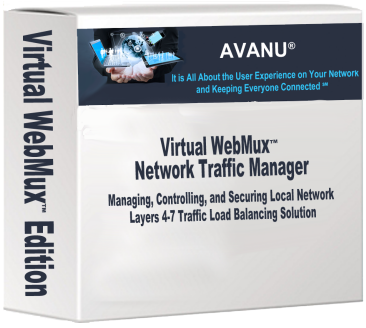
Virtual WebMux™

Network Traffic Manager



Virtual WebMux Installation on VMware® ESXi

www.avanu.com

Virtual WebMux Installation on VMware ESXi

vSphere Clinet GUI Method with VMX / VMDX Files

Summary

These instructions walk you through installing a virtual Web Mux on a VMware ESXi server using the vSphere graphical user interface. There are other guides as examples using command-line options.

Contents

Download a Virtual WebMux from AVANU

These instructions are for VMware users who wish to have "VMX" and ".VMDX" files instead of OVA files. Please see the separate instructions for using OVA files at the AVANU Virtual WebMux page. You have the option to download a **FREE** time-limited version or download the licensed version if you have made a purchase.

FREE 30-Day Trial Download

Register for a non-production demonstration limited license and you will receive an e-mail containing a link to download your demonstration. Here is the link for a time-limited version:

https://avanu.com/virtual-webmux-appliance-request/

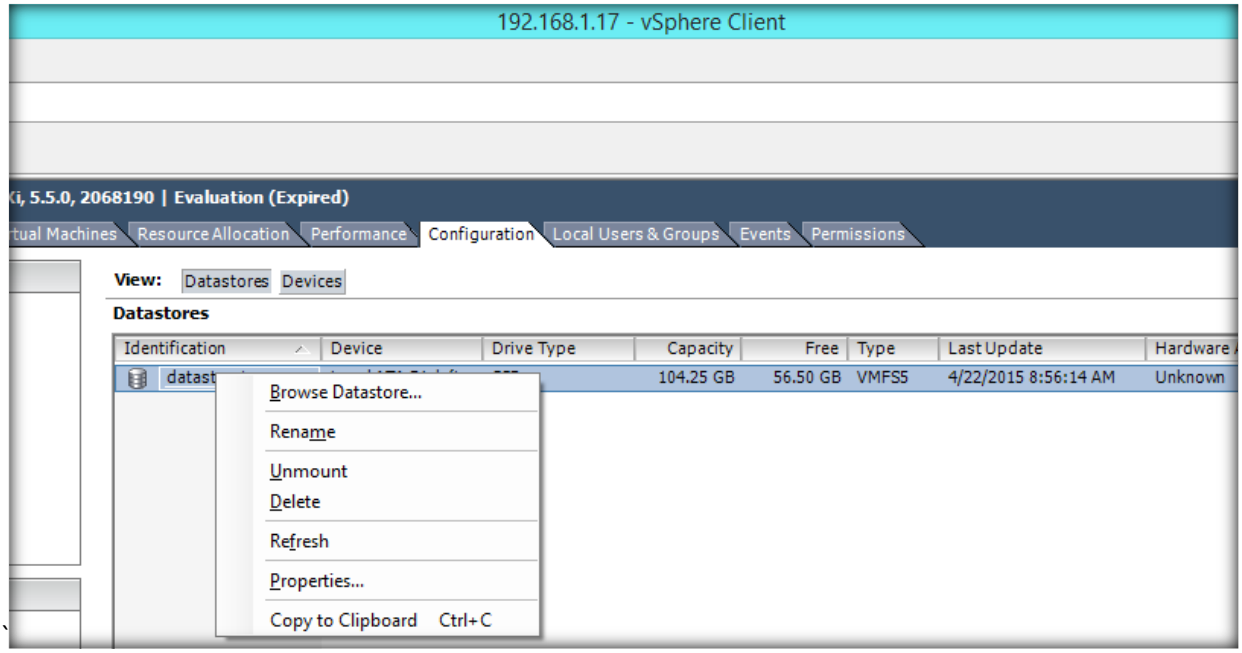
Then, once you have received the e-mailed response, follow the link that you receive via e-mail and download the files to your workstation. You will get a link to download two files, a ".VMX" file and a ".VMDX" file. Take note of the location that you put the files and proceed to the installation instructions.

