the Virtual Desktop Manager and is not part of the existing VI3 licensing server infrastructure.

This section will also be used to configure the certificate used for the Security Server component of Virtual Desktop Manager.

Global Settings

Go back to the main configuration page of the VDM connection broker and locate the **Global Settings** dialog. These settings affect every user logged into the connection broker.



The image shows a 'Global Settings' dialog box with a title bar. In the top right corner, there is a blue 'Edit...' link. The settings are listed as follows:

Session Timeout:	0 hour
Force Re-authentication on Session Disconnect:	No
Direct Connect to Virtual Desktop:	No
USB Redirection:	Yes
SSL for Security Server:	No

Click **Edit** to modify the following options.

Session Timeout: time duration in hours

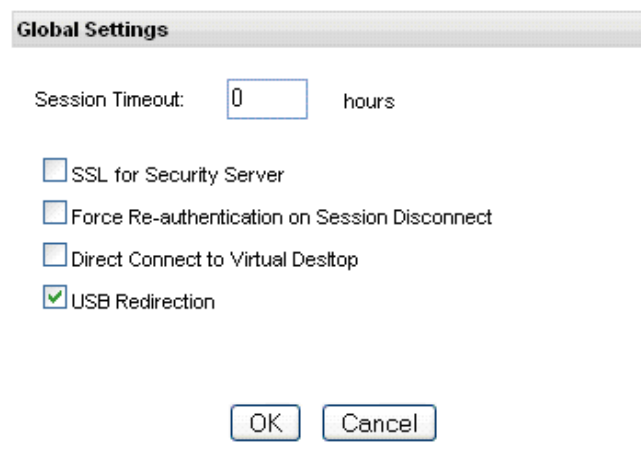
Force re-authentication on Session Disconnect: yes/no

Direct Connection to Virtual Desktop: yes/no

USB Redirection: yes/no

SSL for Security Server: yes/no

The following screen will appear and allow you to edit these settings.

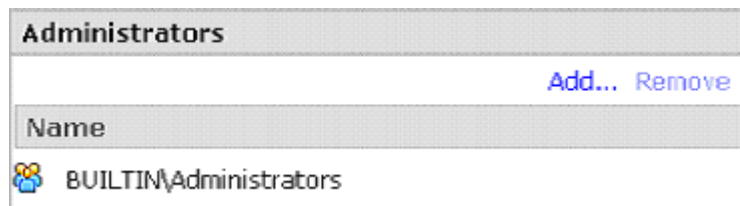


The image shows the 'Global Settings' dialog box in edit mode. It has a title bar and the following controls:

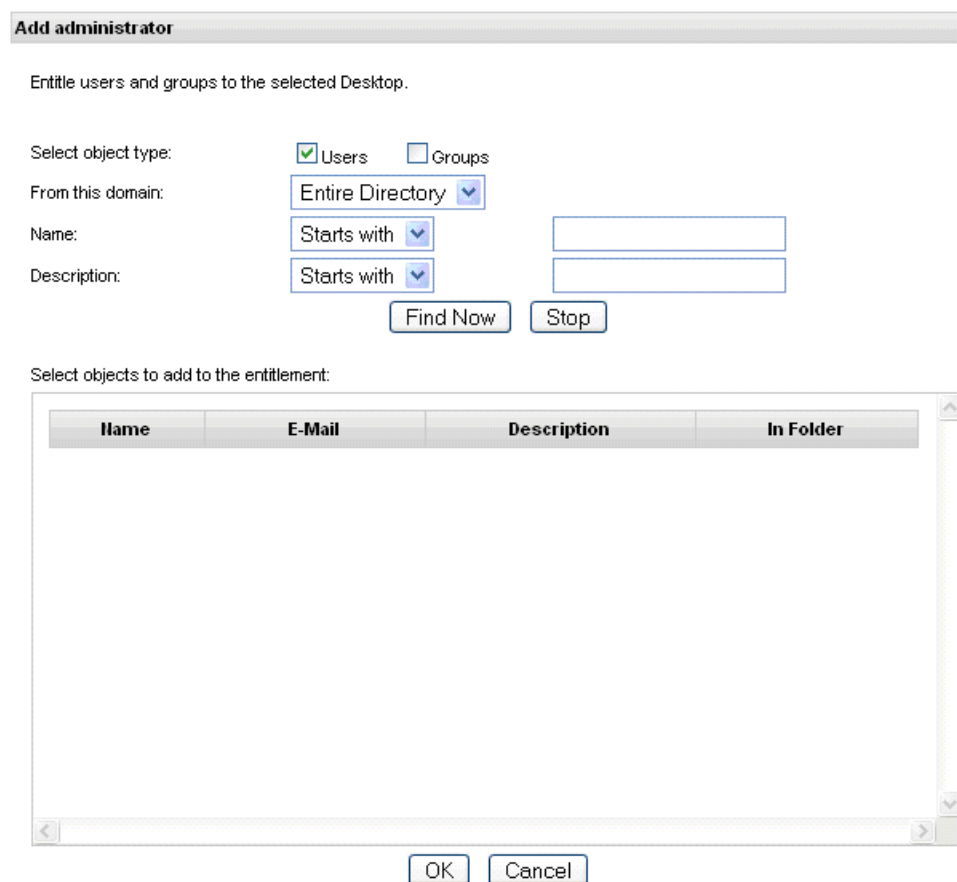
- Session Timeout: A text box containing '0' followed by the text 'hours'.
- Four checkboxes:
 - ☐ SSL for Security Server
 - ☐ Force Re-authentication on Session Disconnect
 - ☐ Direct Connect to Virtual Desktop
 - ☒ USB Redirection
- At the bottom, there are two buttons: 'OK' and 'Cancel'.

Check each option you want to enable and enter a time in hours for the session timeout. Click **OK** when done to return to the main configuration screen.

Administrators



Go back to the main configuration page of the VDM connection broker. Locate the **Administrators** dialog and click **Add** to create additional administrators for the connection broker. The following screen will appear. You may search Active Directory for groups or users and add them.

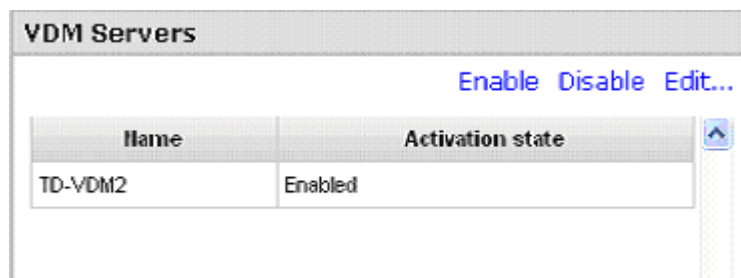


When you have found the correct Group or User highlight them and click **OK**.

To remove a user or group, click on their name in the primary configuration window and then click the **Remove** hyperlink.

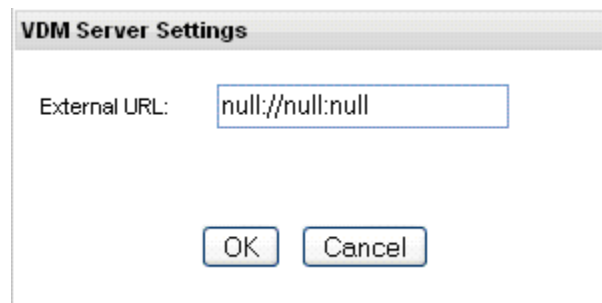
The connection broker will not let you remove the last administrator from the system.

VDM Servers



Go back to the main configuration page of the VDM connection broker. Locate the **VDM Servers** dialogue, click on the server name, and then click on **Enable** or **Disable** to toggle back and forth between the two activation states.

Click the **Edit** hyperlink to add a new VDM server. The following screen appears.



Enter the URL of the VDM replica you wish to add to the configuration. Click **OK** to save the server information. The replica will be added to the pool of VDM servers and will be updated via ADAM. Refer to the section in the lab on ADAM for more information.

Adding A Static Desktop

Step 1:

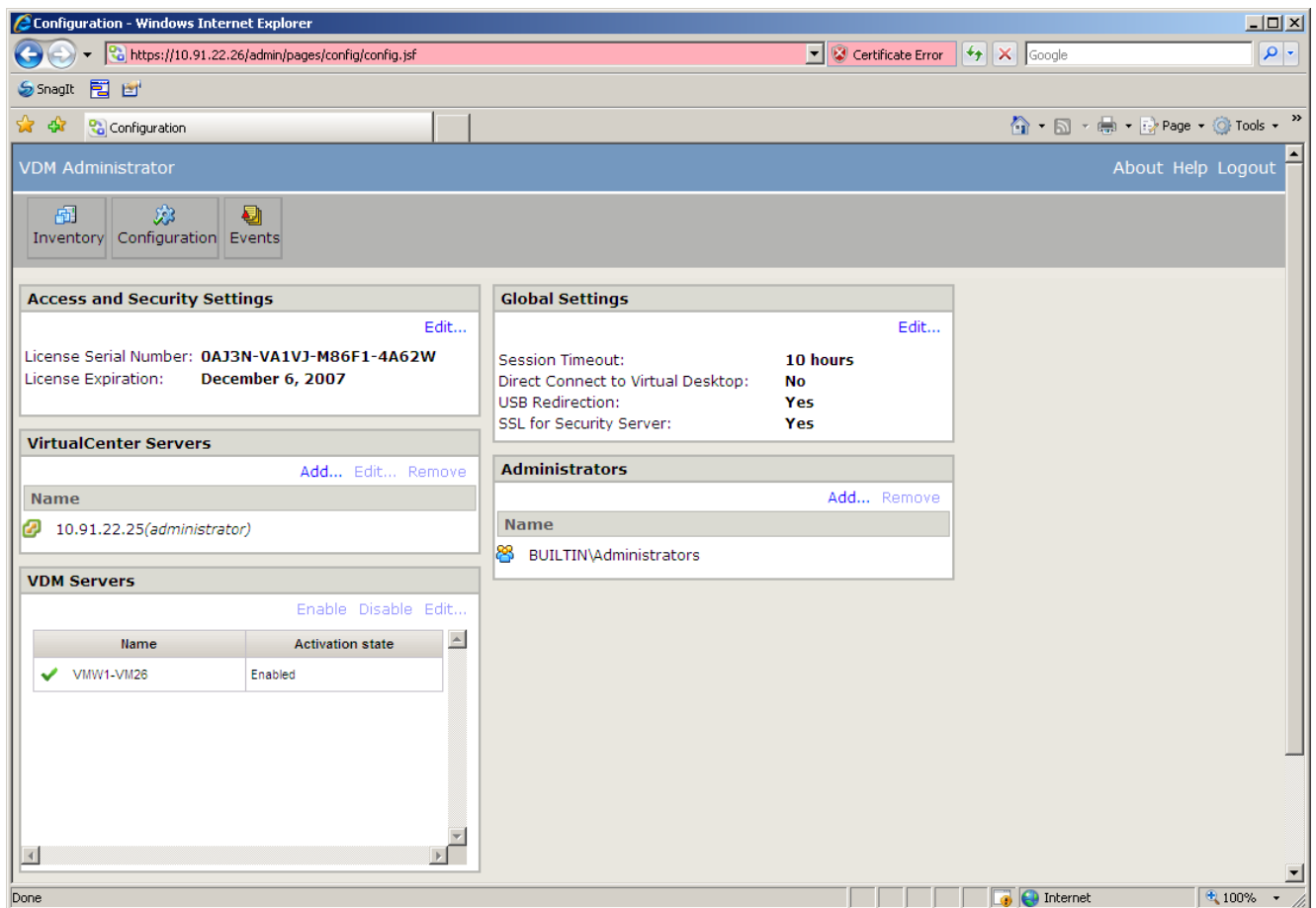
Using Internet Explorer Login to the VDM using the vmware1 account.

Username: vmware1

Password: vmware

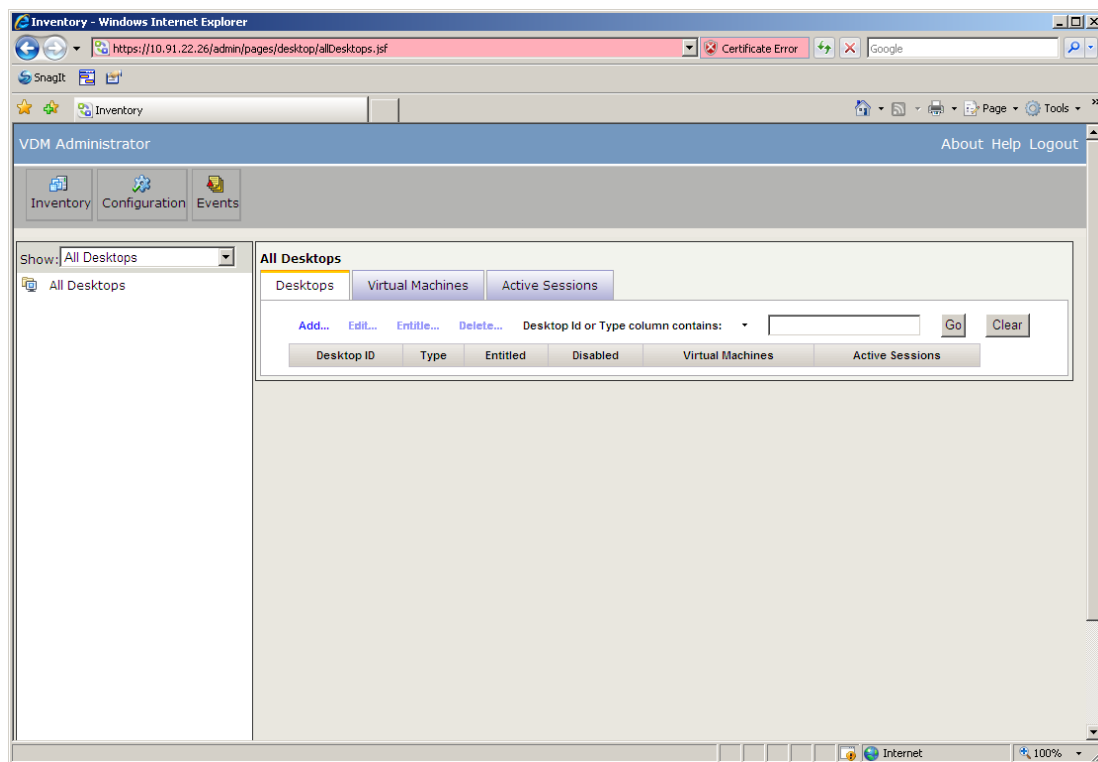
Step 2:

Click on the **Inventory** tab



Step 3:

On the **Desktops** tab, click on **Add**



Step 4:

Select **Individual Desktop** radio button and click on **Next**

A screenshot of the 'Add Desktop' dialog box. It features a section titled 'Desktop Type' with the instruction 'Select Desktop Type'. There are three radio button options: 'Individual desktop', 'Desktop pool - persistent', and 'Desktop pool - non-persistent'. The 'Individual desktop' option is selected and circled in red, with a red arrow pointing to it. Below each option is a descriptive paragraph. At the bottom of the dialog, there are 'Next>' and 'Cancel' buttons.

Add Desktop

Desktop Type
Select Desktop Type

☒ Individual desktop
Virtual Machines for the Desktop are brought in directly from VirtualCenter and manually assigned to users by the Administrator.

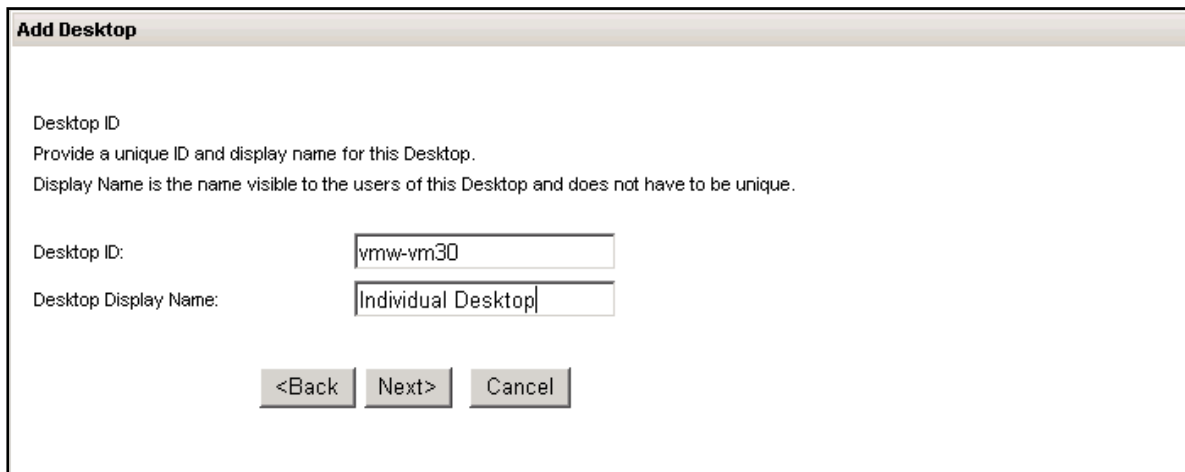
☐ Desktop pool - persistent
Virtual Machines in this Desktop are automatically created and assigned to users by the VMware Virtual Desktop Manager. Once the assignment happens, each user has the same dedicated Virtual Machine every time they sign in.

☐ Desktop pool - non-persistent
Virtual Machines in this Desktop are automatically created and assigned to users by the VMware Virtual Desktop Manager. The assignment happens on a per session basis.

Next> Cancel

Step 5:

Enter a unique **Desktop ID** to uniquely identify the VM in the system which can be any unique alpha numeric string of your choice. Next enter a **Desktop Display Name** that will be seen by the user that will be entitled to use this VM (this does not need to be unique).



Add Desktop

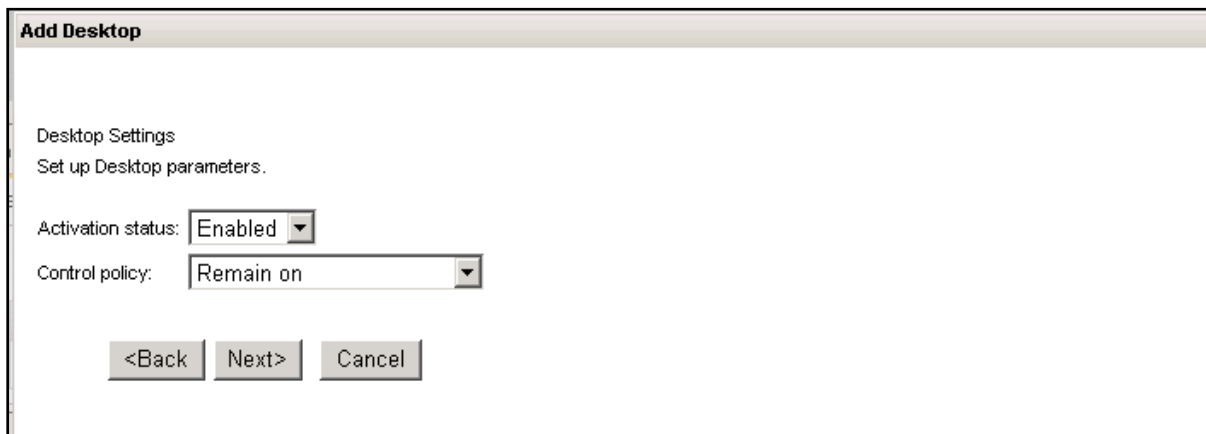
Desktop ID
Provide a unique ID and display name for this Desktop.
Display Name is the name visible to the users of this Desktop and does not have to be unique.

Desktop ID:

Desktop Display Name:

Step 6:

Set the **Activation Status** for this desktop to **Enabled**. Next, set the **Control policy** for this desktop to **Remain on**. This ensures that the desktop is readily available to us in this lab.



Add Desktop

Desktop Settings
Set up Desktop parameters.

Activation status:

Control policy:

Step 7:

Add the VirtualCenter that controls the desktop here, then click **Next**

Add Desktop

VirtualCenter Server

Select the VirtualCenter server that will be used by this Desktop.

VirtualCenter Server: 10.91.22.25

<Back

Next>

Cancel







Step 8:

Select the virtual machine then click **Next**

Add Desktop

Virtual Machine Selection

Select one or more Virtual Machines for this Desktop to use.

