Virtualization for Professionals

ISACA NTX

November 10, 2016

RCI

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Agenda

- Hypervisor basics & options
- VMWare client tools & snapshots
- VMWare networking
- Shared folders
- USB devices
- Useful links

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Virtualization Basics

- Terminology
- Bare-metal vs software
- Popular hypervisors
- VMWare product line
- Hardware requirements

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Virtualization Terminology

- Hypervisor
  - Software which enables running multiple virtual operating system environments on one computer
- Host
  - The computer running the hypervisor
- Guest
  - A virtual machine running on the hypervisor on a host

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Bare Metal vs Software Hypervisors

- Type 1: Bare metal (hardware)
  - Hypervisor is the operating system
  - Usually a stripped-down Linux
  - Used on servers
- Type 2: Software
  - Hypervisor is an application
  - Used on workstations/laptops

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Popular Hypervisors – Type 1

- VMWare vSphere Hypervisor(ESXi)
- Citrix XenServer
- Free/paid versions available for each

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Popular Hypervisors – Type 2

- Vmware products (next slide)
- Microsoft Hyper-V (not just for servers)
  - Installs as a Windows feature
  - No simultaneous use with VMWare products
- VirtualBox
  - Free, open source

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

VMWare Product Line

- vSphere/ESXi – Bare metal for servers
- Workstation: non-free; available for Linux and Windows
- Workstation Player: maybe free; available for Linux and Windows
- Fusion: non-free, for Mac

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Workstation vs Player

Advanced Features		
Run encrypted VM	●	●
Drag-able tabbed interface		●
Run Multiple VMs at one time		●
Create/manage encrypted VM		●
Snapshots		●
Advanced networking		●
Linked clone		●
Share virtual machine (as a server)		●
Connect to vSphere/ESXi server		●
Connect to vCloud Air		●
Command line operation: vmrun and VIX		●

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

VMWare Pricing

Local Desktop Virtualization

Fusion 8.5 Pro

Designed for advanced users, developers, QA, and IT.

Save 20% on New Licenses.
Save 33% on Upgrades.

~~$199.99~~ $159.99	~~$119.99~~ $80.39
Buy	Upgrade

Fusion 8.5

The ultimate Windows on Mac experience.

$79.99	$49.99
Buy	Upgrade

Workstation 12.5 Pro

Leading Edge PC Virtualization.

$249.99	$149.99
Buy	Upgrade

Workstation 12.5 Player

Streamlined PC Virtualization for Business.

$149.99	$79.99
Buy	Upgrade

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Hardware Requirements

- CPU Support for EM64T and VT
  - Extended memory 64 technology
  - Virtualization technology (often has to be enabled in BIOS)
  - Execute disable bit

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Check Hardware - Windows

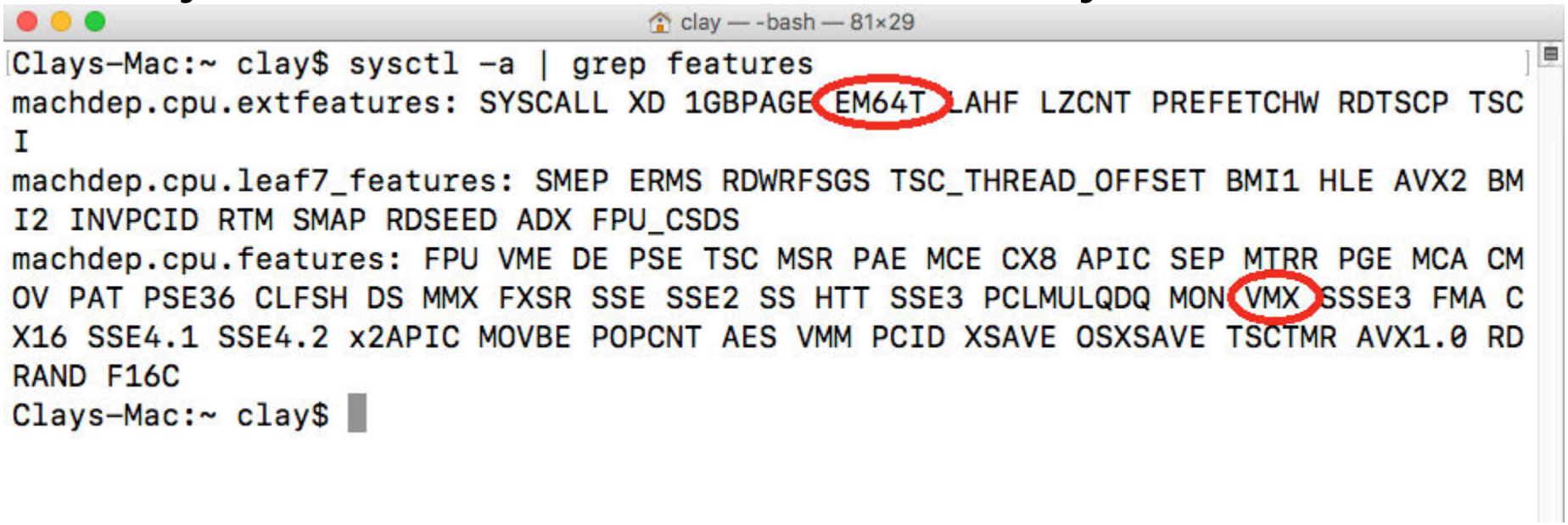
- Use systeminfo.exe from command line
- Look for Hyper-V section (requirements are the same)

```
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Check Hardware - Mac

- System kernel control tool – sysctl



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Check Hardware - Linux

- Use the /proc/cpuinfo file