Unlimited-Time Licensed Product Download

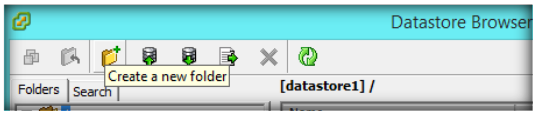
Once you have purchased a full time-unlimited license to the virtual machine you simply follow the download link to get the two files, one a ".VMDX" file and the other a ".VMX" file. They will be named with their serial number, such as "VX-100XAA0A3.vmdx" and "VX-100XAA0A3.vmx."

vSphere Client Installation of the Virtual WebMux

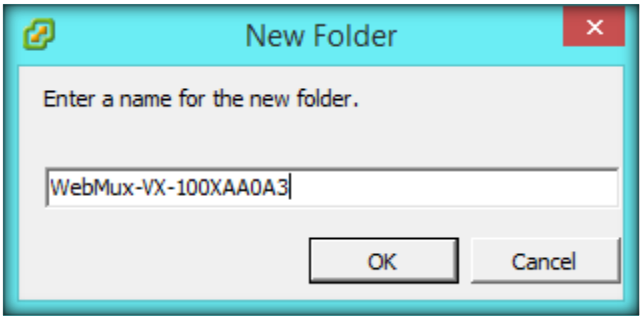
Connect to your ESXi server via your vSphere client, click on the VM on which you wish to install the WebMux, click on the **Configuration** tab, and right-click on the datastore where the WebMux will be installed. Choose "**Browse Datastore**."



Create a New Folder



Click on the “New Folder” icon.

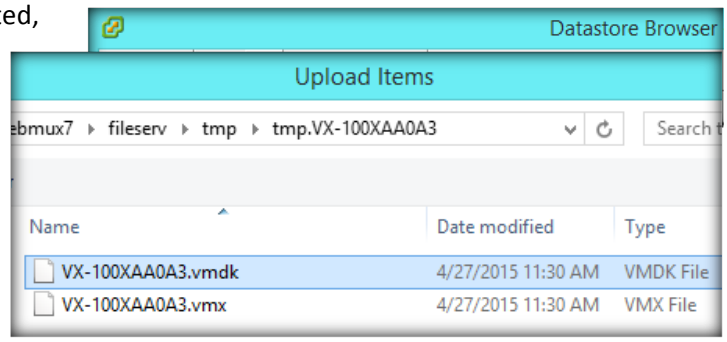


Name the folder the same name as the virtual machine that you will create. This Is not required but it can help keep things straight. We suggest “WebMux-“ and then the filename, which also contains the serial number of your virtual WebMux, as in:

webmux-vx-100xaa0a3

Upload Files to the Datastore

Now, with that new folder highlighted, click on the “Upload Files to this Datastore”



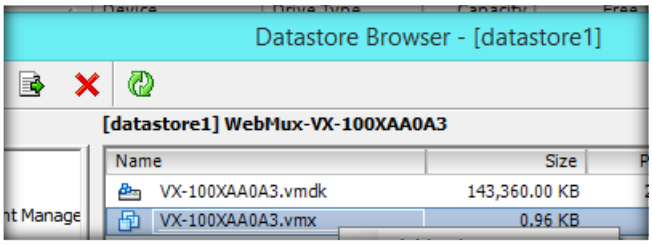
Navigate to the location to which you downloaded the virtual WebMux files and click on the first file, the **.VMDK** file, and click “Open.” Respond to any pop-up messages as appropriate and the file will be transferred into the folder.

Repeat the Upload for the **.VMX** file.

Verify that the files are in the designated folder by double-clicking on the folder name to open it.