Name	Type	Path
 VDI-test	Microsoft Windows XP Professional	/Pod 5/vm/VDI-test
 vmw1-vm28-xp2	Microsoft Windows XP Professional	/Pod 5/vm/vmw1-vm28-xp2
 vmw1-vm29-xp3	Microsoft Windows XP Professional	/Pod 5/vm/vmw1-vm29-xp3
 vmv1-vm25-VC	Microsoft Windows Server 2003, Enterprise Edition	/Pod 5/vm/vmv1-vm25-VC
 vmw1-vm26-VDM	Microsoft Windows Server 2003, Enterprise Edition	/Pod 5/vm/vmw1-vm26-VDM
 vmw1-vm27-xp1	Microsoft Windows XP Professional	/Pod 5/vm/vmw1-vm27-xp1

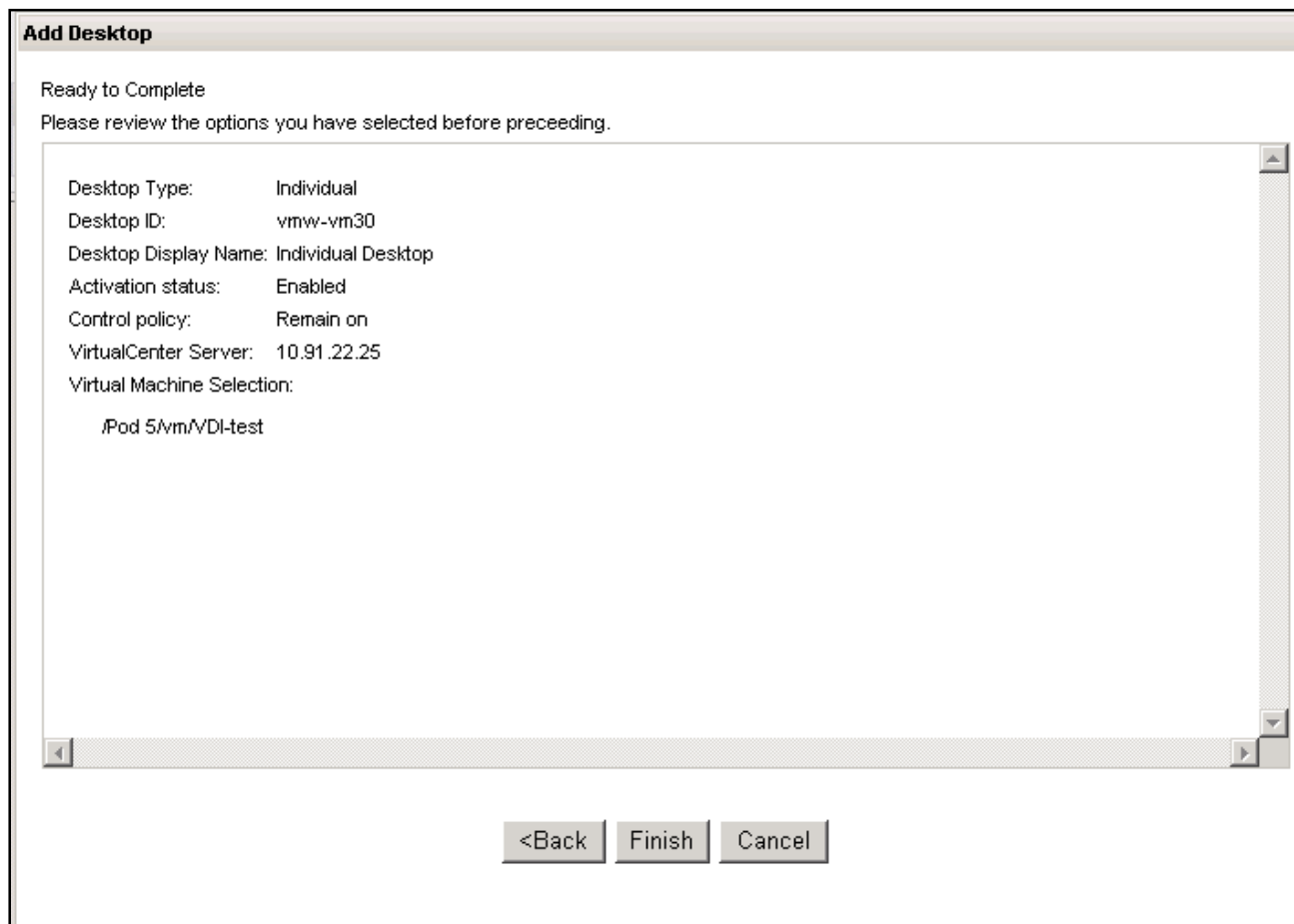
<Back

Next>

Cancel

Step 9:

Review what you have entered for accuracy, then click **Finish**



Add Desktop

Ready to Complete

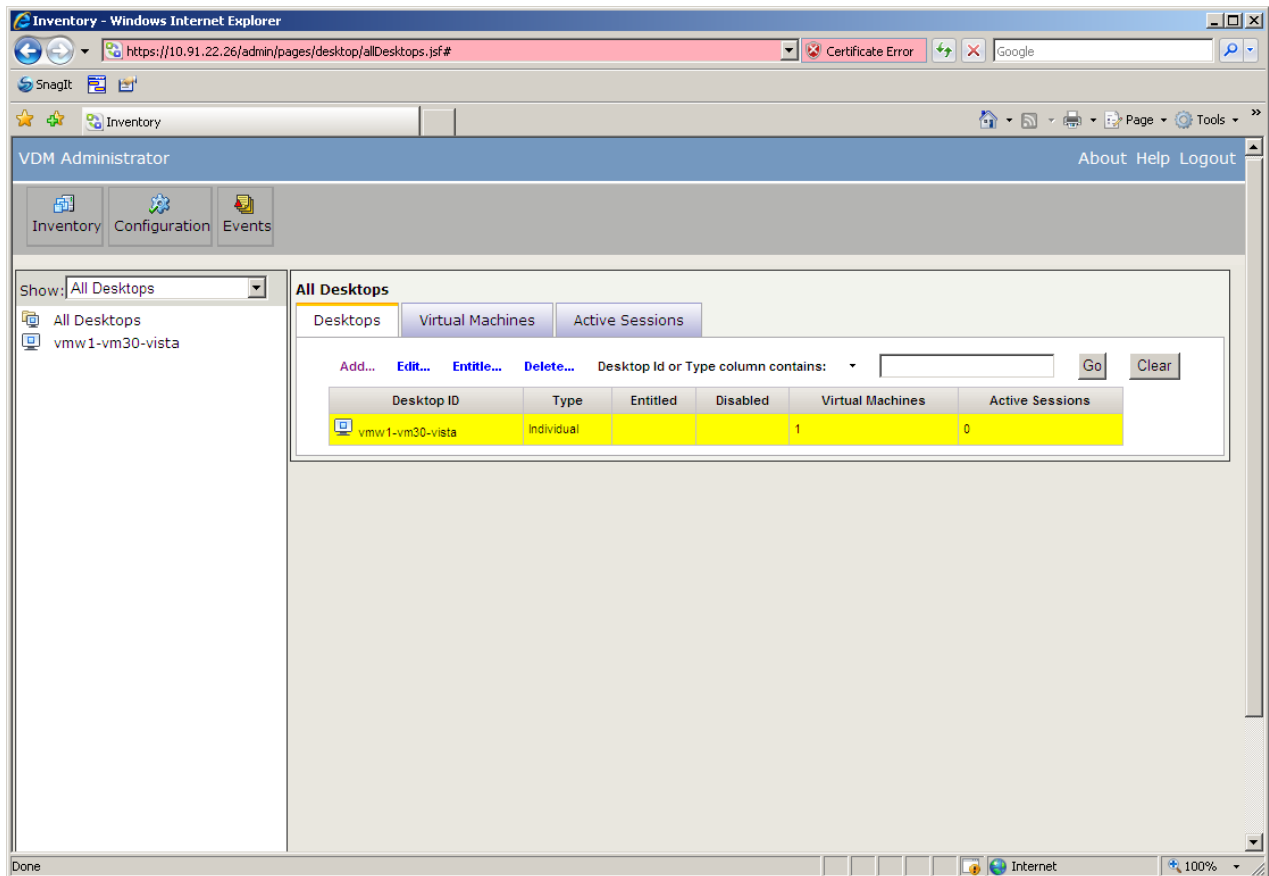
Please review the options you have selected before preceeding.

Desktop Type:	Individual
Desktop ID:	vmw-vm30
Desktop Display Name:	Individual Desktop
Activation status:	Enabled
Control policy:	Remain on
VirtualCenter Server:	10.91.22.25
Virtual Machine Selection:	/Pod 5/vm/VDI-test

<Back **Finish** Cancel

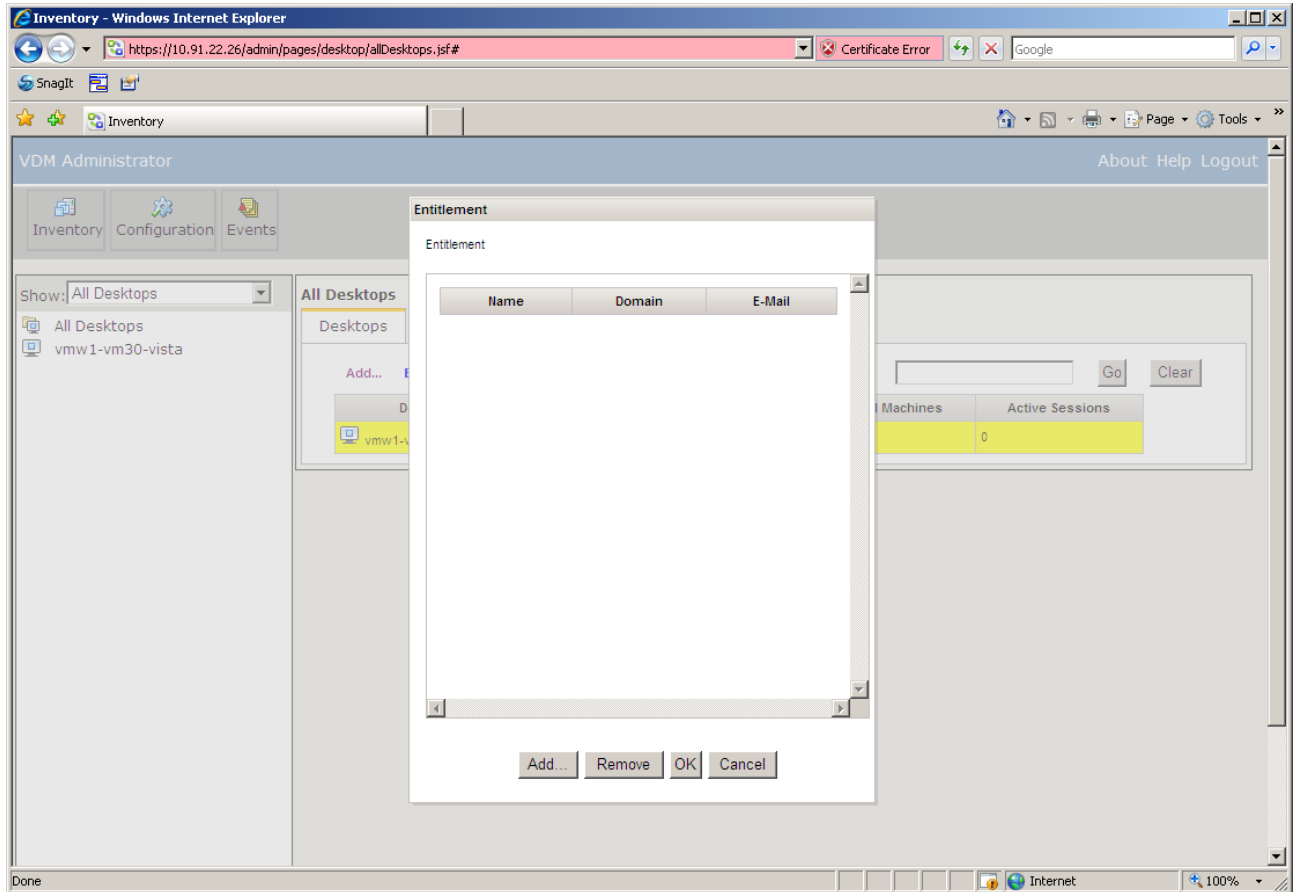
Step 10:

We now need to now entitle a specific user to access this new desktop. Select your newly added desktop then click **Entitlements**.



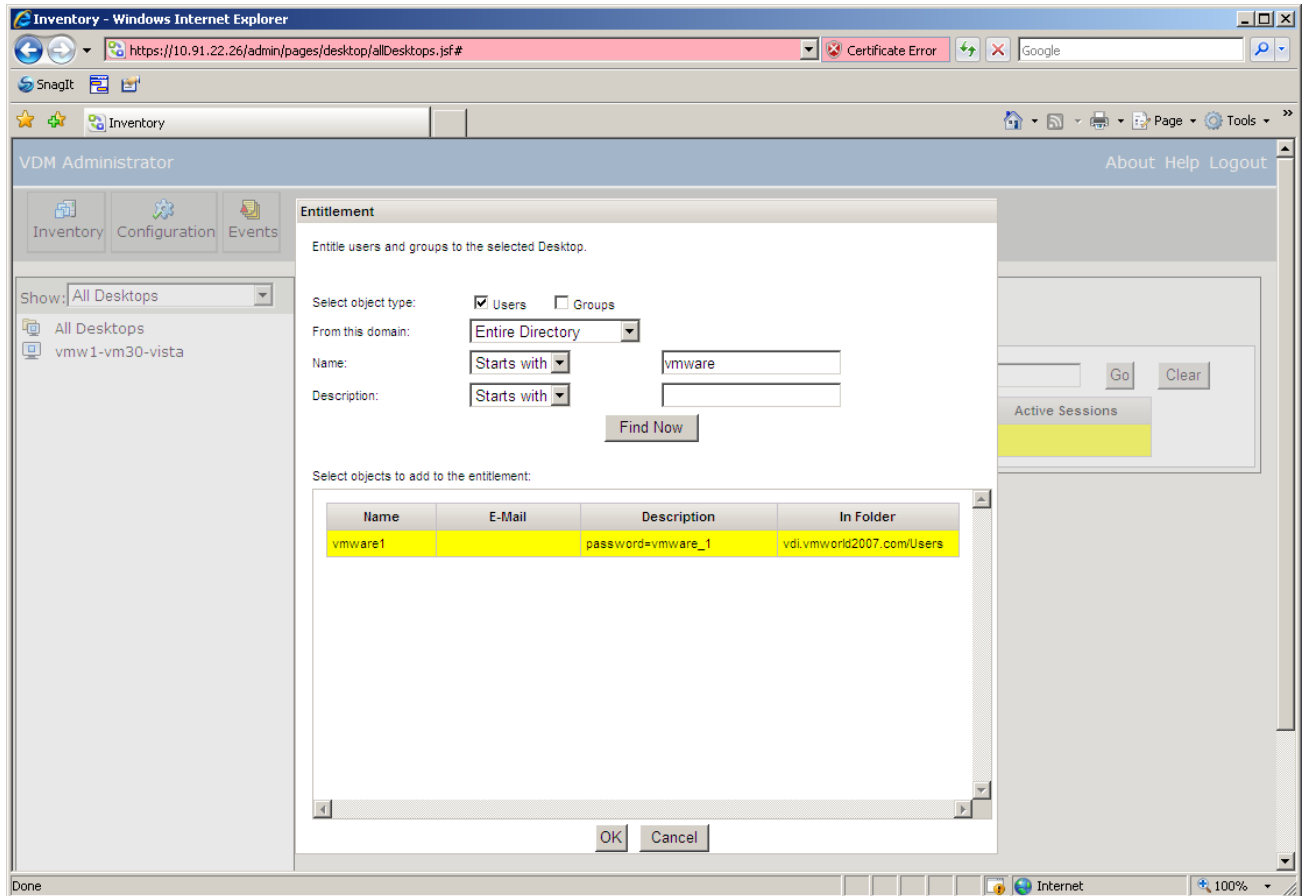
Step 11:

Click **Add**.



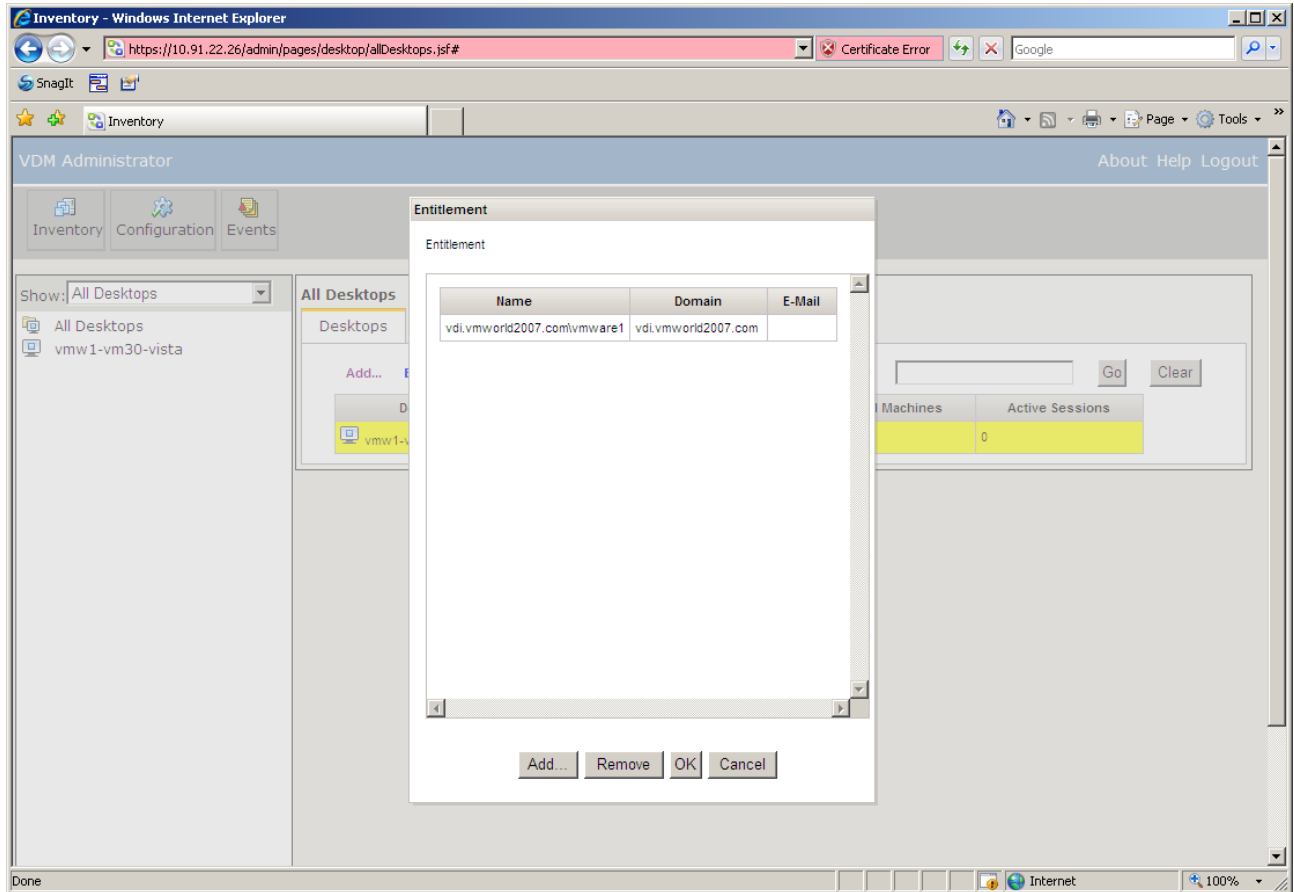
Step 12:

Click into the **Name** field. Type enough of the user's name to narrow the search down. Click **Find Now**. Next, select the user you wish to entitle and then click on **OK**.