```
clay@NUC:~$ cat /proc/cpuinfo | grep flags
flags           : fpu vme de pse tsc msr pae mce cx8 apic
sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr
sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm constan
t_tsc arch_perfmon pebs bts rep_good nopl xtopology nonsto
p_tsc aperfmperf eagerfpu pni pclmulqdq dtes64 monitor ds_
cpl vmx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1
sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave av
x f16c rdrand lahf_lm abm 3dnowprefetch epb intel_pt tpr_s
hadow vnmi flexpriority ept vpid fsgsbase tsc_adjust bmi1
avx2 smep bmi2 erms invpcid rdseed adx smap xsaveopt dther
m ida arat pln pts
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Notes on Selecting Hardware

- Prioritize in this order:
  - RAM: more memory = more VMs
  - Disk speed:
    - Multiple VMs sharing one disk
    - SSD if possible
  - CPU:
    - More cores before higher speed
    - Higher frequency not as helpful for laptops

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

VMWare Client Tools

- Software installed in guest OS
- Allow enhanced interaction with host
- Video/mouse drivers
- Shared folders
- Time sync (use sparingly – NTP is better)

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

VMWare Client Tools (2)

- Installed from ISO image or package
  - See VMWare PDF in links section
- Command line tool for some functions
  - Windows: VMwareToolboxCmd.exe
  - Mac: vmware-tools-cli
  - Linux: vmware-toolbox-cmd

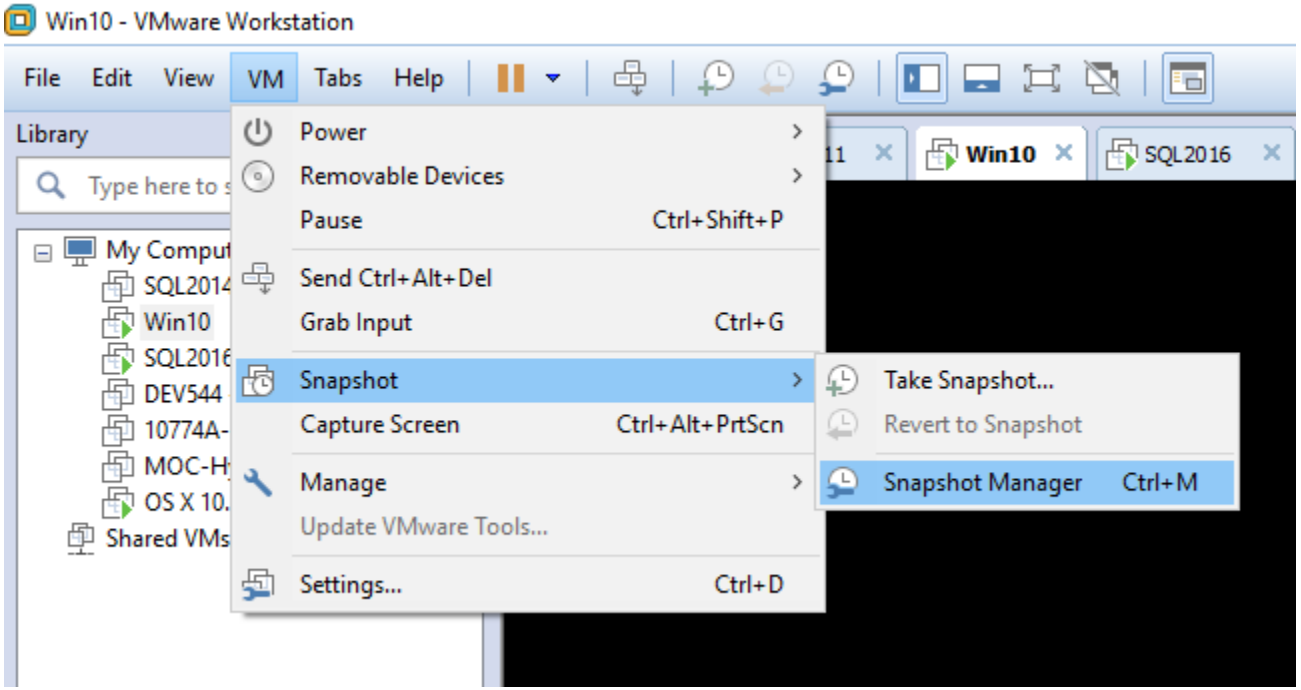
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Guest Snapshots