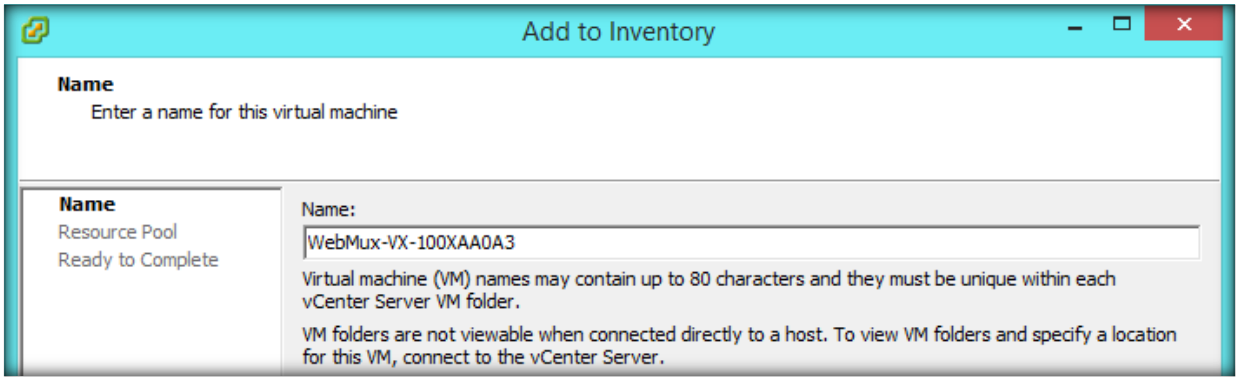
Add the WebMux VM to Inventory

Right-click on the .VMX file and choose “Add to Inventory.”



Name the Virtual Machine

You will see the filename already populating the “Name” field. Insert the word, “WebMux” to make the name start with “WebMux” and end in the Serial Number if you wish to use that



naming scheme.

Select the Resource Pool

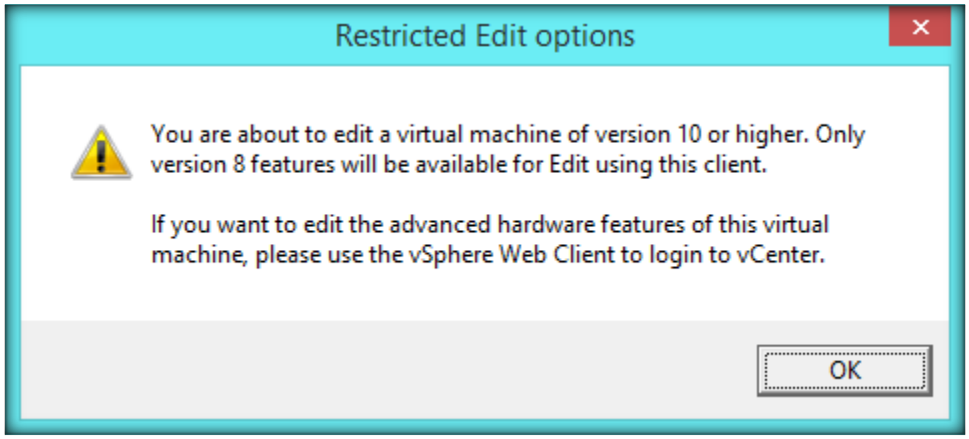
Accept the Resource Pool and click "Next."

Finish "Add to Inventory"

Review the setting and click "Finish." Close the datastore browser window.

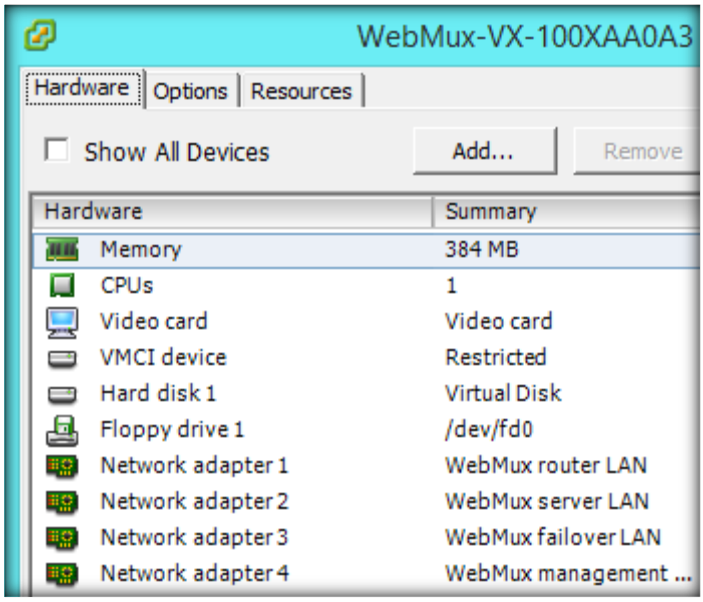
View the WebMux in the vSphere GUI

You should now see the new WebMux listed in the virtual machine inventory in the left frame of the GUI. Click on the name and the "Getting Started" tab for the WebMux will show "Edit Virtual Machine Settings." Click on that link. You may get a warning about the version of the virtual machine, like the following, which you can dismiss.