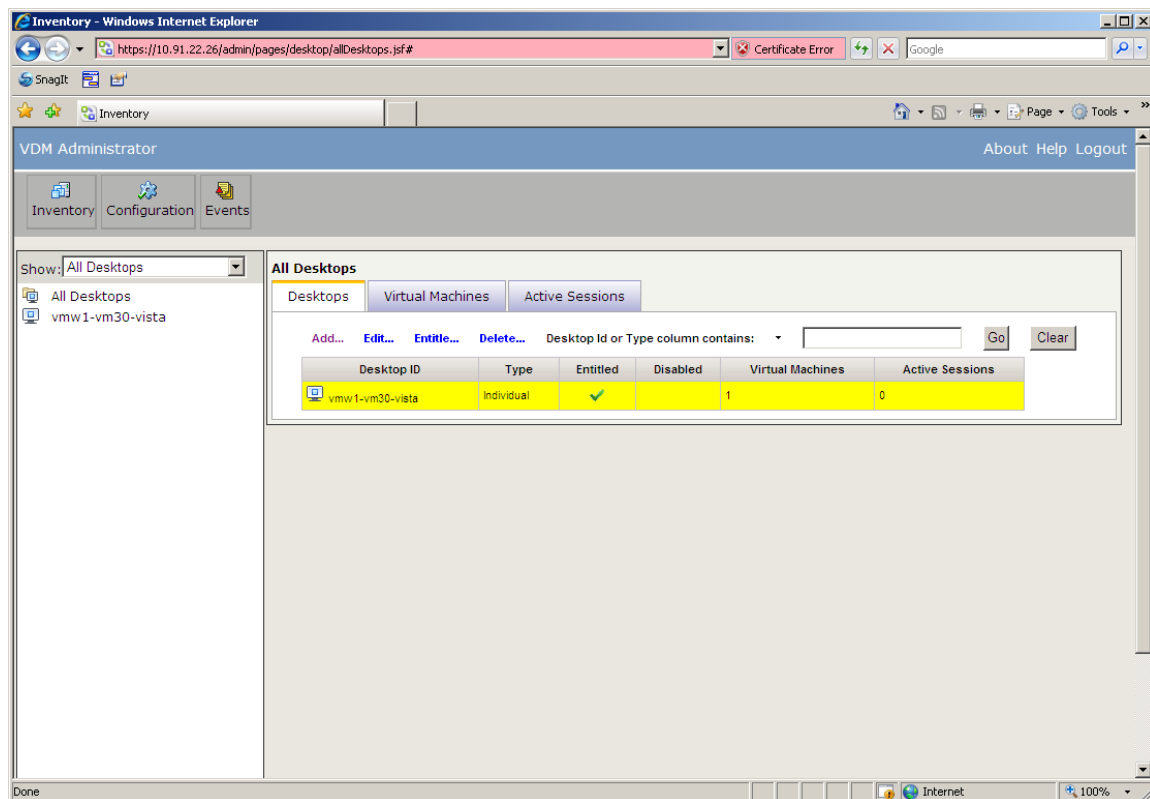
Step 13:

Review your choice for accuracy, then click on **OK**



Step 14:

You have now entitled your user to access your desktop. You should now notice a green check mark in the entitlement column next to the desktop.



Non-persistent pools

The following section of the guide will walk you through creating a non persistent pool within VDM 2.0. The creation process is essentially the same as with a persistent pool but the behavior is different in that the desktop sessions are not persistent between logins.

Step 1:

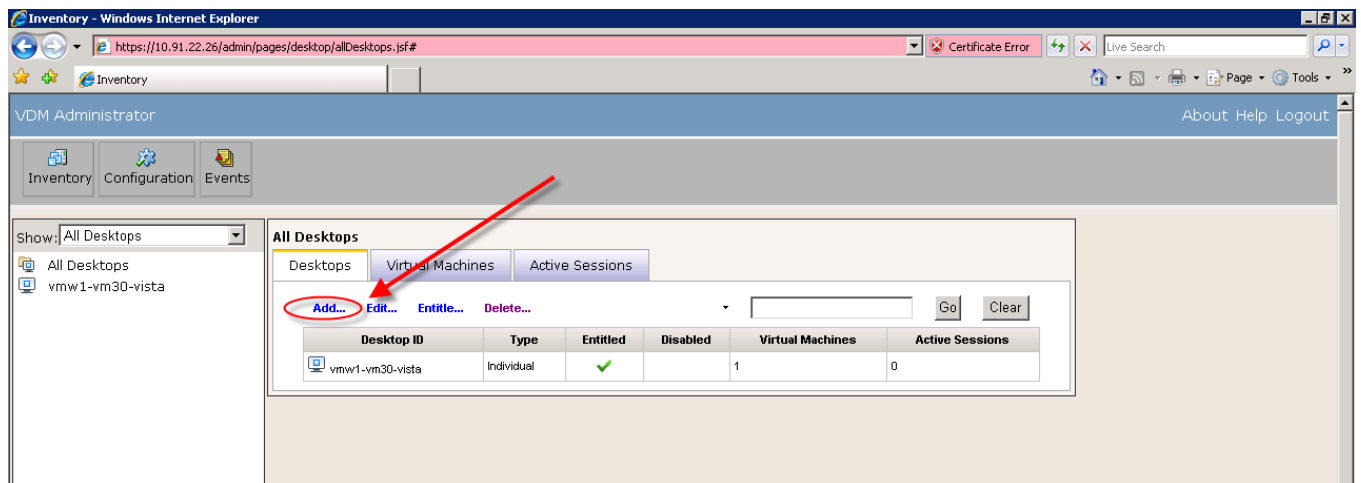
Using your browser, log in to the VDM admin console using the administrative account.

Username: vmware1

Password: vmware

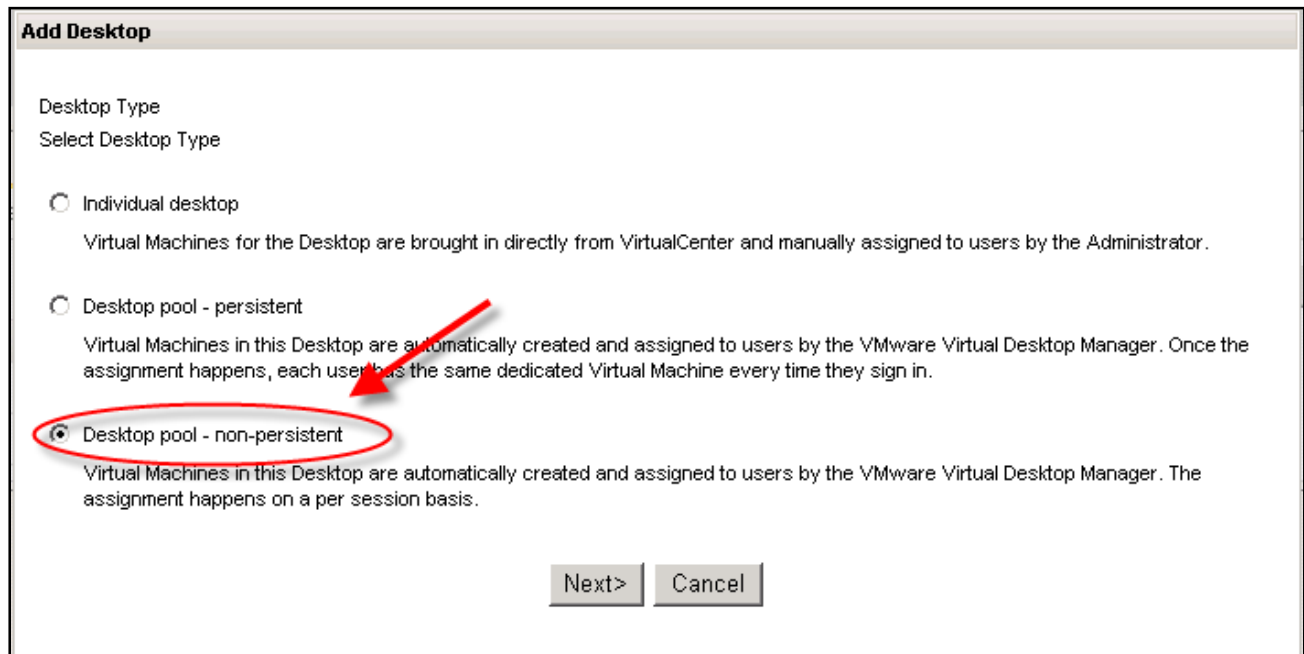
Step 2:

In the **Inventory > Desktops** tab click on **Add**.



Step 3:

Select **Desktop pool – non persistent**



Add Desktop

Desktop Type
Select Desktop Type

☐ Individual desktop
Virtual Machines for the Desktop are brought in directly from VirtualCenter and manually assigned to users by the Administrator.

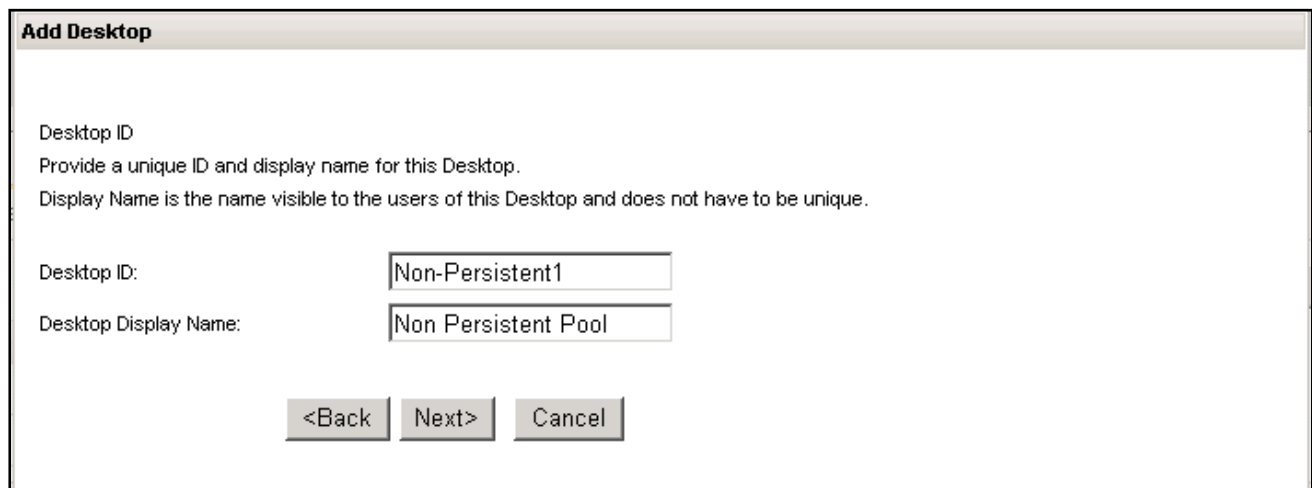
☐ Desktop pool - persistent
Virtual Machines in this Desktop are automatically created and assigned to users by the VMware Virtual Desktop Manager. Once the assignment happens, each user has the same dedicated Virtual Machine every time they sign in.

☒ **Desktop pool - non-persistent**
Virtual Machines in this Desktop are automatically created and assigned to users by the VMware Virtual Desktop Manager. The assignment happens on a per session basis.

Next> Cancel

Step 4:

Fill in the pertinent fields. Choose a unique **Desktop ID** and **Desktop Display Name**.



Add Desktop

Desktop ID
Provide a unique ID and display name for this Desktop.
Display Name is the name visible to the users of this Desktop and does not have to be unique.

Desktop ID:

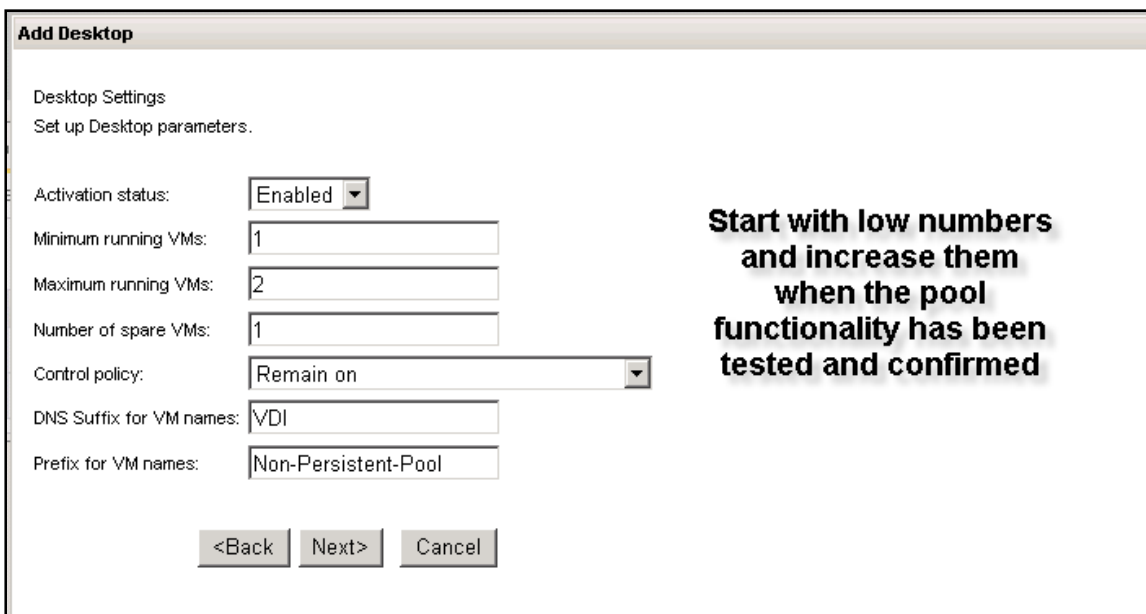
Desktop Display Name:

<Back Next> Cancel

Step 5:

Modify the appropriate settings including **DNS Prefix** and **DNS Suffix for VM names**.

- **Minimum Running VMs:** There will never be fewer than this number of VMs running and ready for immediate use in the pool at any given time. Set this number to 1.
- **Maximum Running VMs:** There will never be more that this number of VMs available for use in the pool at any given time. Set this number to 2.
- **Number of Spare VMs:** VDM will always attempt to ensure that there is this number of VMs running available to connect to. This number may not always be achieved at any one instant due to delays in cloning and creating VMs. If this number is exceeded the **Control Policy** will be utilized to decrease the number of running VMs, thus conserving resources. Set this number to 1.
- **Control Policy:** Controls what state the machine is placed in while not in use. The **Remain On** control policy ensures the machine is always on and ready to be used.
- **DNS Suffix for VM names:** DNS name which will be appended to each VM name.
- **Prefix for VM names:** String that each VM name will start with.



The screenshot shows a dialog box titled "Add Desktop" with a section for "Desktop Settings". Below the title bar, it says "Set up Desktop parameters." The settings are as follows:

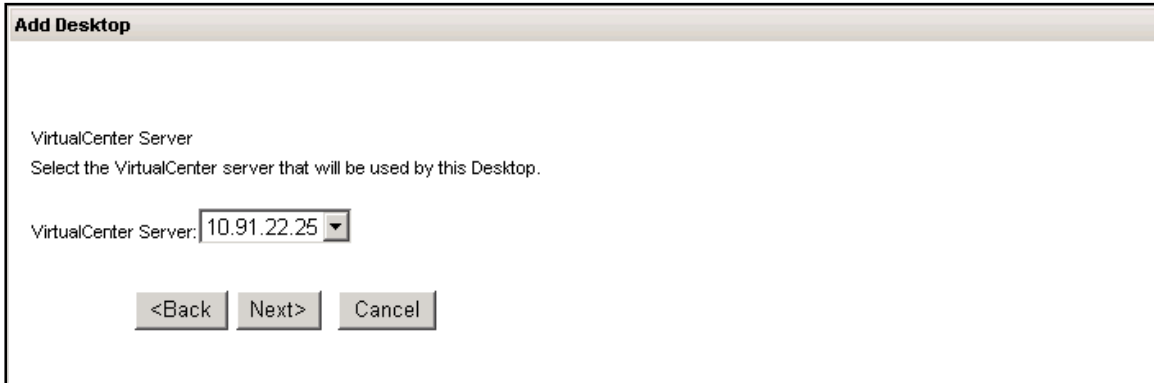
- Activation status: Enabled (dropdown menu)
- Minimum running VMs: 1 (text input)
- Maximum running VMs: 2 (text input)
- Number of spare VMs: 1 (text input)
- Control policy: Remain on (dropdown menu)
- DNS Suffix for VM names: VDI (text input)
- Prefix for VM names: Non-Persistent-Pool (text input)

At the bottom are three buttons: "<Back", "Next>", and "Cancel".

Start with low numbers and increase them when the pool functionality has been tested and confirmed

Step 6:

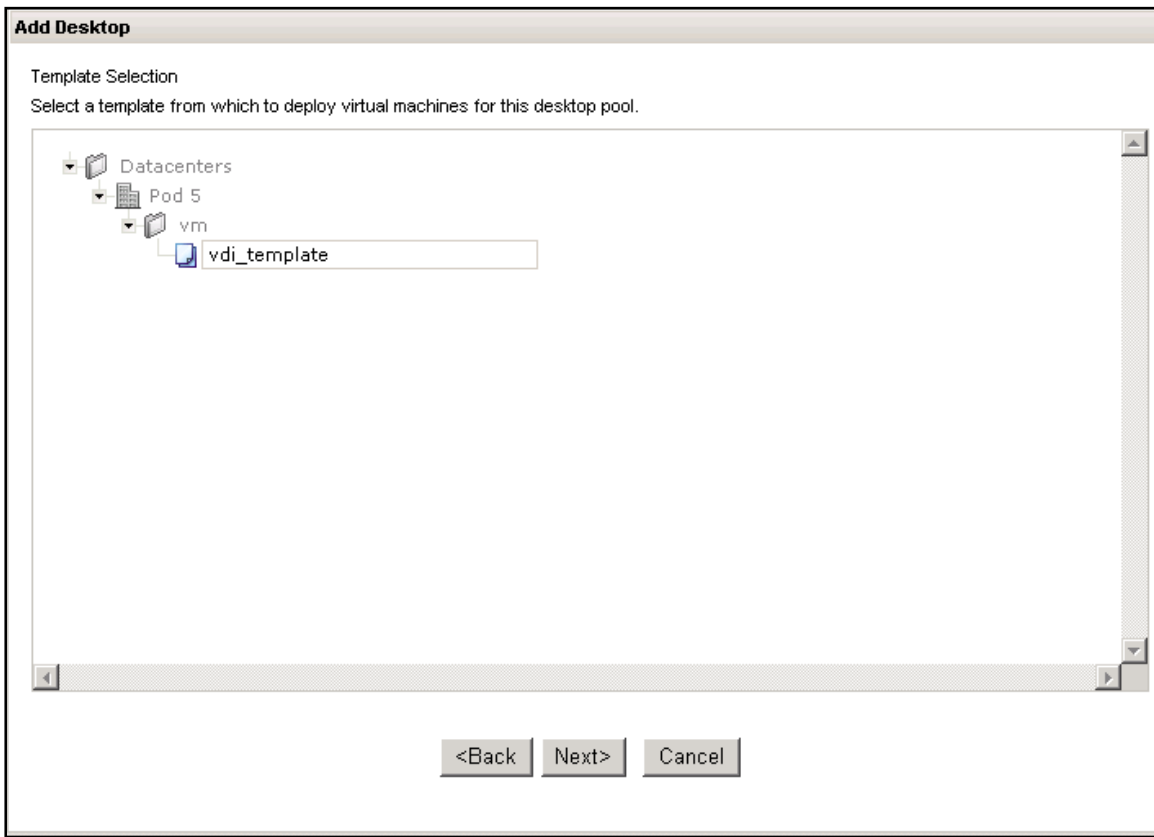
Select the VirtualCenter server to associate the pool with.



The screenshot shows a window titled "Add Desktop". Inside, the text "VirtualCenter Server" is followed by the instruction "Select the VirtualCenter server that will be used by this Desktop." Below this, there is a label "VirtualCenter Server:" and a dropdown menu showing "10.91.22.25". At the bottom, there are three buttons: "<Back", "Next>", and "Cancel".