- Save the current state of the guest
  - Hard disk – creates “delta” files
  - Memory
  - Hardware configuration
- Can use a lot of disk space

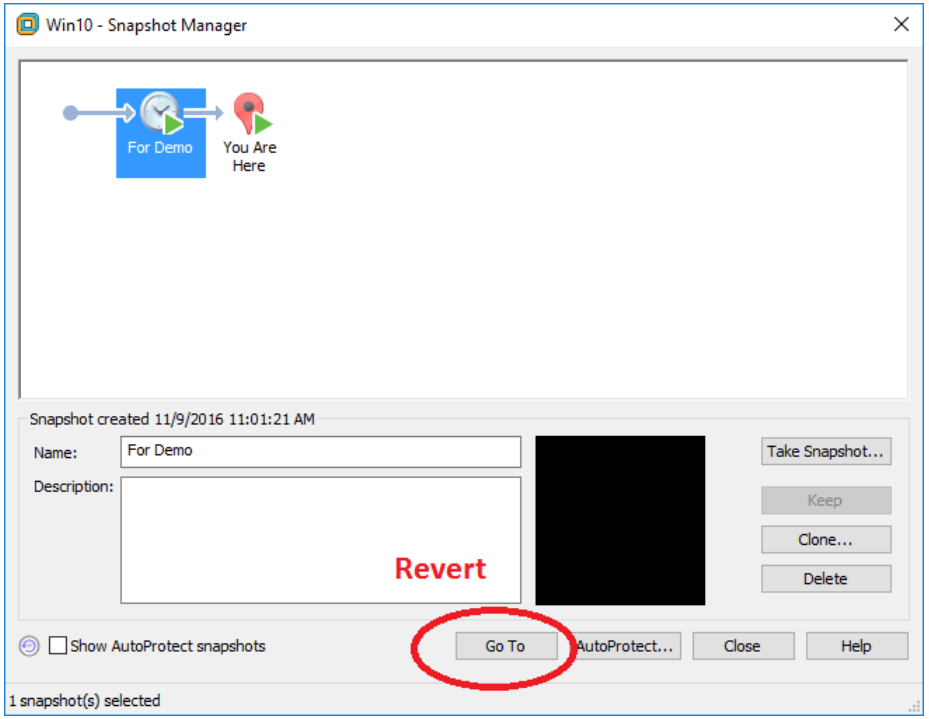
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Guest Snapshots (2)



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Guest Snapshots (3)



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

When to Use Snapshots

- To clone a system
- Before a major change
- Before an engagement

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

VMWare Networking Modes

- Bridged
  - Shares physical network interface: guest has IP on physical LAN
  - No DHCP server
  - VMNet0
- Host-only
  - Only your PC and VMs (can't talk outside PC)
  - VMNet1
- NAT (network address translation)
  - "Hides" VMs behind PC's IP address
  - VMNet8

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

VMWare Networking Limits

- Bridged: one per physical NIC
- NAT: one per physical host
- Host-only: not restricted
- Can have up to 20 total virtual networks (VMNet0 – VMNet19)