Configure Networking

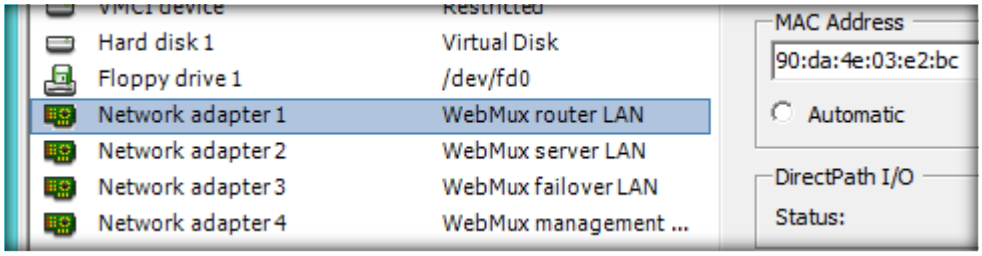
You need to connect the virtual WebMux to your infrastructure. This brings us to the intersection of the physical interface decisions common to load-balancer configuration.



WebMux Interfaces

The WebMux has four physical interfaces. You will need to plug the WebMux virtual interfaces into your infrastructure, into portgroups that match the functions of the WebMux ports. The properties for your new Virtual WebMux will show four network interfaces, "Network adapter 1" through 4. Each has a separate function, the "**router LAN**," "**server LAN**," "**failover LAN**," and **management LAN**." Each of them is also identified by the

AVANU OUI portion of the MAC address (the beginning of the MAC address, “90:da:4e”). You can verify them by clicking on each interface.



You will need port groups for any of the interfaces that you want to connect. Setting up your port groups is beyond the scope of this document but the basic information is provided here. If you want the security of a separate LAN for management then you should assign the “**Management**” interface to a port group with restricted access/traffic. If you are pairing this WebMux with another one in a **High-Availability (HA)** pair then you should connect the “failover LAN” port to a VMware port group with just the other WebMux in the HA pair (preventing any other machines from interfering on that LAN).

The other two ports are where the load-balancing happens. You will need to carefully consider the load balancing tasks to determine how the “**router LAN**” and “**server LAN**” ports should be connected to the virtual infrastructure. If you will be using the WebMux in a 2-Arm mode, such as NAT mode or in “Transparent Bridging” mode, then you will need both the Router LAN and Server LAN connections. If you will use a 1-Arm configuration, such as “Direct Server Return” or “Single Network,” then you will only need to connect one of them.

Load-Balancing “Arms” and Network Architecture

The “Arms” are just how many connections are used, one or two, and that is determined by how the WebMux fits in the network architecture. If the traffic flows into the WebMux on one interface, then on to the back-end servers on another interface, then it is a 2-Arm configuration. If the traffic goes to the WebMux on one interface and the WebMux then directs the traffic to the servers using that same interface then it is a 1-Arm configuration. The following are descriptions of the Arms and Architectures.

2-Arm NAT, is the required configuration when you have two subnets. It is the common "Destination" NAT configuration in which the clients connect to an IP address on the WebMux and the WebMux proxies to the back-end servers. The servers "see" the IP address of the client, as if the WebMux was not there. This is the required configuration when there are two IP subnets (Internet-side and Internal).

2-Arm Transparent makes the WebMux an inline bridge--seeing all of the traffic below the IP layer and able to manage traffic without IP address changes. Note that, being a bridge, you must avoid bridge loops--having a circular path through inter-connected bridges. Also, being inline and 2-Arms, the load-balanced traffic flows through the WebMux.

1-Arm Single Network is a special case of bridging in which the WebMux bridges internally on one interface (that can be bonded for higher capacity). The bridge loop issue is eliminated. Note that all traffic is "source NATted" (aka SNAT)--so the WebMux becomes the client and the server does not see the IP address of the client. A limitation of this configuration is that an additional IP address must be

assigned to the WebMux for each 65,000 simultaneous connections--because of that SNAT configuration and client-server relationship.

1-Arm Direct Server Return (DSR) the highest-performance option in cases where it is supported, also known as "Direct Routing" or "Out-of-Path (OOP)" this makes the WebMux the traffic director for incoming traffic but return traffic can route back bypassing the WebMux (unless the WebMux does SSL termination). Note that this requires a simple configuration of a "loopback adapter" on the servers and also not there is no performance advantage if SSL or TLS termination is required as the WebMux becomes the endpoint for the SSL/TLS security relationship.