Step 7:

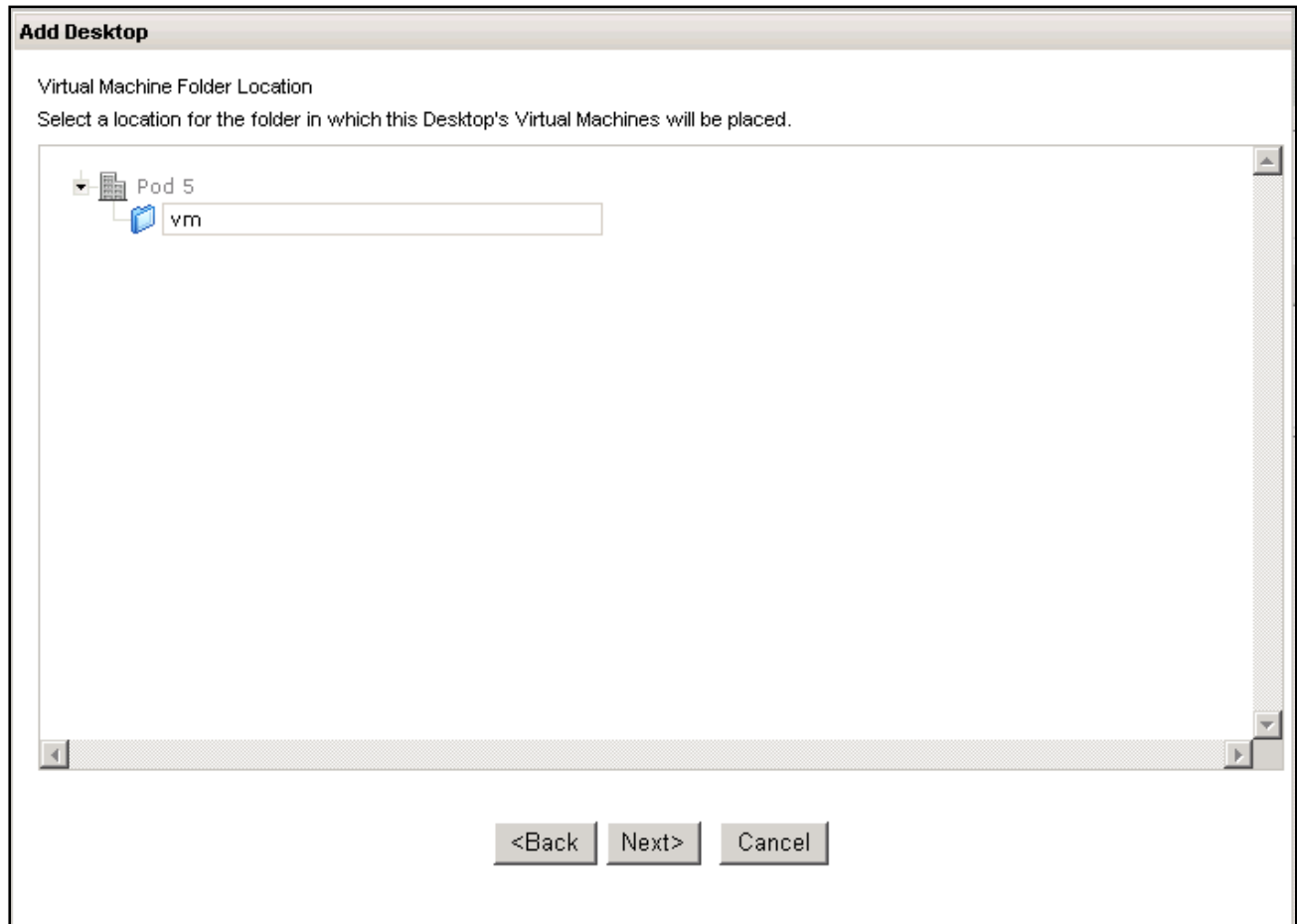
Select the template within VirtualCenter that will be used to deploy virtual machines within this pool.



The screenshot shows a window titled "Add Desktop". Inside, the text "Template Selection" is followed by the instruction "Select a template from which to deploy virtual machines for this desktop pool." Below this is a tree view showing a hierarchy: "Datacenters" (expanded) -> "Pod 5" (expanded) -> "vm" (expanded) -> "vdi_template" (selected). At the bottom, there are three buttons: "<Back", "Next>", and "Cancel".

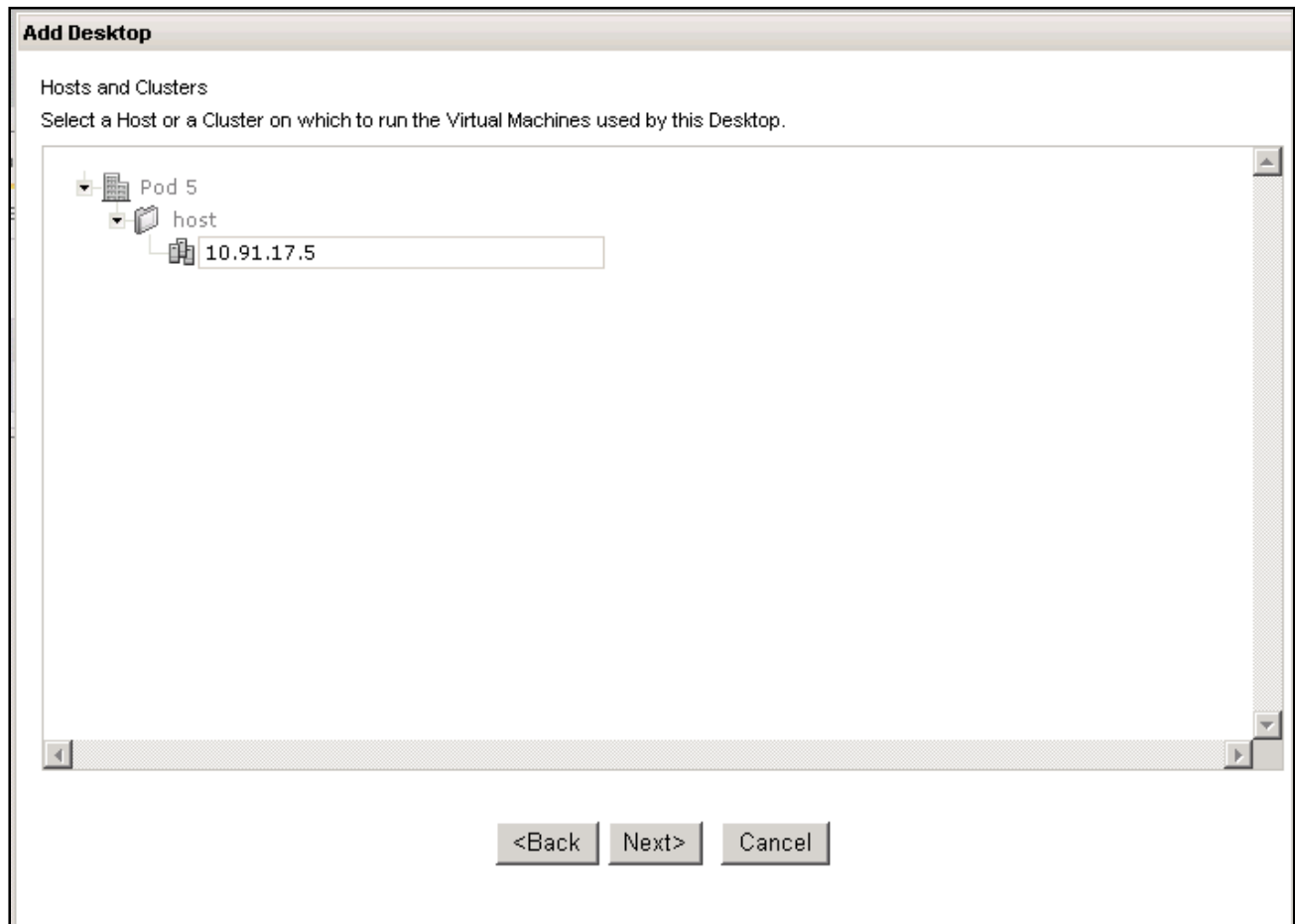
Step 8:

Select the VirtualCenter folder location that VMs will be reside in after being deployed from the template.



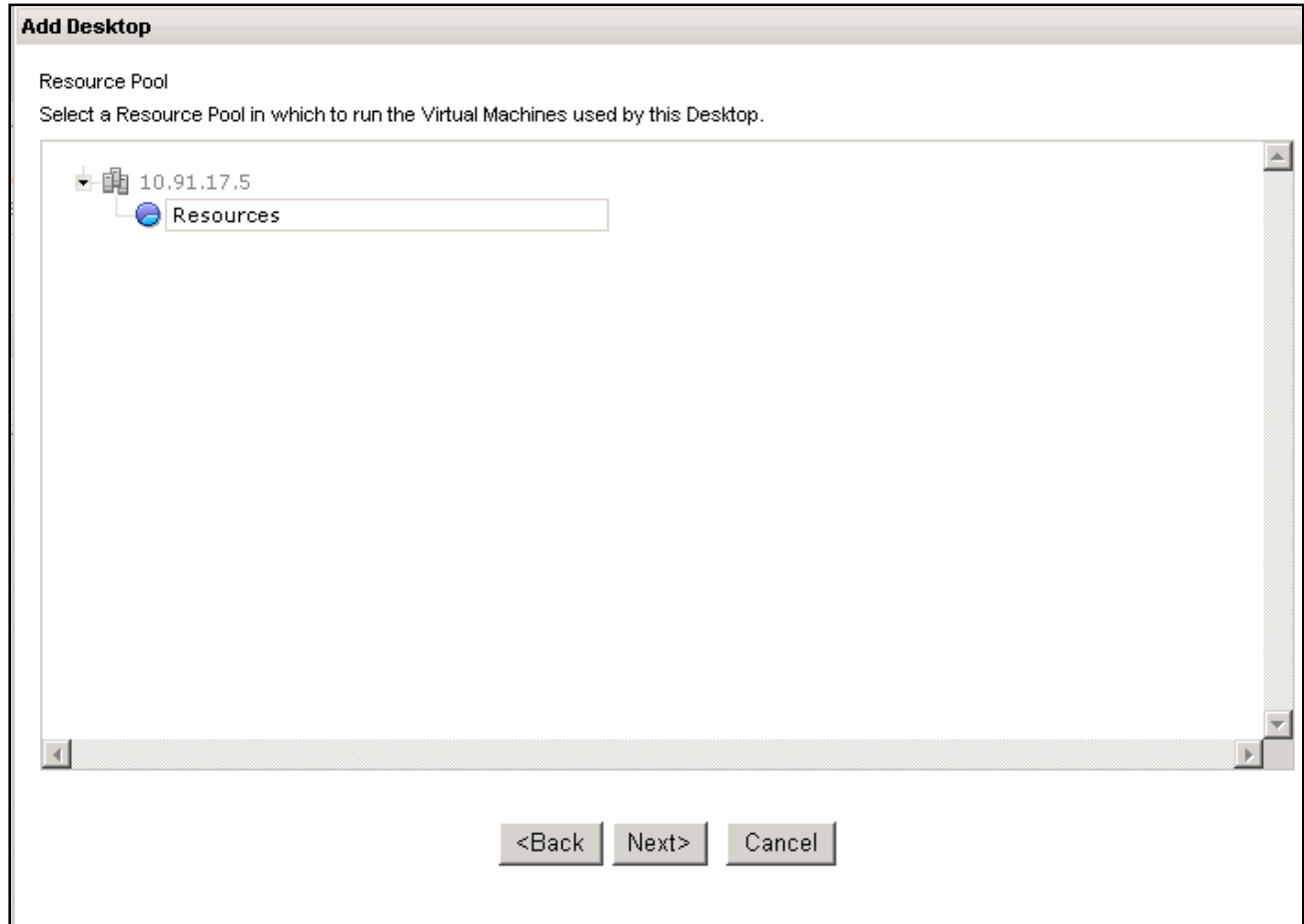
Step 9:

Select the host or cluster that the deployed VMs will reside on.



Step 10:

Select the resource pool that the new VMs will automatically be put into after being deployed.



Step 11:

Select the data store where the VM's files will reside. There can only be one datastore per pool.

Add Desktop

Datastore

Choose a Datastore to store the Virtual Machine files.

Name	Capacity (GB)	Free (GB)	Type	Access
vmw1-esx05	49.75	1.01	VMFS	Single host
storage1 (6)	60.75	47.88	VMFS	Single host

<Back Next> Cancel

Step 12:

Select the Guest Customization script to be run during the automatic sysprep of the template associated with the pool.

The screenshot shows a dialog box titled "Add Desktop". Inside, under the "Guest Customization" section, there is a text prompt: "Select a customization specification to customize the guest operating system for Virtual Machines used in this Desktop." Below this prompt is a table with three columns: "Name", "Guest OS", and "Description:". The table contains one row with the values "XP-Sysprep", "Windows", and an empty "Description:" field. At the bottom of the dialog box are three buttons: "<Back", "Next>", and "Cancel".

Name	Guest OS	Description:
XP-Sysprep	Windows	

Step 13:

Complete the configuration of the static pool.

Add Desktop




Ready to Complete
Please review the options you have selected before preceeding.



Desktop Type:	Persistent
Desktop ID:	Persistent-Pool1
Desktop Display Name:	Persistent Pool
Activation status:	Enabled
Minimum running VMs:	1
Maximum running VMs:	2
Number of spare VMs:	1
Control policy:	Remain on
DNS Suffix for VM names:	VDI
Prefix for VM names:	Persistent-Pool
VirtualCenter Server:	10.91.22.25
Template:	/Pod 5/vm/vdi_template
Virtual Machine Folder Location:	/Pod 5/vm
Host/Cluster:	/Pod 5/host/10.91.17.5
Resource Pool:	/Pod 5/host/10.91.17.5/Resources
Datastore:	/Pod 5/host/10.91.17.5/storage1 (6)
Customization specification:	XP-Sysprep-Nik

<Back Finish Cancel

Step 14:

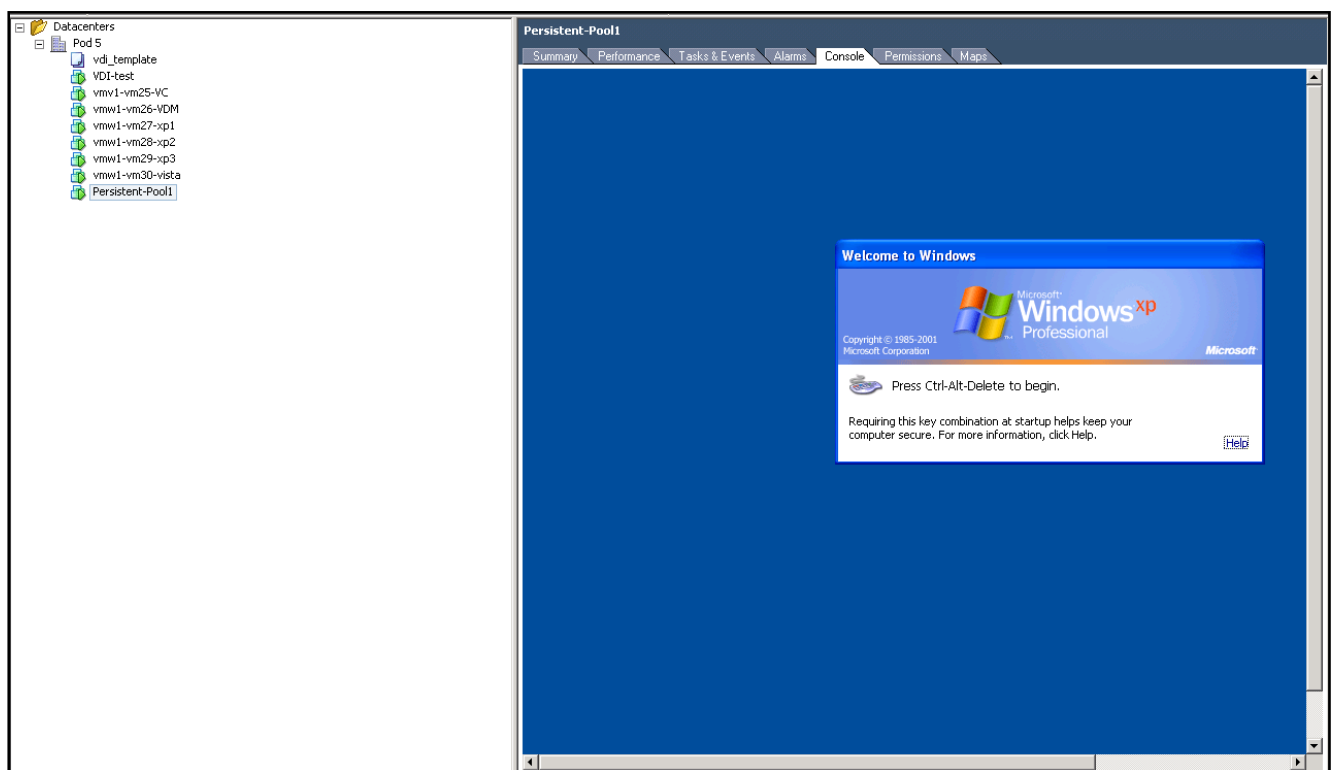
Confirm that VirtualCenter has started deploying the first machine in the pool.

Recent Tasks						
Name	Target	Status	Initiated by	Time	Start Time	Complete Time
 Clone Virtual Machine	 vdi_template	12% 	Administrator	8/23/2007 7:15:26 AM	8/23/2007 7:15:26 AM	

 Tasks  Alarms

Step 15:

After cloning a new VM, VirtualCenter will power on the new VM and the MS sysprep process will begin. Go to the console of this new VM to ensure that the sysprep process has been completed successfully.



Persistent pools

The following section of the guide will walk you through creating a persistent pool within VDM 2.0. You will not be carrying out this section during the lab.

Step 1:

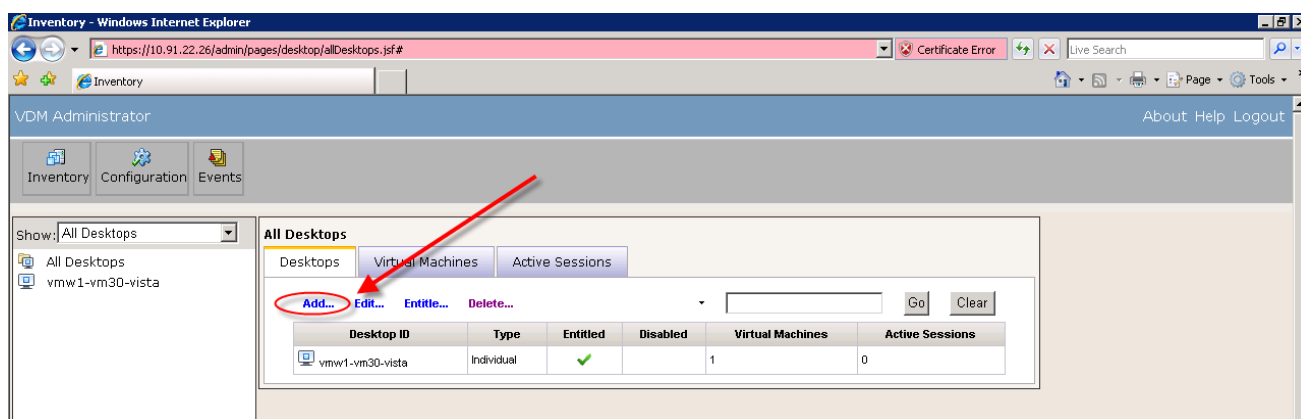
Using your browser, log in to the VDM admin console using the administrative account

Username: vmware1

Password: vmware

Step 2:

In the **Inventory > Desktops** tab click on **Add**.



Step 3:

Select **Desktop pool – persistent**

Add Desktop

Desktop Type
Select Desktop Type

☐ Individual desktop
Virtual Machines for the Desktop are brought in directly from VirtualCenter and manually assigned to users by the Administrator.

☒ Desktop pool - persistent
Virtual Machines in this Desktop are automatically created and assigned to users by the VMware Virtual Desktop Manager. Once the assignment happens, each user has the same dedicated Virtual Machine every time they sign in.

☐ Desktop pool - non-persistent
Virtual Machines in this Desktop are automatically created and assigned to users by the VMware Virtual Desktop Manager. The assignment happens on a per session basis.

Next> Cancel

Step 4:

Fill in the pertinent fields. Choose a unique **Desktop ID** and **Desktop Display Name**.

Add Desktop

Desktop ID

Provide a unique ID and display name for this Desktop.

Display Name is the name visible to the users of this Desktop and does not have to be unique.