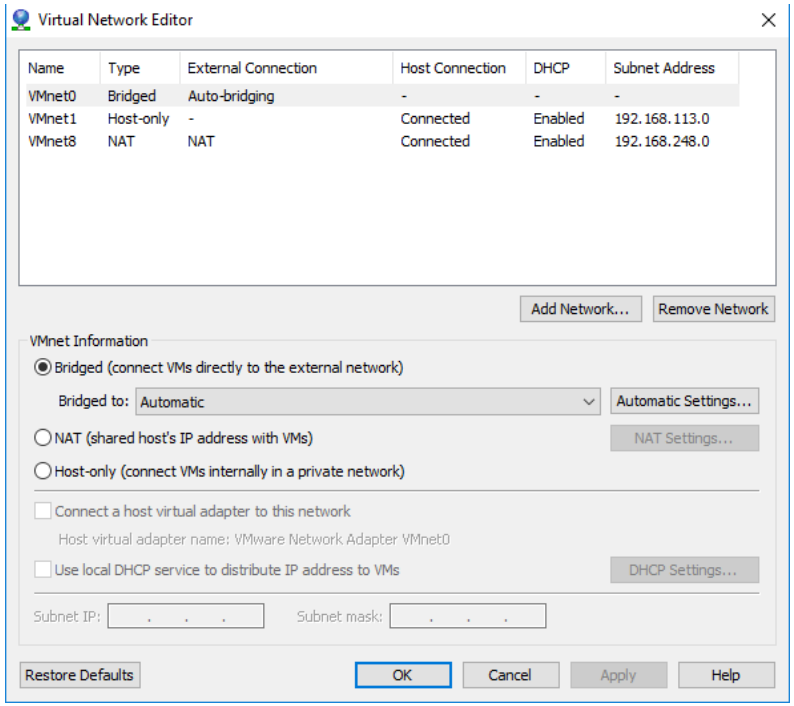
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

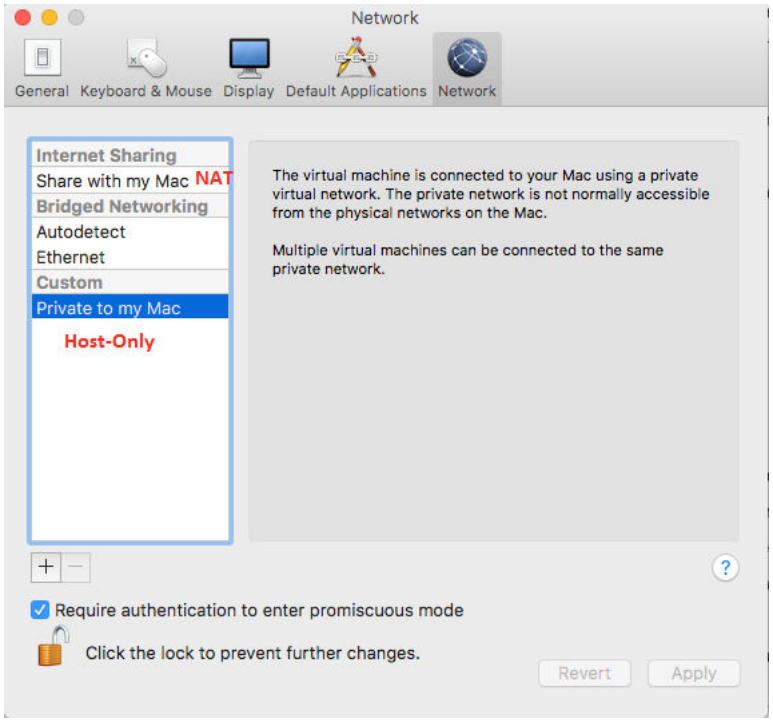
Virtual Network Editor

- Workstation on Windows
  - vmnetcfg.exe
- Player on Windows
  - vmnetcfg.exe (copied from machine with Workstation installed)
- Fusion on Mac:
  - VMWare Fusion|Preferences|Network

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Virtual Network Editor (2)





© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Managing the DHCP Server

- Fusion:
  - /Library/Preferences/VMware Fusion/networking
- Linux:
  - /etc/vmware/vmnetX/dhcp/dhcp.conf
- Windows: GUI