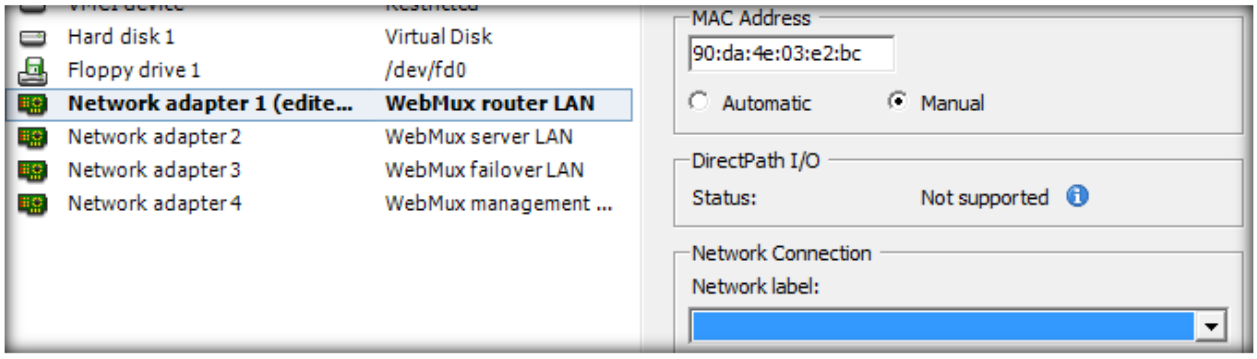
For further illustration of the Arms and Architectures please review our guidance at:
http://www.avanu.com/WebMux-Arms-Architecture/arms_and_architecture.html

This table may help you document where you will connect the virtual WebMux, to assign the network interfaces to port groups:

NIC	Port Group
router LAN	
server LAN	
failover LAN	
management LAN	

Making Port Group Connections

You will see a section in the GUI for “Network Connection” in which there is a drop-down selection for “Network Label.” (See below.) The assignment is simple if the port groups are set up. Click on each interface, on the left side, then choose a matching port group from the “Network label” drop-down.



Start the VM

You can start the WebMux once all the network interfaces are connected.

Connection Options for the WebMux

Your WebMux VM is shipped with an IP address that you provided when requesting the VM. The address is assigned to the Managment/MGMT port (which shows up in firmware as "ethx0") and, for your convenience, it is found in the e-mail that contained the link to download the VM. You can now reach the virtual WebMux by any of the following methods. The administrative user account, used for configuration, is "superuser." The operator account (read-access only), used for monitoring, is "webmux." Note that you can use TACACS+ and RADIUS to set up additional accounts with "superuser" and "webmux" permissions if those technologies are in use in your organization.

Web GUI—Port 35/HTTPS

```
https://<WebMux_MGMT_IP_Address>:35
```

Web Wizards—Port 35/HTTPS

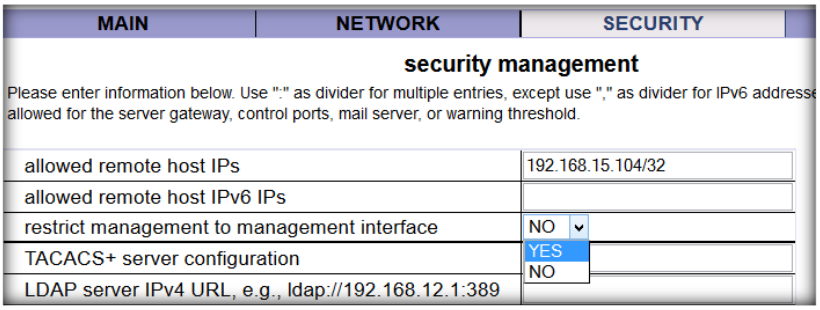
```
https://<WebMux_ MGMT_IP_Address>:35/wizards
```

Command Line—Port 77/SSH

```
ssh -l superuser -p 77 <WebMux_ MGMT_IP_Address>
```

Security Note

The WebMux management GUI and SSH CLI can be reached by any IP addresses that you configure as you configure load-balancing. Turn that access **OFF** once you have determined you have access. Log in, hover over "Security," choose "Security Management," and set "Restrict management to management interface" to YES.



Configure Load Balancing

Your next steps will either be via the configuration wizards or you can configure the WebMux manually. The wizards provide shortcuts to many common scenarios so that may be the best starting point. The wizards configure all of the ports, create farms, and walk you through most of the questions and decisions while hiding complexity. Refer to the User Guide or the configuration guidance for individual systems, such as Microsoft Skype for Business, Exchange, etc. See those and other documents at:

http://www.avanu.com/webmux-tech-tips/