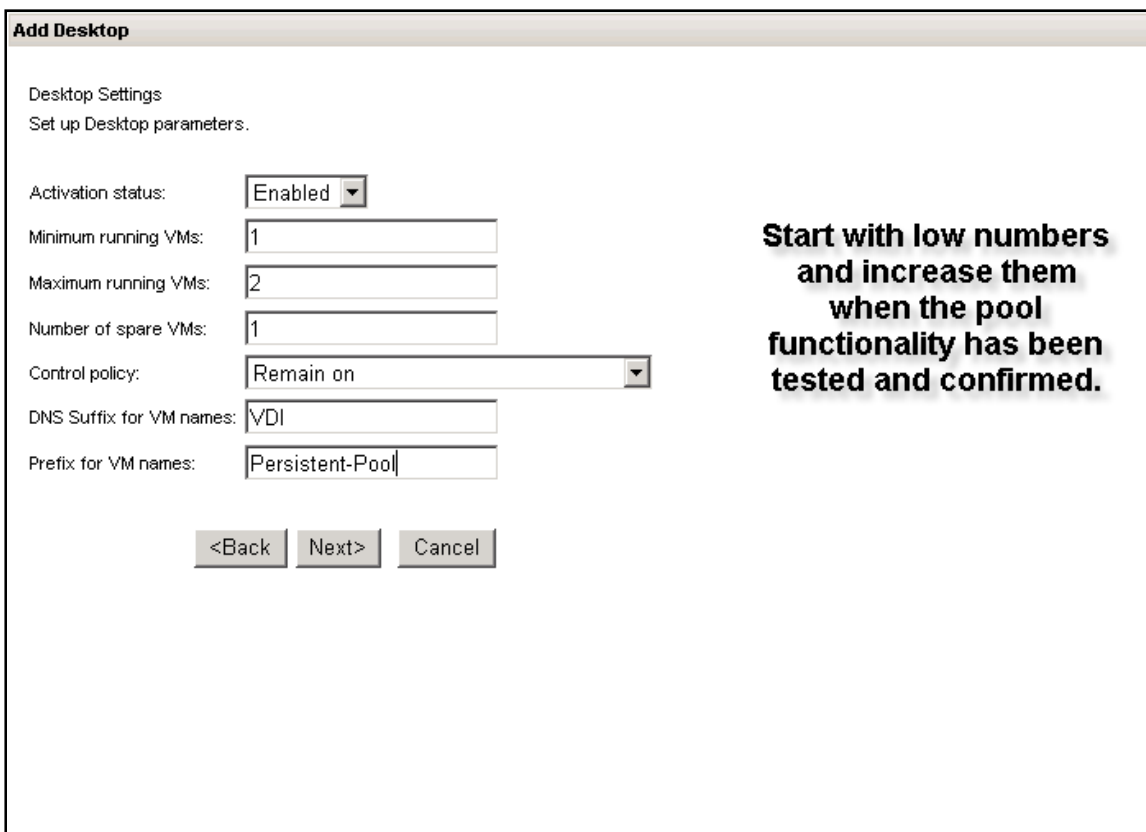
Desktop ID:

Desktop Display Name:

Step 5:

Modify the appropriate settings including **DNS Prefix** and **DNS Suffix for VM names**.

- **Minimum Running VMs:** There will never be fewer than this number of VMs running and ready for immediate use in the pool at any given time. Set this number to 1.
- **Maximum Running VMs:** There will never be more that this number of VMs available for use in the pool at any given time. Set this number to 2.
- **Number of Spare VMs:** VDM will always attempt to ensure that there is this number of VMs running available to connect to. This number may not always be achieved at any one instant due to delays in cloning and creating VMs. If this number is exceeded the **Control Policy** will be utilized to decrease the number of running VMs, thus conserving resources. Set this number to 1.
- **Control Policy:** Controls what state the machine is placed in while not in use. The **Remain On** control policy ensures the machine is always on and ready to be used.
- **DNS Suffix for VM names:** DNS name which will be appended to each VM name.
- **Prefix for VM names:** String that each VM name will start with.



The screenshot shows a dialog box titled "Add Desktop". Inside, there is a section "Desktop Settings" with the instruction "Set up Desktop parameters." Below this are several configuration fields:

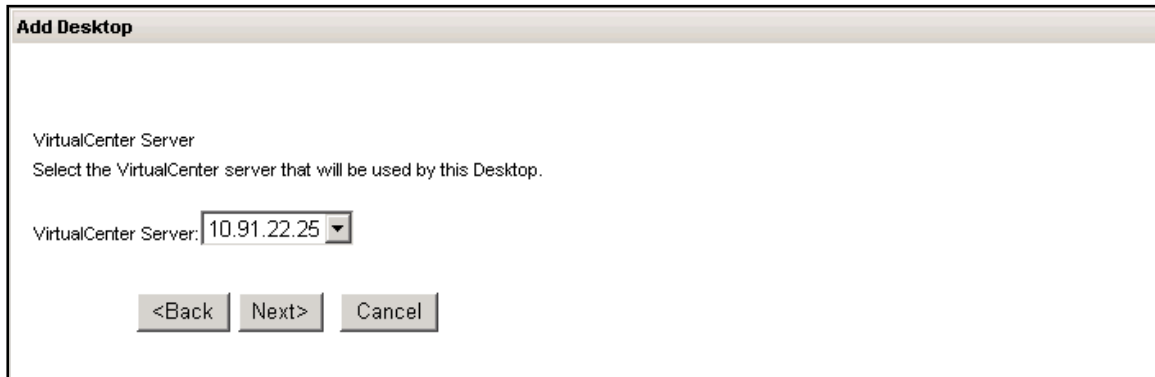
- Activation status: A dropdown menu set to "Enabled".
- Minimum running VMs: A text input field containing the number "1".
- Maximum running VMs: A text input field containing the number "2".
- Number of spare VMs: A text input field containing the number "1".
- Control policy: A dropdown menu set to "Remain on".
- DNS Suffix for VM names: A text input field containing "VDI".
- Prefix for VM names: A text input field containing "Persistent-Pool".

At the bottom of the dialog are three buttons: "<Back", "Next>", and "Cancel".

To the right of the input fields, there is a text box with the following text: **Start with low numbers and increase them when the pool functionality has been tested and confirmed.**

Step 6:

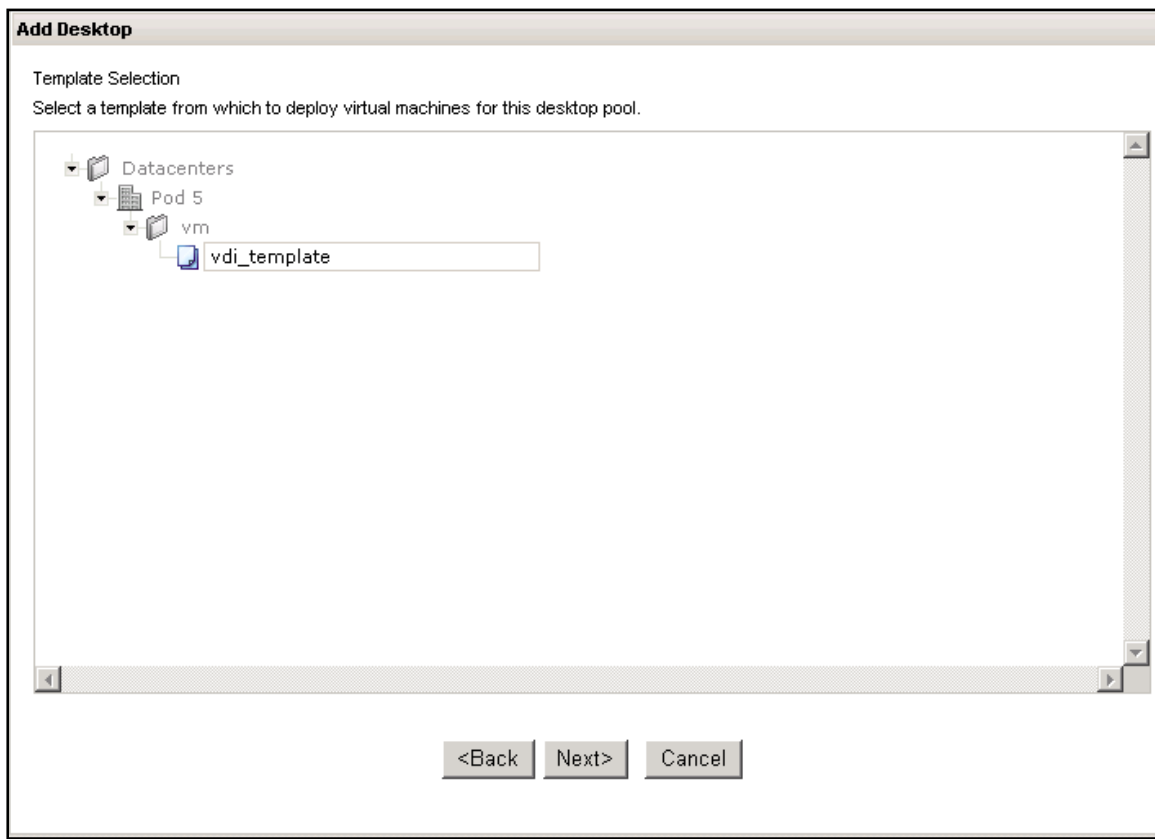
Select the VirtualCenter server to associate the pool with.



The screenshot shows a window titled "Add Desktop". Inside, the text "VirtualCenter Server" is followed by the instruction "Select the VirtualCenter server that will be used by this Desktop." Below this, there is a label "VirtualCenter Server:" and a dropdown menu showing "10.91.22.25". At the bottom, there are three buttons: "<Back", "Next>", and "Cancel".

Step 7:

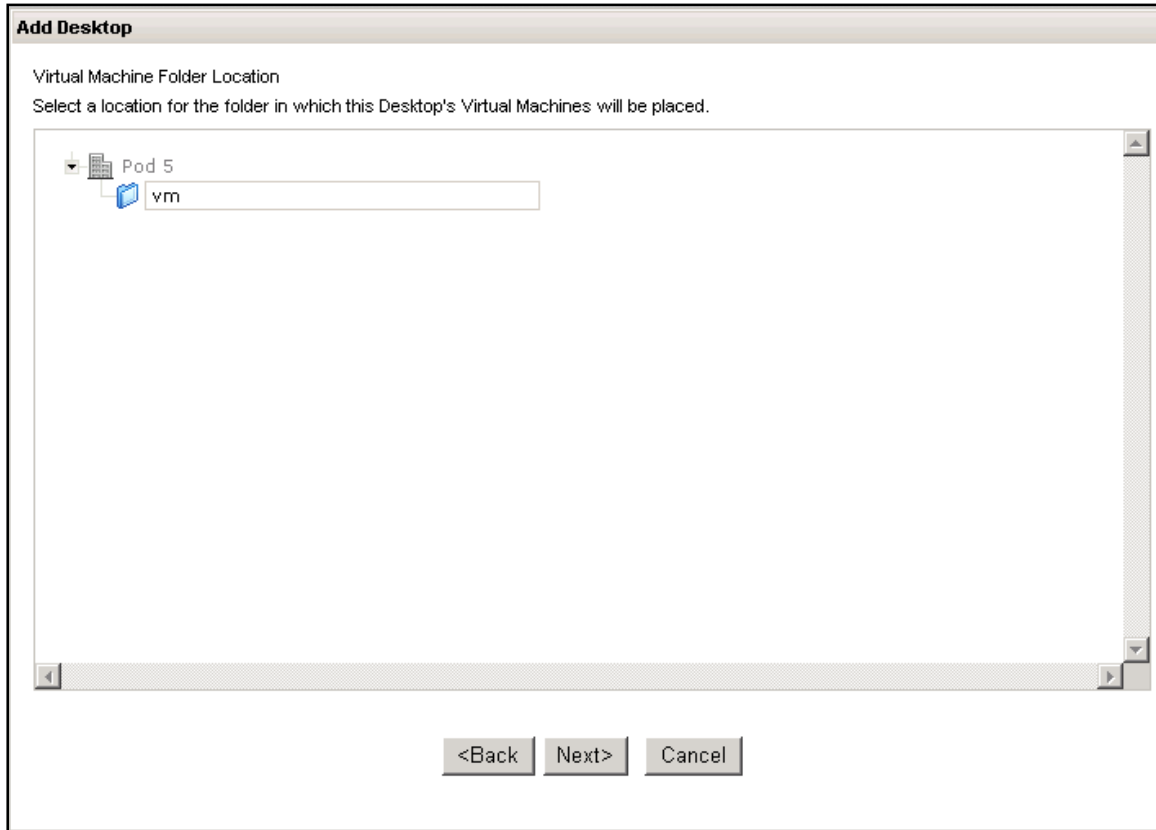
Select the template within VirtualCenter that will be used to deploy virtual machines within this pool.



The screenshot shows a window titled "Add Desktop". Inside, the text "Template Selection" is followed by the instruction "Select a template from which to deploy virtual machines for this desktop pool." Below this is a tree view showing a hierarchy: "Datacenters" (expanded) -> "Pod 5" (expanded) -> "vm" (expanded) -> "vdi_template" (selected). At the bottom, there are three buttons: "<Back", "Next>", and "Cancel".

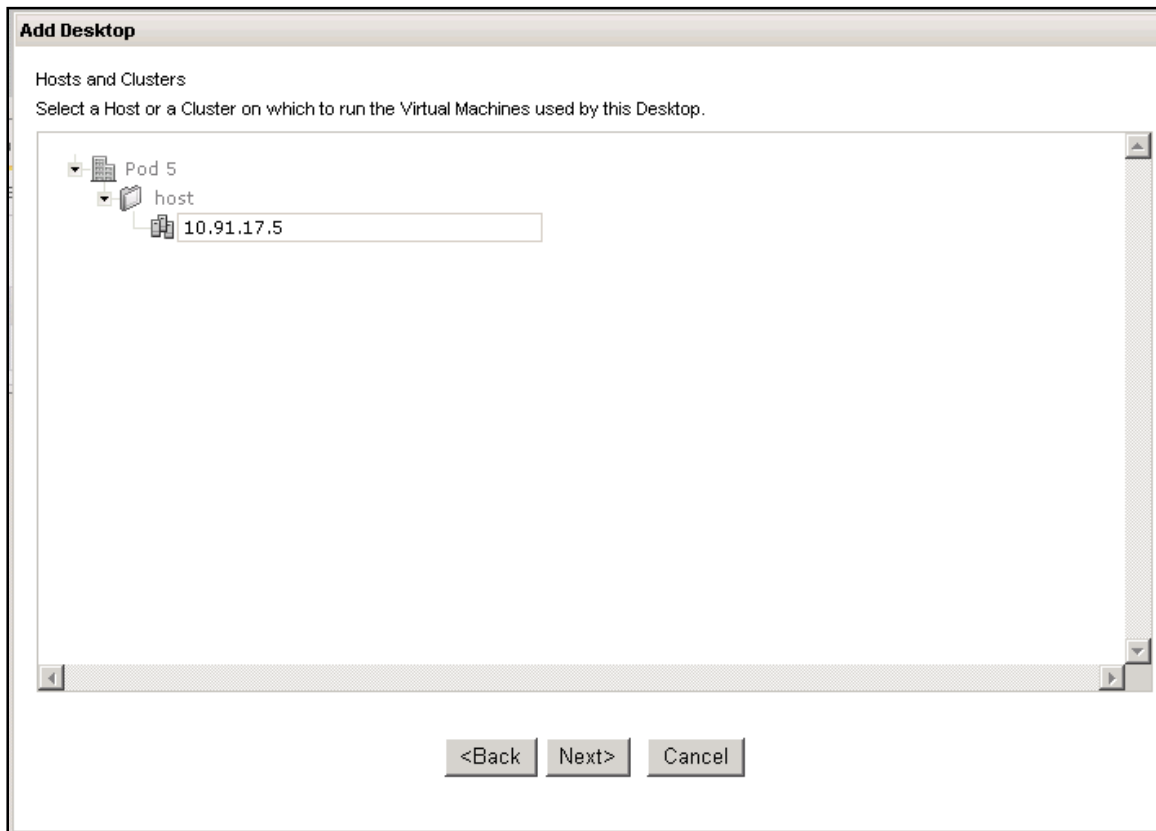
Step 8:

Select the VirtualCenter folder location that VMs will be reside in after being deployed from the template.



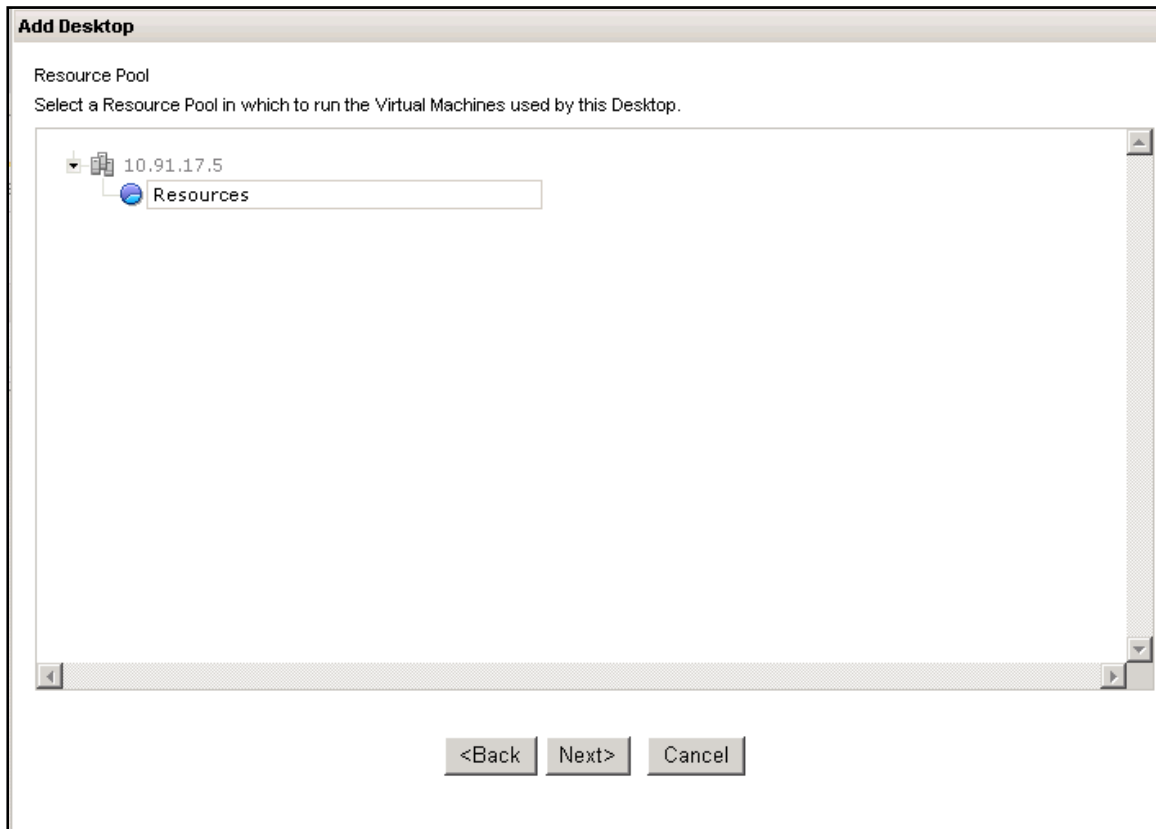
Step 9:

Select the host or cluster that the deployed VMs will reside on.



Step 10:

Select the resource pool that the new VMs will automatically be put into after being deployed.



Step 11:

Select the data store where the VM's files will reside. There can only be one datastore per pool.