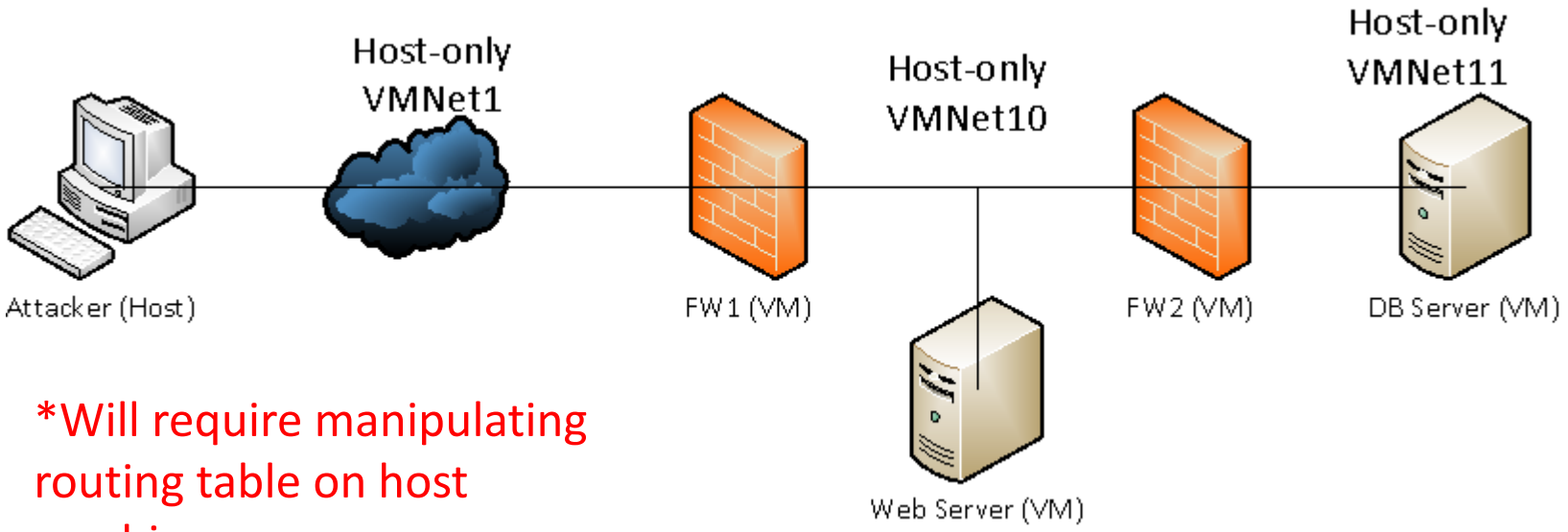
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Default DHCP Address Allocation

- Class C private subnet created randomly
- Host machine: X.X.X.1
- NAT Device (on NAT networks): X.X.X.2
- Reserved for static addresses: .3 – .127
- DHCP clients: X.X.X.128 – 253
- DHCP Server: X.X.X.254

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

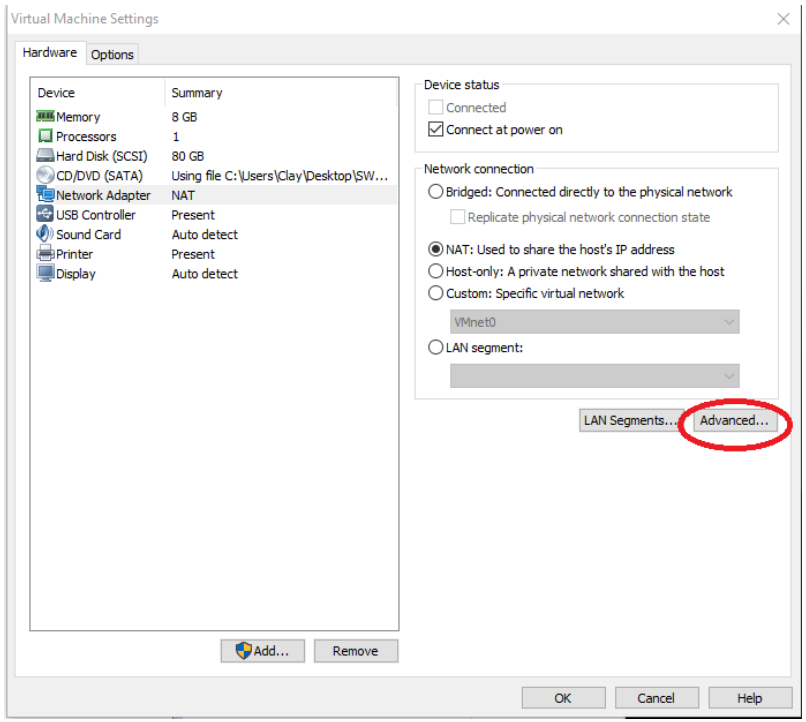
Why Create/Edit Networks?

