

VMware ESXi Survival Guide  
By Robert Chase [rchase@systemv.org](mailto:rchase@systemv.org)

VMware ESXi is a free product provided by VMware that has a number of features that have been streamlined. ESXi presents a number of administrative challenges due to many of the features that have been removed.

One of the things that one will notice initially when dealing with ESXi is that VMware makes the claim that there is no direct command line interface. This is not exactly true. There is a very stripped down command line interface that is quite useful and one only has to enable SSH on the system to take advantage of many of the features this CLI offers. There is also the remote cli but quite honestly it tends to be intentionally clunky and poorly documented.

Enabling SSH in VMware is a simple process. Press ALT F1 at the physical console of the system and type unsupported and then the root password of the machine. From there uncomment ssh in /etc/inetd.conf and restart services with a /sbin/services.sh restart. SSH is now enabled. There are a number of security implications from enabling ssh on ESXi. You will need to evaluate the security implications of this in your environment before hand. Additionally if you have any support from VMware ssh logins are logged to the system and VMware seems to be paranoid about ssh logins.

Once you have SSH enabled on the system you can do a number of functions such as moving and renaming VMDK and VMX files via the command line and cloning and moving VM's as well as generation of new UUID's. You can also directly edit the VMX files beyond what the ESXi GUI allows. A word of caution on editing VMX files. Do this at your own risk and if you know what you are doing.

You also may want to install the VMware remote CLI on a Linux workstation on your network. Even though it has limited functionality it does come in handy from time to time if you are not able to use the GUI to control the server. Since the remote CLI runs it's commands on remote systems you will have to get used to using the -H flag and providing authentication for your hosts.

## Moving VM's in VMware ESXi

The first step is to connect to the hypervisor that your VMDK files are on via ssh. From there you can navigate to the vmx and vmdk files you wish to migrate under the /vmfs directory. Your VM's should be under /vmfs/volumes/datastore#. Once you are in the directory you wish to migrate you can use SCP to copy the physical disk files to the other machine. With a command similar to `scp * root@hostname:/vmfs/volumes/datastore#/vm-dir`. You will need to have the destination directory created ahead of time.

Once the files have copied you will need the specific command VMware-cmd for the registration of the VM with the hypervisor and to power on the VM. A command similar to `VMware-cmd -H hostname_of_hypervisor -s register /vmfs/volumes/datastorename/`

vm-dir/vm.vmx datacenter-name resource-pool. The easiest way to register VM's is through the VMware Console. VM's can be registered with the hypervisor by navigating to the datastore on the summary tab under the main hypervisor in the GUI. Double click on the datastore to browse the files. Right click on the VMX file you wish to register and select add to inventory.

Now that our VM has been moved and registered we are ready to boot it. You can do this from the remote command line with `VMware-cmd -H hostname_of_hypervisor /vmfs/volumes/datastorename/vm-dir/vm.vmx start` or through the GUI.

### Duplicate Mac Addresses after moving VM's

When cloning virtual machines the VMX file stores information about the virtual MAC address of the virtual NIC installed within VM. When moving VM's a new UUID should always be generated as the UUID is used to generate the mac address. In the event that a new UUID is not generated a machine can have a duplicate mac address which might cause problems with the machine's networking.

"The UUID is a 128-bit integer. The 16 bytes of this value are separated by spaces, except for a dash between the eighth and ninth hexadecimal pairs. So a sample UUID looks like this: 00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff The UUID is based on the physical computer's identifier and the path to the virtual machine's configuration file." From VMware support documentation.

To generate a new UUID do the following within VMware ESXi. Remove the VM from your inventory. SSH into the hypervisor and go to `/vmfs/volumes/datastore#` Rename the directory that your VM lives in with `mv vmdir newvmdir`. Go into your VM directory and edit the VMX files and remove these the lines that start with this.

`uuid.location=`

`uuid.bios=`

`ethernet0.GeneratedAddress=`

`uuid.Action=`

Add the VM to inventory and do your initial power up. The new UUID will generate a new and unique MAC address will be generated.

### Cloning of VM's in VMware

The easiest way to clone VM's in VMware is through the CLI. Before you begin you want to shut down the VM that you are trying to clone as when the VM's are booted the disk files are locked. Log into the CLI and navigate to `/vmfs/volumes/datastore#` and use `cp -r path_of_vm_to_clone path_of_new_vm` to copy the physical VMDK and VMX files

in the vmfs. Even though we are on disk this will take a moment to complete. Once the file copy finishes bring the new VM into inventory with the GUI. When you initially power the VM VMware will prompt you to generate a new UUID for the VM. If you don't do this the new VM will have the exact same MAC address as the old VM and may cause you issues. Additionally you may want to take into consideration IP address conflicts bringing up a "clone" of a system in the VM environment. If the VM is a windows VM you will want to rename the VM and remove and re-add it to your active directory.

## ESXi Loosing Network settings

Due to the appliance like nature of VMware ESXi there are very few things that can be accomplished troubleshooting wise if there is a problem. Rebooting is often the only choice when things go wrong. Caution must be taken when rebooting a VMware host as sometimes the system will lose its IP settings. When the system is rebooted it will no longer be pingable on the network and the remote console will not function requiring manual intervention on the console. It is important to weigh the uptime of all of the VM's on the system versus the need for the reboot as in most cases even if there is a serious issue the VM's remain running. I have seen VMware lose its network settings during reboots several times and recovery is sometimes painful especially if there is limited remote access to the system console.

When you go to the console of the system you will notice that the ip address is set to 0.0.0.0 and that you will not be able to edit the network settings within the console. The system will not be able to reach the network at all. I have observed that one sees "odd" behavior on some of the administrative functionality of the console. If your not able to add users or make changes to the systems settings or see odd behavior you may want to schedule a downtime and have someone ready in the datacenter to assist.

At this point the only choice for recovery is to choose the "reset to factory defaults" setting on the console which resets ALL of your settings including resource pools, networking information, users, and machine inventory. You will need the IP address information for the host and will need to set the root password on the system again so its good to have these ready ahead of time. After the initial IP configuration and password change the host is back up on the network and you can start reconfiguring and bringing the VM's back into inventory (they are still on the disk). Since vicfg-cfgbackup is missing out of ESXi all of the configuration has to be done by hand.

## Additional Resources

If your not a unix user and need to SCP from a windows host you can download WinSCP to do your transfers. While its not as efficient as VMware host to VMware host transfers it gives you an easy to use interface that's a little more usable than the unix command line. Its Free and open source as well. <http://winscp.net/>

VMware remote CLI users guide [www.VMware.com/pdf/vi3\\_35/esx\\_3/r35u2/vi3\\_35\\_25\\_u2\\_rcli.pdf](http://www.VMware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_rcli.pdf)