Add Desktop

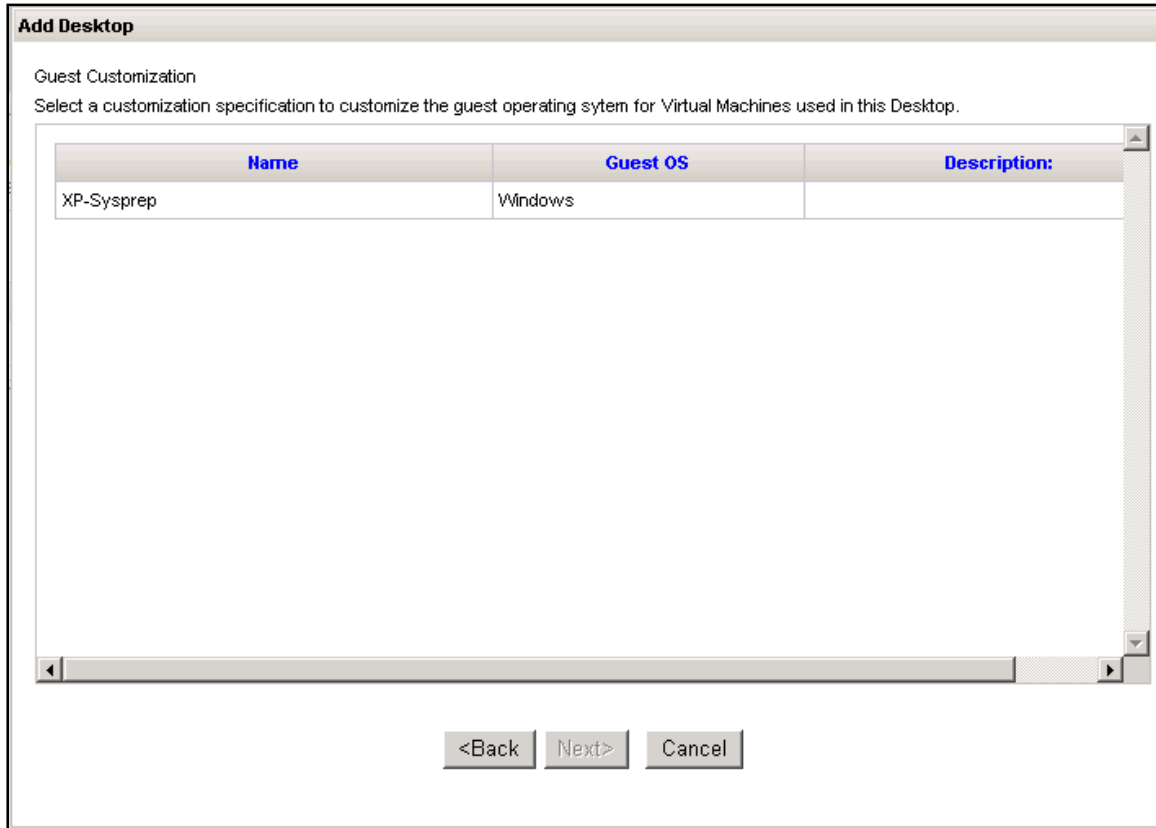
Datastore
Choose a Datastore to store the Virtual Machine files.

Name	Capacity (GB)	Free (GB)	Type	Access
vmw1-esx05	49.75	1.01	VMFS	Single host
storage1 (6)	60.75	47.88	VMFS	Single host

<Back Next> Cancel

Step 12:

Select the Guest Customization script to be run during the automatic sysprep of the template associated with the pool.



Step 13:

Complete the configuration of the pool.

Add Desktop




Ready to Complete
Please review the options you have selected before preceeding.



Desktop Type:	Persistent
Desktop ID:	Persistent-Pool1
Desktop Display Name:	Persistent Pool
Activation status:	Enabled
Minimum running VMs:	1
Maximum running VMs:	2
Number of spare VMs:	1
Control policy:	Remain on
DNS Suffix for VM names:	VDI
Prefix for VM names:	Persistent-Pool
VirtualCenter Server:	10.91.22.25
Template:	/Pod 5/vm/vdi_template
Virtual Machine Folder Location:	/Pod 5/vm
Host/Cluster:	/Pod 5/host/10.91.17.5
Resource Pool:	/Pod 5/host/10.91.17.5/Resources
Datastore:	/Pod 5/host/10.91.17.5/storage1 (6)
Customization specification:	XP-Sysprep-Nik

<Back Finish Cancel

Step 14:

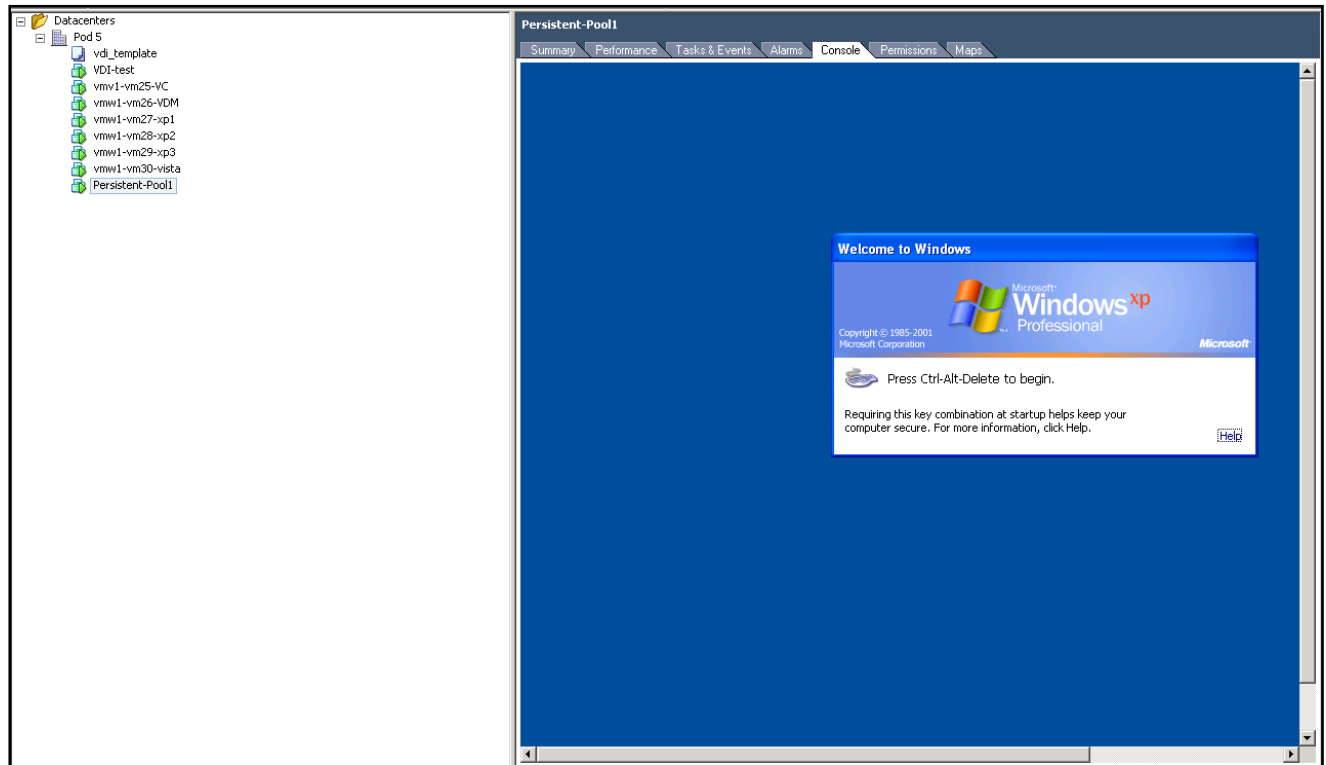
Confirm that VirtualCenter has started deploying the first machine in the pool.

Recent Tasks						
Name	Target	Status	Initiated by	Time	Start Time	Complete Time
 Clone Virtual Machine	 vdi_template	12% 	Administrator	8/23/2007 7:15:26 AM	8/23/2007 7:15:26 AM	

 Tasks  Alarms

Step 15:

After cloning a new VM, VirtualCenter will power on the new VM and the MS sysprep process will begin. Go to the console of this new VM to ensure that the sysprep process has been completed successfully.

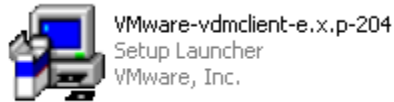


Installing the VDM 2.0 client

The following section of the guide will walk you through installing the VDM 2.0 client.

Step 1:

Launch the VDM Client installer.



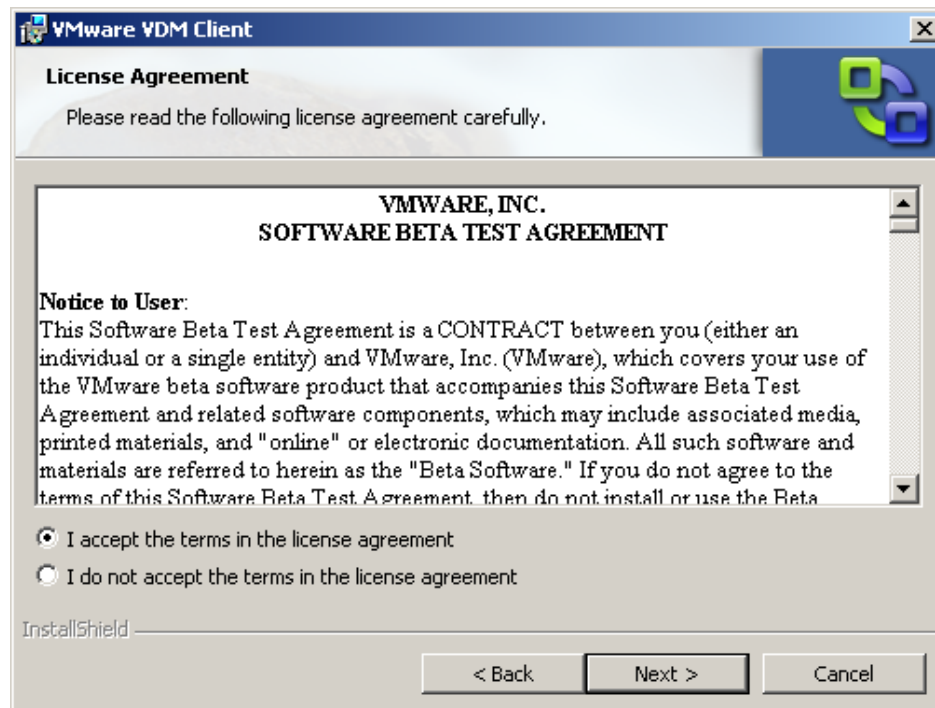
Step 2:

Click **Next** on the welcome screen



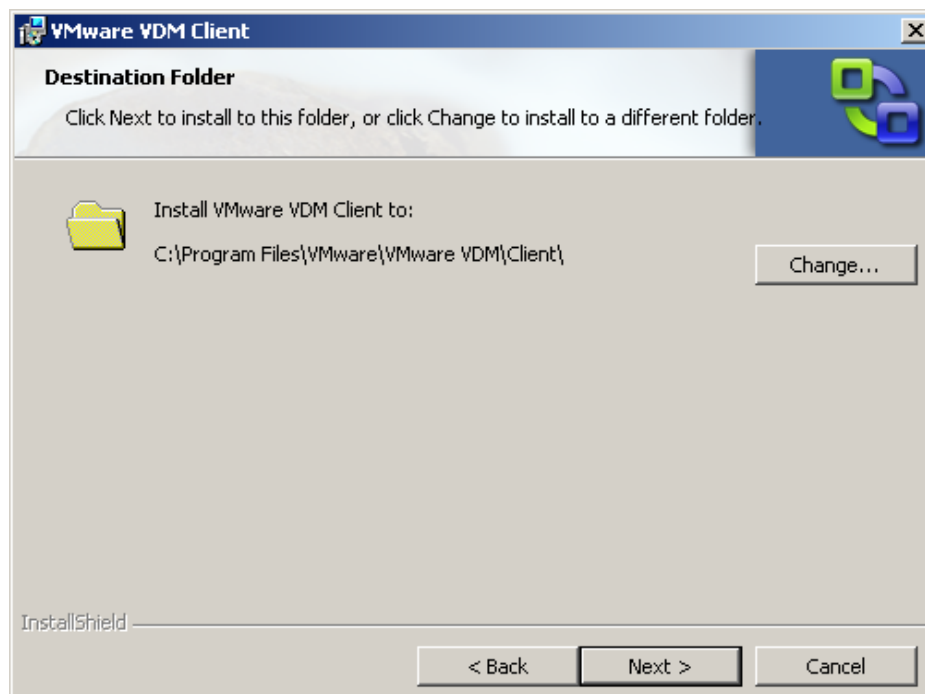
Step 3:

Accept the license terms and click **Next**



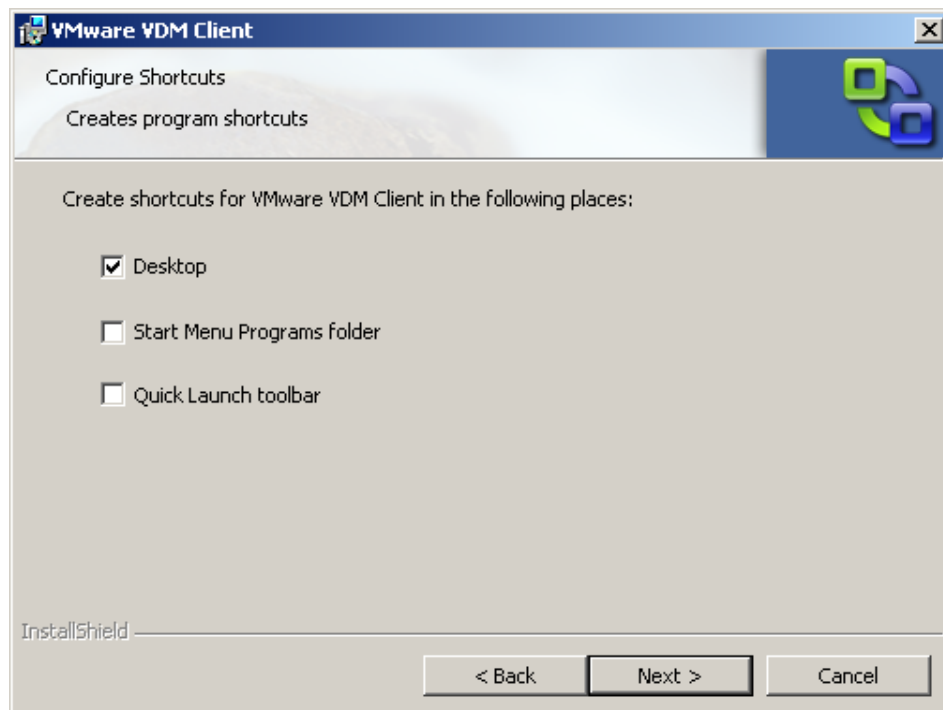
Step 4:

Accept the default destination and click **Next**



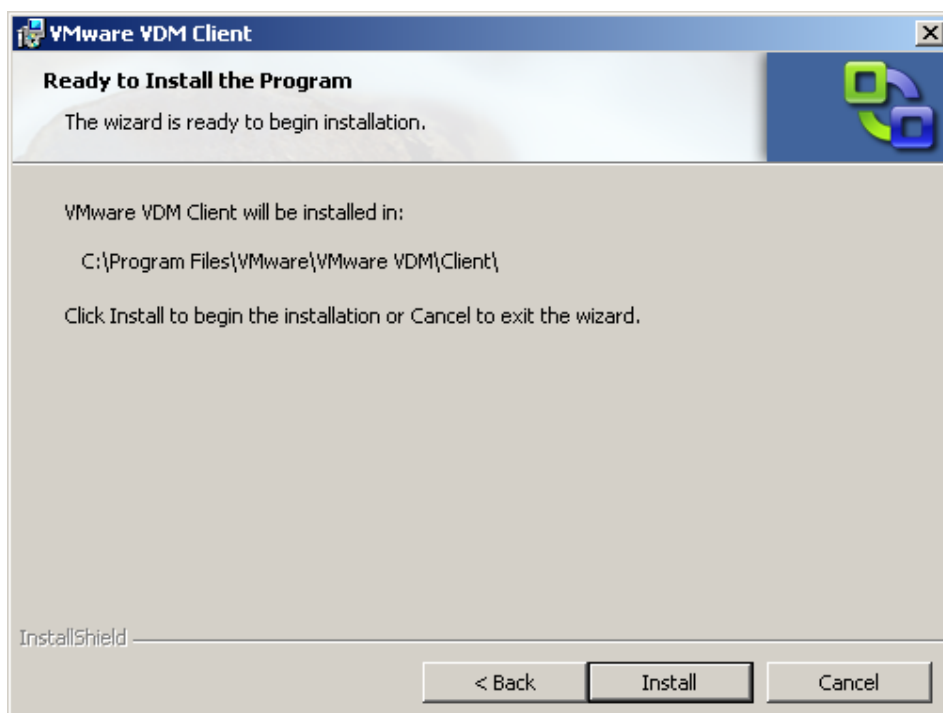
Step 5:

Choose the desired shortcuts and click **Next**



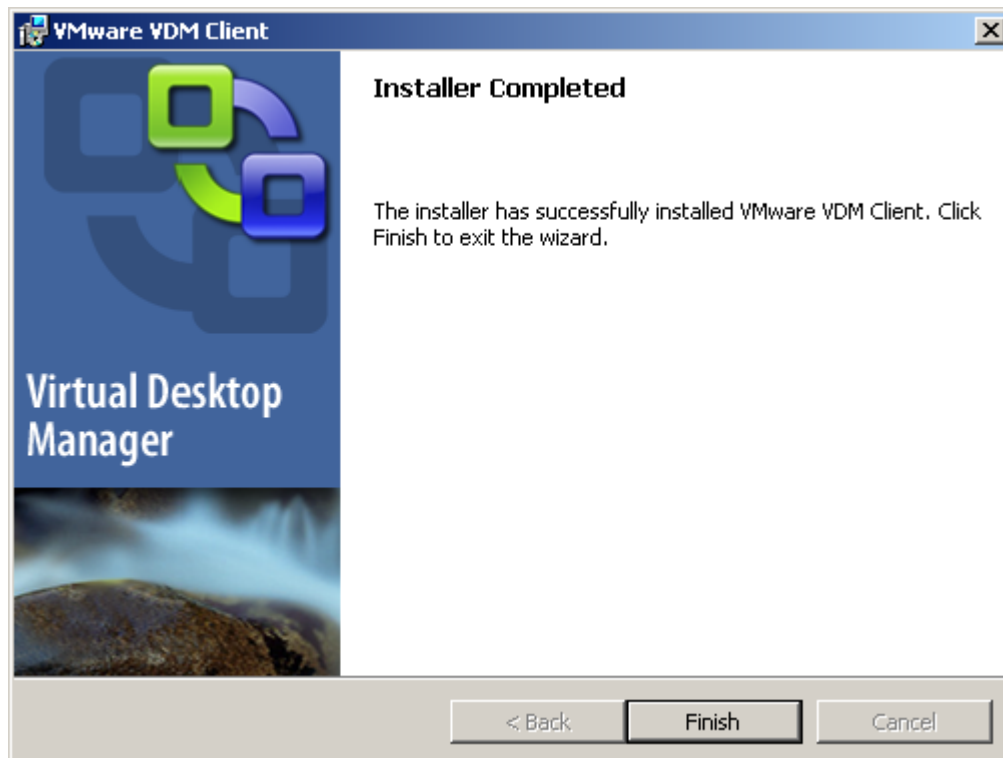
Step 6:

Installation is ready to begin, click **Next**



Step 7:

When the install completes, click **Next**

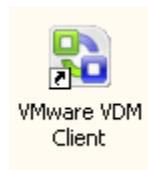


Connecting to a Desktop

The following section of the guide will walk you through connecting to one of the desktops you added earlier (either Static or Pools).

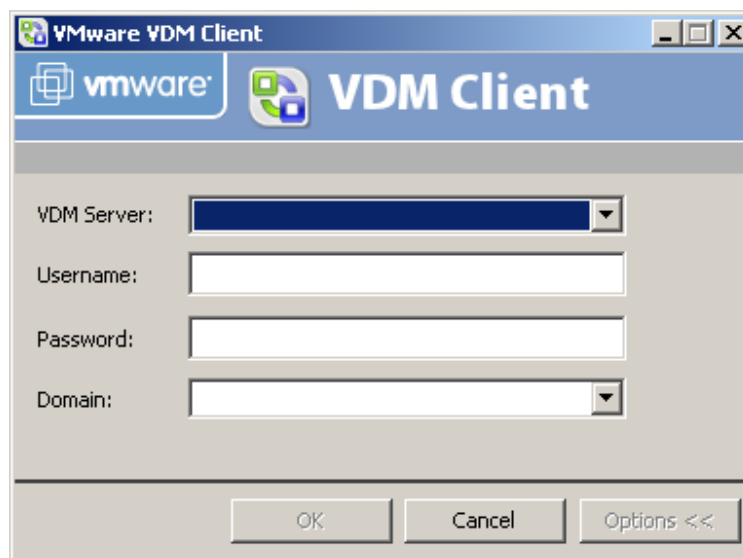
Step 1:

Launch the Client Connection by double clicking the shortcut on the desktop.



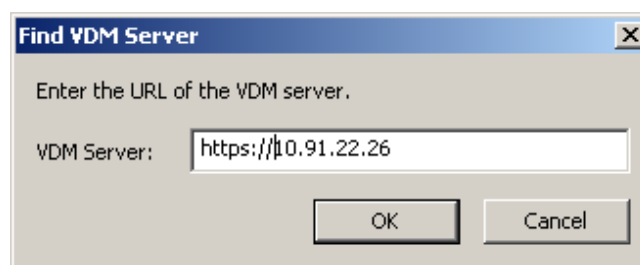
Step 2:

Click on the drop down to access the VDM Server entry field



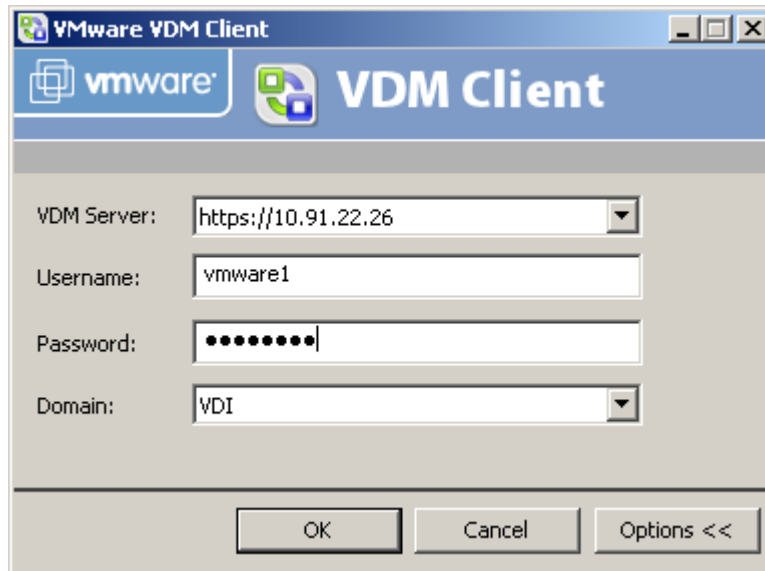
Step 3:

Enter the address of your VDM server. Note: If you are using SSL for the connection, then enter https:



Step 4:

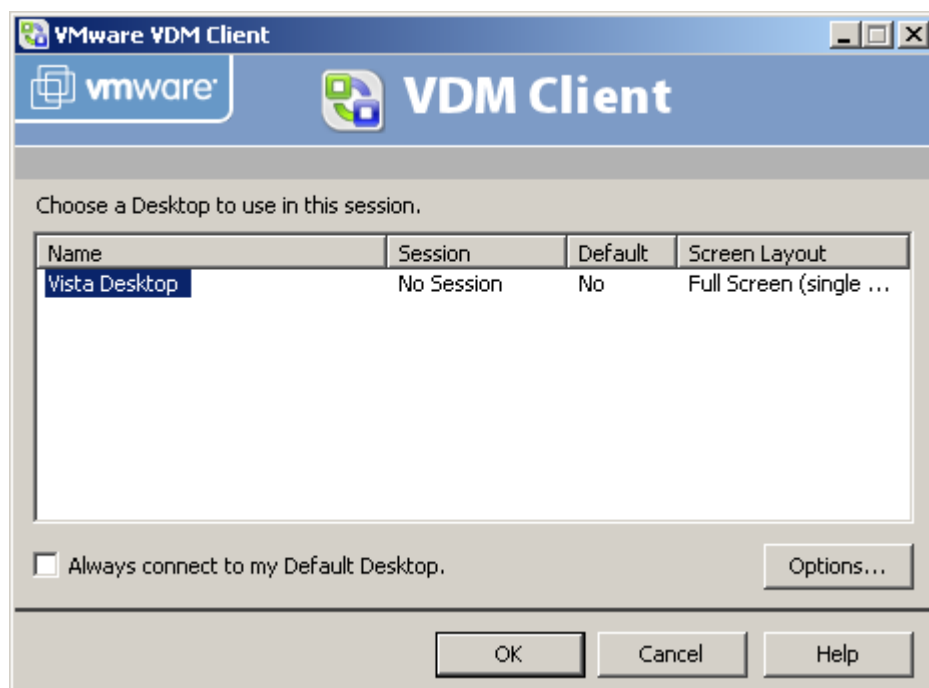
Enter your **Username**, **Password**, and **Domain**. Click **OK**



The VMware VDM Client login dialog box. It has a title bar with the VMware logo and 'VDM Client'. The main area contains four fields: 'VDM Server:' with a dropdown menu showing 'https://10.91.22.26', 'Username:' with a text box containing 'vmware1', 'Password:' with a masked text box (dots), and 'Domain:' with a dropdown menu showing 'VDI'. At the bottom are three buttons: 'OK', 'Cancel', and 'Options <<'.

Step 5:

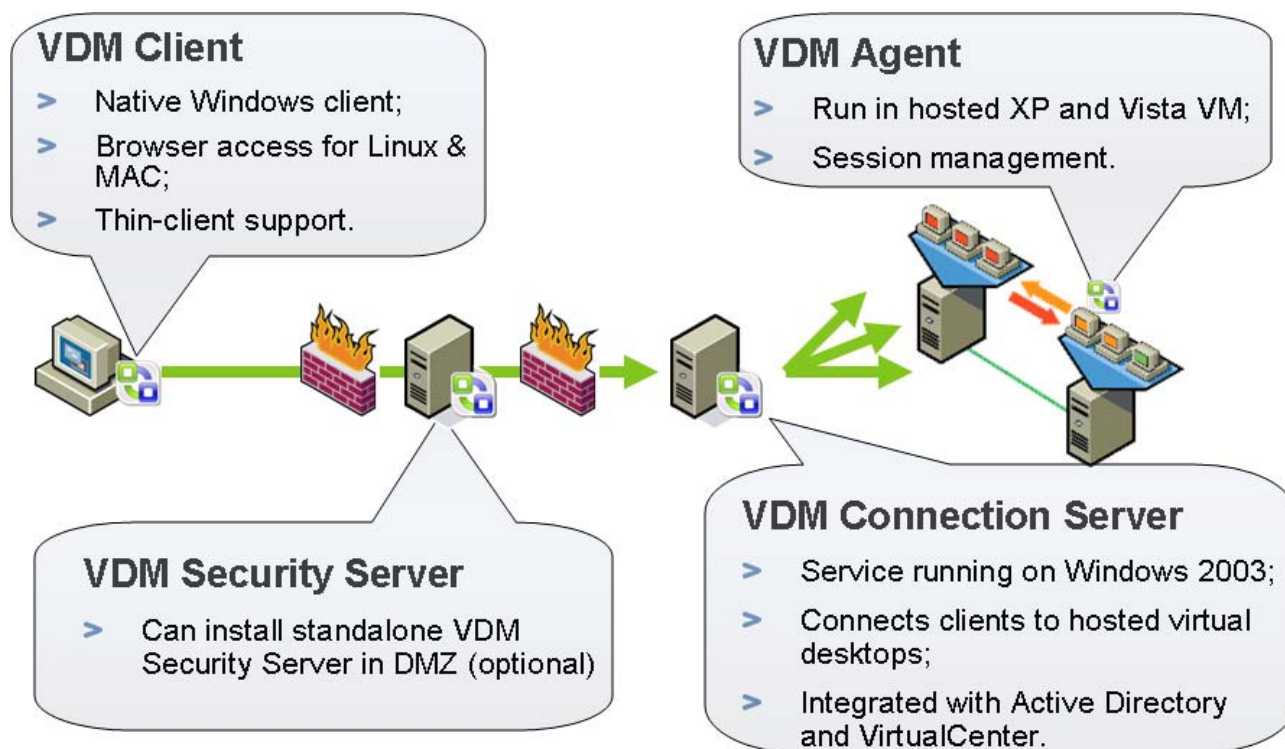
Select your desktop and Click **OK**



The VMware VDM Client desktop selection dialog box. It has a title bar with the VMware logo and 'VDM Client'. The main area contains the text 'Choose a Desktop to use in this session.' followed by a table with four columns: 'Name', 'Session', 'Default', and 'Screen Layout'. The table has one row with the values 'Vista Desktop', 'No Session', 'No', and 'Full Screen (single ...'. Below the table is a checkbox labeled 'Always connect to my Default Desktop.' and an 'Options...' button. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

Name	Session	Default	Screen Layout
Vista Desktop	No Session	No	Full Screen (single ...

The VMware VDM 2.0 Architecture



VDM Connection Server

The connection server is the component that brokers connections between VDM clients and VMs through desktop definitions. It also provides the admin console and web access for clients which don't have a native client. All configuration screens are part of the connection broker. This component runs on the Java enterprise application server Jboss (installed with the connection server), and interacts with guest agents running in the VMs being connected to, clients, and VirtualCenter servers.

All entitlements used in Virtual Desktop Manager 2.0 (authorization) are persisted in a directory. For Virtual Desktop Manager 2.0 ADAM (Active Directory Application Mode) is used as the directory server. Information like desktop definitions, virtual machines, and pools that are used in VDM and defined by the VDM administrator are stored in the directory. The connection server is configured to use the Active Directory for the domain of which it is a member for authentication and for retrieving list of users and groups. VDM-specific configuration is also persisted in the directory. Most components use standard LDAP/JNDI code to read/write data from the directory.

VDM Security Service

The security service provides the main point of contact for the environment; all web UI, native client control and SSL VPN traffic is routed via this component. Web UI and native client control traffic is forwarded to the broker component. This is the single point of integration for SSL and load balancing.

The Security Server also provides the SSL VPN functionality in the product. It is responsible for establishing a tunnel between the client machine and the server. The tunnel mediates all the traffic between the client and the desktop. This allows end users to have secure access to the desktop without being on the same network as the desktop running on the ESX Server. The tunnel is essentially a network conveyor that forwards all the RDP traffic from the client to the desktop and from the desktop to the client. The network connection from the client to the server is secured using SSL/TLS. The connection between the server and the desktop is not secured since it is limited by RDP support.

A connection server installation includes the security service. Additional security service instances can be placed in a DMZ to make a VDM installation internet-accessible.

VDM Agent

All guests run the VDM agent. This service enables guest-based features such as RDP connection monitoring (user connected, user disconnected, etc), remote USB support (access to some client-connected USB devices in the guest), and Single Sign-on (secure single sign-on to the guest without sending the user password in clear text).

VDM Client

The client component is installed on the end user's machine where it is running a supported OS. It is a Windows application that allows the user to connect directly to the desktop without going through the web interface. After logging in users are presented with a list of desktops, and connect to and disconnect from one or more desktops.

Authentication

This section describes the LDAP authentication mechanisms available with ADAM. Most, if not all ADAM authentication is handled by WinAuth mechanisms in Virtual Desktop Manager. This authenticates to ADAM which uses Windows authentication mechanisms in conjunction with AD.

Simple Bind

ADAM supports conventional LDAP simple binds over LDAP and LDAPS.

In addition to being able to perform a simple LDAP bind to ADAM using user DN (e.g. cn=admin,ou=people,dc=workspace,dc=int) and password, it is also possible to bind to ADAM using a userPrincipalName (instead of DN) and password. e.g. admin@workSpace.int. For this, the userEntry requires a userPrincipalName attribute. This can be useful when using the generic Java LDAP Browser/Editor or when using non Microsoft tools with LDAP.

ADAM also supports LDAP SASL binds. This is used to bind as a windows user. The ADAM Management tools allow the user to specify simple binds or the ability to bind as a windows user. In the case of a Windows user the tools have the option to specify a user, domain and password or to log on as the existing logged on user without specifying any credentials.

When binding to ADAM as a Windows user, there are two choices:

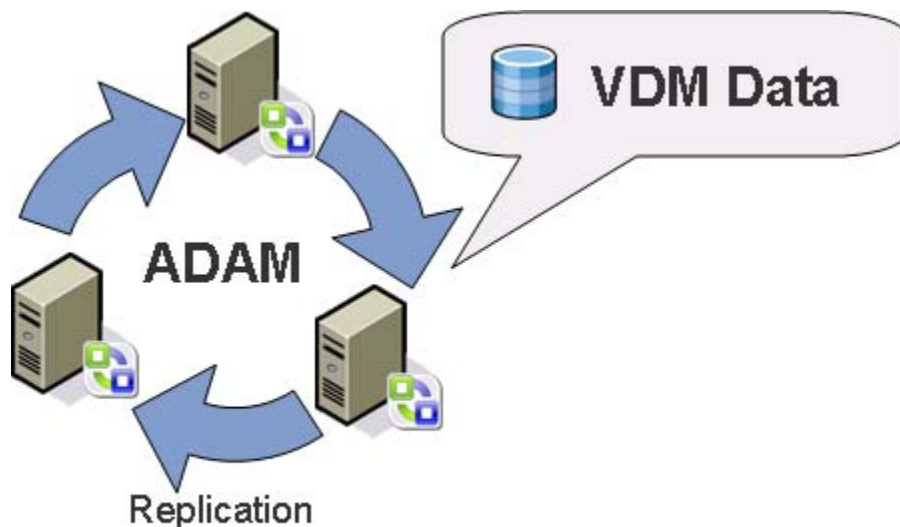
Bind as the currently logged-on user without needing to specify a password.

Bind specifying the Username, password and domain name.

Replication

ADAM supports multi-master LDAP replication and uses optimized techniques for replication on high-speed LAN located ADAM servers. ADAM also supports site-to-site replication over a WAN.

ADAM intrasite (LAN) replication uses bidirectional ring topology to minimize replication connections.



The standard deployment scenario for ADAM is to deploy a first (primary) ADAM server with its own configuration set. Subsequent ADAM servers can then be installed to use the configuration set of the primary. This logical grouping of ADAM servers is called a *configuration set*. ADAM servers within a configuration set perform replication between each other so that LDAP writes on any one ADAM server is replicated automatically to all the others within a configuration set.

High availability and failover in VDM 2.0

The components are installed as 1 discreet service (i.e. NT system service) on each server machine running 4 processes:

Security Server

Connection Server

VDI Directory Services (i.e. ADAM)

VDI Message router (Swiftmq)

All three of these services, when installed on a single machine, will be configure to communicate with the corresponding local services - i.e. the SSL Gateway will

communicate with the local Connection Broker on 127.0.0.1, and similarly, the Connection Broker will use the local ADAM.

ADAM replication between the instances in a multi-server installation will ensure configuration information is current. The JMS system swiftmq uses a multicast system to join all the routers together as a cluster, and the JMS libraries take care of locating an instance to use (any instance works as the routers route messages between themselves).

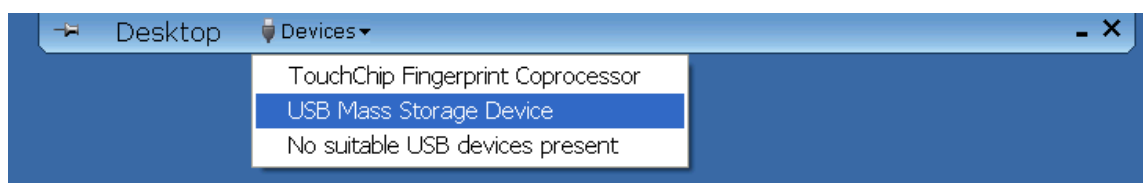
To enable a 3rd party web load balancer to make a level 7 decision about which instance to use, a deep-probe capability will be built into the login page so that the load balancers can tell if the complete stack is functional or not on a particular server. The deep probe page will also return a list of VDI servers that it is believed are also functioning.

The configuration of the SSL Gateway when in a DMZ is slightly different - the SSL gateway will use JMS to decide which Connection Broker to direct traffic to. However, an alternate mechanism could be simply to have an SSL gateway configured to just one Connection Broker server, and the deep-probe load balancing method used here also.

The native client will use the information in either DNS or the login page to maintain a list of servers that exist, and so are able to fail over to a second one if required. This allows an HA experience without using a web load balancer.

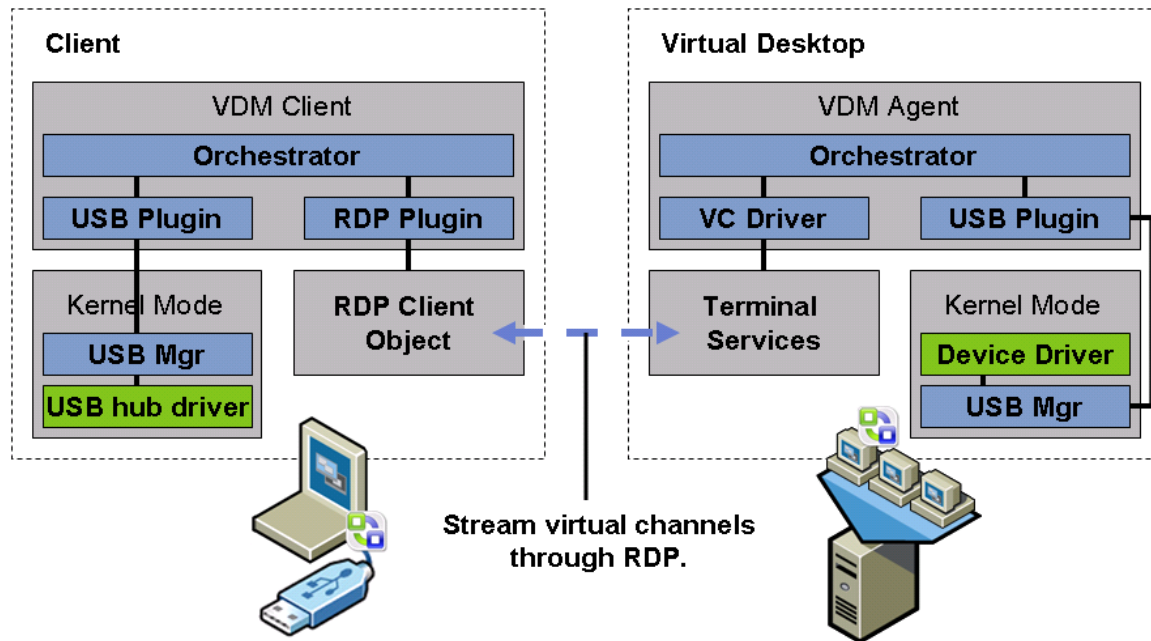
USB Support with Virtual Desktop Manager

Virtual Desktop Manager allows users to connect USB devices to their local client access device and have them available during their session. The user clicks on **“Devices”** and the drop down window appears where they can choose which device they would like to make available for their session.



The VDM Client and VDM Agent have a ‘plug-in’ framework controlled by an internal ‘orchestrator’. This is a flexible and highly extensible framework, which has been used to support redirection between applications running in virtual desktops to devices attached to the client by USB (1.1 and/or 2.0). This solution is architected to support generic USB device although in practice it is not possible to support ‘any’ USB device due to the size of the test and QA matrix. For the list of devices officially supported in the VDM 2.0 release consult product management. VDM 2.0 is able to support USB redirection by handling communication between the USB hub driver installed on the client and specific device drivers installed in the virtual desktop. The communications are directed

channeled through 'virtual channels' in the RDP data stream, using native terminal-services APIs. The VDM Client is exposed to the devices attached to the client and presents the user with the option to connect (pass through the communication) or disconnect (block the communication) between the device to the virtual desktop.

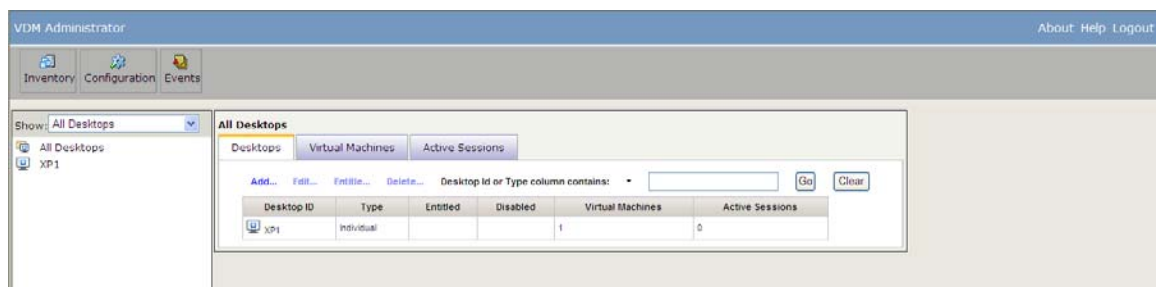


Using Entitlements within VDM 2.0 Connection Broker

The following section of the guide will walk you through the Entitlement functionality found within the VDM 2.0 connection broker.

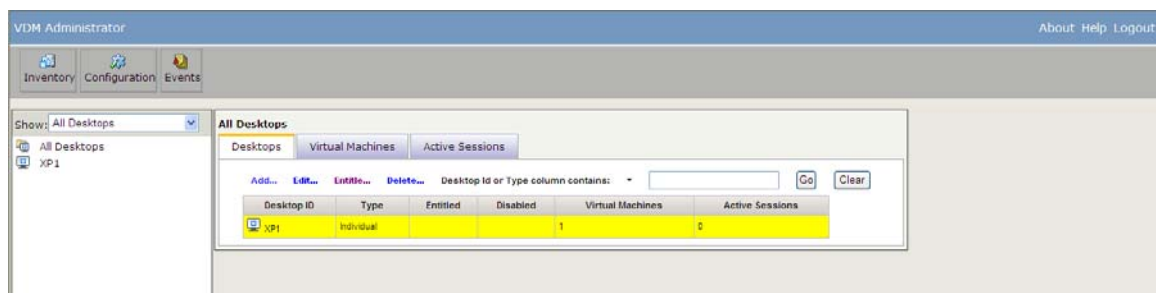
Step 1:

Click on **Inventory** button at the top left hand corner. Displayed is the Inventory available from this VDM Connection Server.



Step 2:

Click the Desktop ID XP1 to highlight it.



Step 3:

Click on the **Entitle...** option.

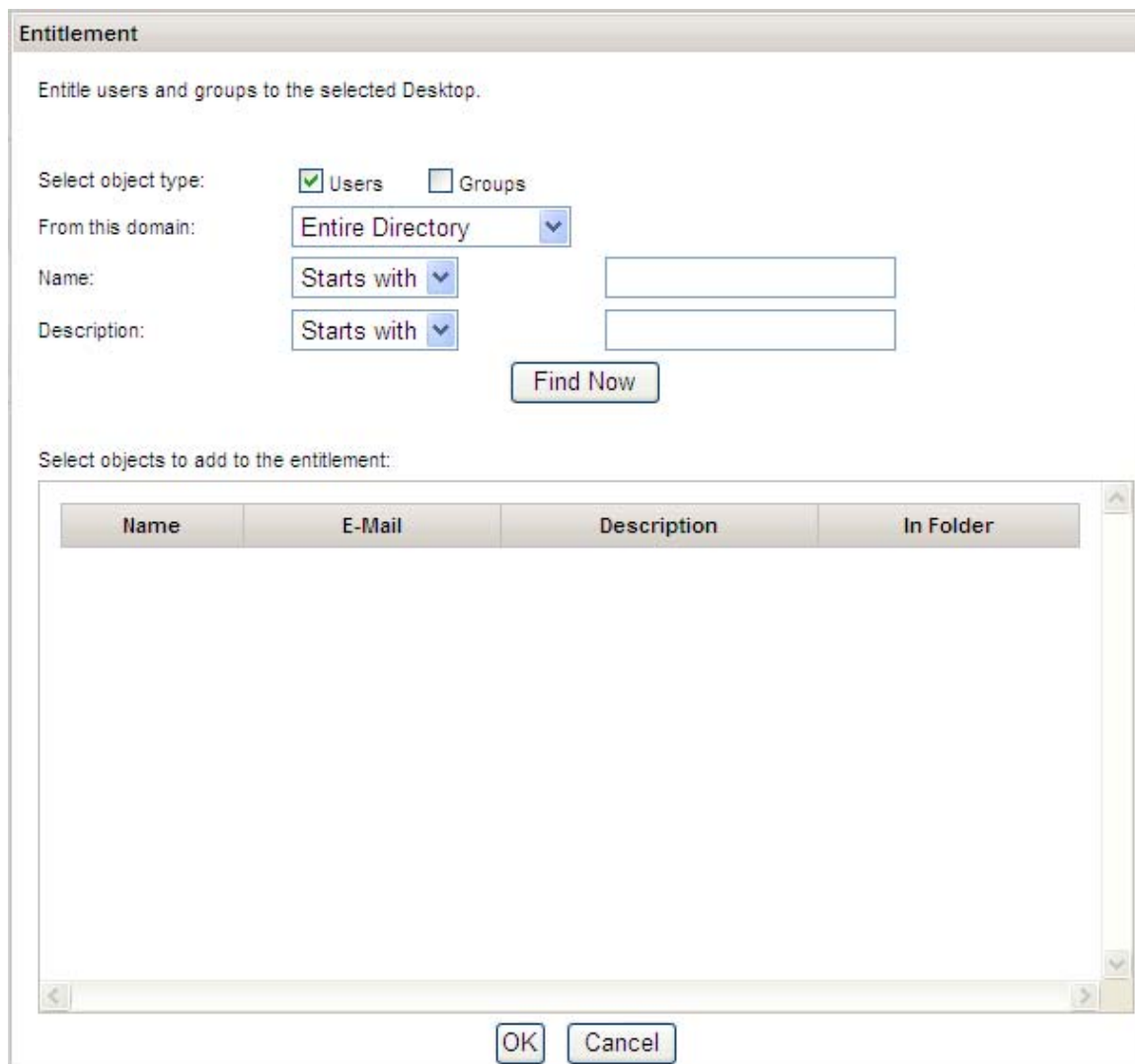
This displays an interface that allows you to Add or Remove users or groups and their entitlement to desktop virtual machines.



Step 4:

Click on **Add**

From the Entitlement interface you are able to entitle users and groups to selected desktops that have previously been made available in your VDM Connection Server.



The 'Entitlement' dialog box is used to assign users and groups to a selected desktop. It includes a title bar, a description, and several input fields for filtering search results. Below the search fields is a 'Find Now' button. At the bottom, there is a table to select objects for entitlement, with columns for Name, E-Mail, Description, and In Folder. The dialog concludes with 'OK' and 'Cancel' buttons.

Entitlement

Entitle users and groups to the selected Desktop.

Select object type: ☒ Users ☐ Groups

From this domain: Entire Directory ▼

Name: Starts with ▼

Description: Starts with ▼

Find Now

Select objects to add to the entitlement:

Name	E-Mail	Description	In Folder
------	--------	-------------	-----------

OK Cancel

Step 5:

Type **vmware** in the space next to Name: Starts with

Entitlement

Entitle users and groups to the selected Desktop.

Select object type: ☒ Users ☐ Groups

From this domain: Entire Directory

Name: Starts with vmware

Description: Starts with

Find Now

Select objects to add to the entitlement:

Name	E-Mail	Description	In Folder
------	--------	-------------	-----------

OK Cancel

Step 6:

Click **Find Now**

Displayed are the users that have matched our search criteria.

Entitlement

Entitle users and groups to the selected Desktop.

Select object type: ☒ Users ☐ Groups

From this domain: Entire Directory ▼

Name: Starts with ▼ vmware

Description: Starts with ▼

Find Now

Select objects to add to the entitlement:

Name	E-Mail	Description	In Folder
vmware1		password=vmware_1	vdi.vmworld2007.com/Users

OK Cancel

Step 7:

Click on the user with name **vmware1**, this will highlight the selection.

The dialog box is titled "Entitlement" and contains the following elements:

- Instruction: "Entitle users and groups to the selected Desktop."
- Search criteria section:
 - "Select object type:" with checkboxes for ☒ Users and ☐ Groups.
 - "From this domain:" with a dropdown menu set to "Entire Directory".
 - "Name:" with a dropdown menu set to "Starts with" and a text input field containing "vmware".
 - "Description:" with a dropdown menu set to "Starts with" and an empty text input field.
 - A "Find Now" button.
- Results section:
 - Label: "Select objects to add to the entitlement:"
 - A table with the following data:

Name	E-Mail	Description	In Folder
vmware1		password=vmware_1	vdi.vmworld2007.com/Users
- Buttons: "OK" and "Cancel" at the bottom.

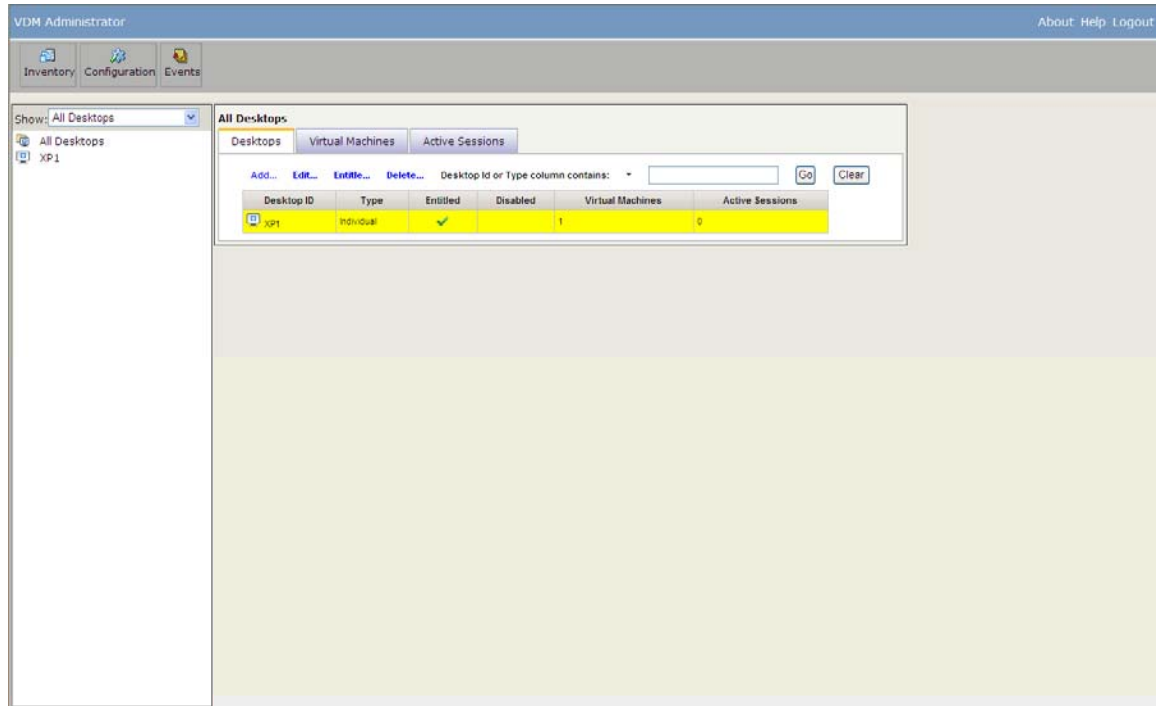
Step 8:

Click **OK**



Step 9:

Click **OK**. The result is now the Desktop ID XP1 has a checkmark in the Entitled column. The entitlement has been defined.



Appendix

Let's go through creating a Windows VM for VDI use. Remember this VM will be used over and over again. It is important to get the image small and optimized. Don't try to rush this process. There are many, many things you can do to customize the desktop for your environment. This is just a sampling to get you started.

1.) Build a Windows XP Professional VM

You should connect to this VM via VC Console because some options won't be available through a terminal Services (RDP) session.

2.) Virtual Machine Systems changes:

Ensure that floppy drive (if present) is not connected at startup

Ensure that cd-rom drive (if present) is not connected at startup

3.) Windows XP Changes:

Ensure SP2 + applicable updates are applied

Install VM Tools

Sync time from host

Disable Windows time update

By default Windows XP sends 16 bit color over Terminal Services. If you want to enable 24 bit color you need to modify a local machine policy.

local computer policy editor, go to Local Computer Policy

Computer Configuration

Administrative Templates

Windows Components

Terminal Services

Then click on the Limit maximum color depth policy. Enable, set to 24 bit, and click on OK.

Restart your RDP session and you will be able to use 24 bit color

It's still not as nice as RGS, but at least the colors will be smoother. J

Disable COM1 & COM2

Right-click My Computer -> Select Manage
Device Manager

Turn off all theme enhancements

Right-click My Computer -> Select Properties
Choose the Advanced Tab
Under Performance Section Choose Settings
Choose Adjust for Best Performance
Optionally choose settings like font smoothing if desired

Disable all screensavers except Blank password protected

Copy the scrnsvr.scr over the top of all the others (because windows has a habit of bringing them back if you delete them). Once you do this, you should enable the only screensaver that will show up which is the Blank/Password Protected.

Delete all background wallpapers

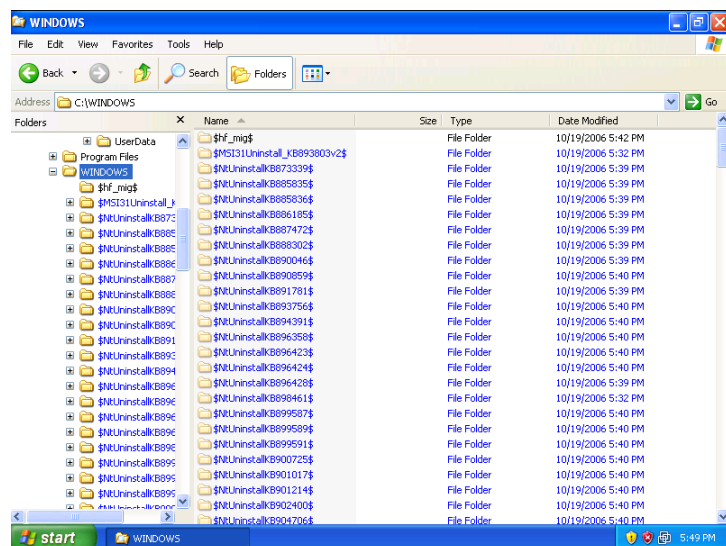
Why waste RAM or disk space on wallpapers that will be covered by an application anyway

Ensure full hardware acceleration

Control Panel -> Display -> Settings Tab -> Advanced Button
Troubleshooting Tab -> Set acceleration to full (that way by default, but check to make sure it hasn't changed in some latest Microsoft Update)

Delete all the hidden update folders (this uses a lot of space and no one is going to uninstall any of those updates). Leave the one that looks like \$hf_mig\$.

Using VMware Virtual Desktop Infrastructure for Hosted Computing



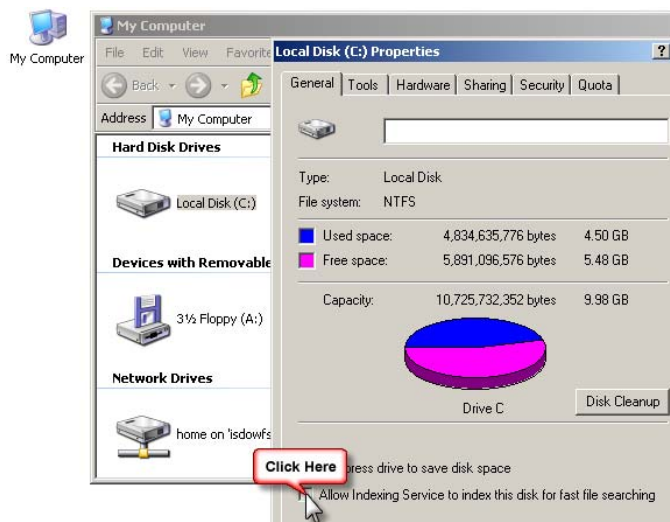
Disable Indexing Services

Indexing Services uses large amounts of RAM. It enables faster searches by scanning the indexed lists. However, indexing typically uses lots of CPU time and if the user doesn't search their computer often, indexing won't help them at all. If they do search frequently, indexing may not make the searches faster.

Go to Start/Control Panel/Add Remove Windows Components

Uncheck the Indexing services

Disable it on the C: drive also



Disable Paging of the executive

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
DisablePagingExecutive=dword:00000001

Create and publish a GPO for folder redirection to the users' storage space on the SAN for the following:

Application Data

My Documents (and all sub-class special folders)

My Desktop

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;232692>

Optimize the Paging File

Right-click My Computer -> Select Properties

Choose the Advanced Tab

Under Performance Section Choose Settings

Click Change. Select the Custom Size option and set the Initial Size and Maximum Size to 512 MB or the exact size of the configured RAM (whichever is greater).

Turn off unnecessary sounds (ie Startup and Shutdown wav's)

Control Panel, double-click Sounds and Audio Devices and move to the sounds tab

Disable unnecessary sounds (mail notification and warnings are probably the only ones you need)

Defragment Prefetch (faster booting)

From DOS Prompt type defrag c: -b

Do NOT clean out the Prefetch directory however

It is a bad idea to periodically clean out that folder as some tech sites suggest. For one thing, XP will just re-create that data anyways; secondly, it trims the files anyways if there's ever more than 128 of them so that it doesn't needlessly consume space. So not only is deleting the directory totally unnecessary, but you're also putting a temporary dent in your PC's performance.

Remove or minimize System restore points

Right-click My Computer, select Properties and go to the System Restore tab.

Remove blinking ICONS from the systrey

Remove the display of icons like the NIC that blink

Alternatively you can hide all ICONS by

Modifying

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.
In the right-hand pane create a new DWORD value called NoTrayItemsDisplay and set its value to 1.

Get Rid of Microsoft Messenger

Edit C:\WINDOWS\INF\SYSOC.INF file

Under the [Components] heading, you'll see a whole bunch of parameters for various Windows applets. Some of them contain the word hide. Those particular programs, which include Windows Messenger (msmsgs), Terminal Server, Pinball, and others, are installed on your XP system, but their entries are hidden from and Add/Remove dialog

Remove the hide from the lines of the programs you wish to remove

Msmgs=msgrocm.dll,OcEntry,msmsgs.inf,hide,7

Save the file

Go to Control Panel Add/Remove Programs

Click on Windows Components button and you'll see Windows Messenger listed.
Uncheck it and click Next

Turn off Disk Performance Counters

In Windows XP Performance Monitor disk counters for physical disks are turned on by default

Stop it by running: DISKPERF -N

Disable any unwanted services

Autoruns from www.sysinternals.com is good for this

Run Disk Cleanup

Double Click My Computer

Right Click C:, properties

Run Disk Defrag

Double Click My Computer

Right Click C:, properties

Run PageDefrag from sysinternals

One of the limitations of the Windows NT/2000 defragmentation interface is that it is not possible to defragment files that are open for exclusive access. Thus, standard defragmentation programs can neither show you how fragmented your paging files or Registry hives are, nor defragment them. Paging and Registry file fragmentation can be one of the leading causes of performance degradation related to file fragmentation in a system.

PageDefrag uses advanced techniques to provide you what commercial defragmenters cannot: the ability for you to see how fragmented your paging files and Registry hives are, and to defragment them. In addition, it defragments event log files and Windows 2000/XP hibernation files (where system memory is saved when you hibernate a laptop).

PageDefrag works on Windows NT 4.0, Windows 2000, Windows XP, and Server 2003.

Download from www.microsoft.com/technet/sysinternals/FileAndDisk/PageDefrag.msp

Save your work to this point as a new template

Install Necessary Software

Repeat the above 5 steps

4) Clone

Now that you have a good template, create clones to work from.

Miscellaneous Information

Large Monitor Support:

You can use an RDP6 client with the /span command line option to enable large display size and use SplitView software to get a multi monitor feel.

Logon problems

For a user to log on to a Terminal Server, the following permissions and rights must be granted:

2003 and Windows XP only: **Allow log on through Terminal Services**

This right is by default granted to Administrators and members of the local Remote Desktop Users group on the server.

W2K only: **Log On Locally**

This right can be granted in the security policy for the server, in Security Settings\Local Policies\User Rights Assignment\Log On Locally.

Permission to use the rdp-tcp connection

2003: The local Remote Desktop Users group has by default User access permission on the rdp-tcp connection.

W2K: The local Users group has by default User access permission on the rdp-tcp connection.

Allow logon to Terminal Server checkbox, in the properties of the user account in AD. By default, this checkbox is checked for all users.

So on standard installations of a 2003 or Windows XP Virtual Desktop, you only have to add your users or user groups to the local Remote Desktop Users group on the local machine.

Error messages - permission problems

Here are some common error messages which users get when they haven't been granted the correct permissions and user rights:

The local policy of this system does not permit you to logon interactively

2003 and Windows XP: The user account is not a member of the local Remote Desktop Users group. See 289289

W2K: The user does not have the Log On Locally right in the servers security policy.

You do not have access to logon to this session

2003 and Windows XP: The user account is not a member of the local Remote Desktop Users group.

W2K: The user doesn't have the necessary permissions on the rdp-tcp connection. This happens when you remove the User group from the properties of RDP-tcp

Your interactive logon privilege has been disabled

The user does not have the Allow Logon to terminal server check box selected on the Terminal Services Profile tab of their account.

Untested for later use:

1) Remove all of the driver cab files. Our VM hardware is already installed so we won't need to autodetect any other hardware. It is in %windows%/driver cache. (82 MB savings)

2) We will never use a modem inside of a VM, so remove all the modem driver description files from search for mdm*.inf in %windows% and free up a few megabytes.

VMWORLD 2007

© 2007 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,961,941, 6,961,806, 6,944,699, 7,069,413; 7,082,598 and 7,089,377; patents pending.

VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.