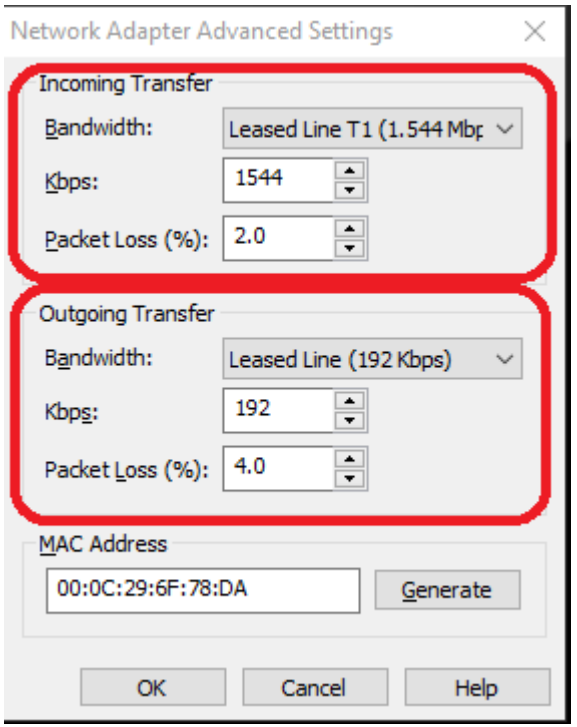


*Will require manipulating routing table on host machine

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Advanced Guest Network Settings





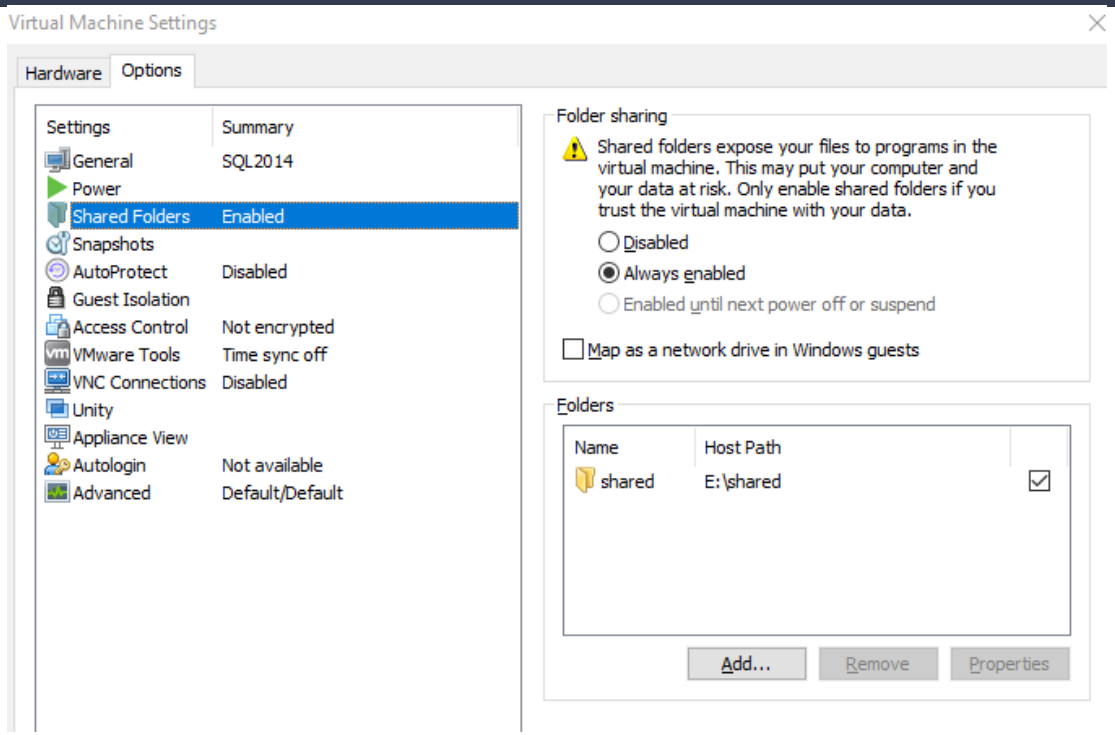
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Shared Folders

- Allows sharing files between host and guests
- Requires tools to be installed on guest

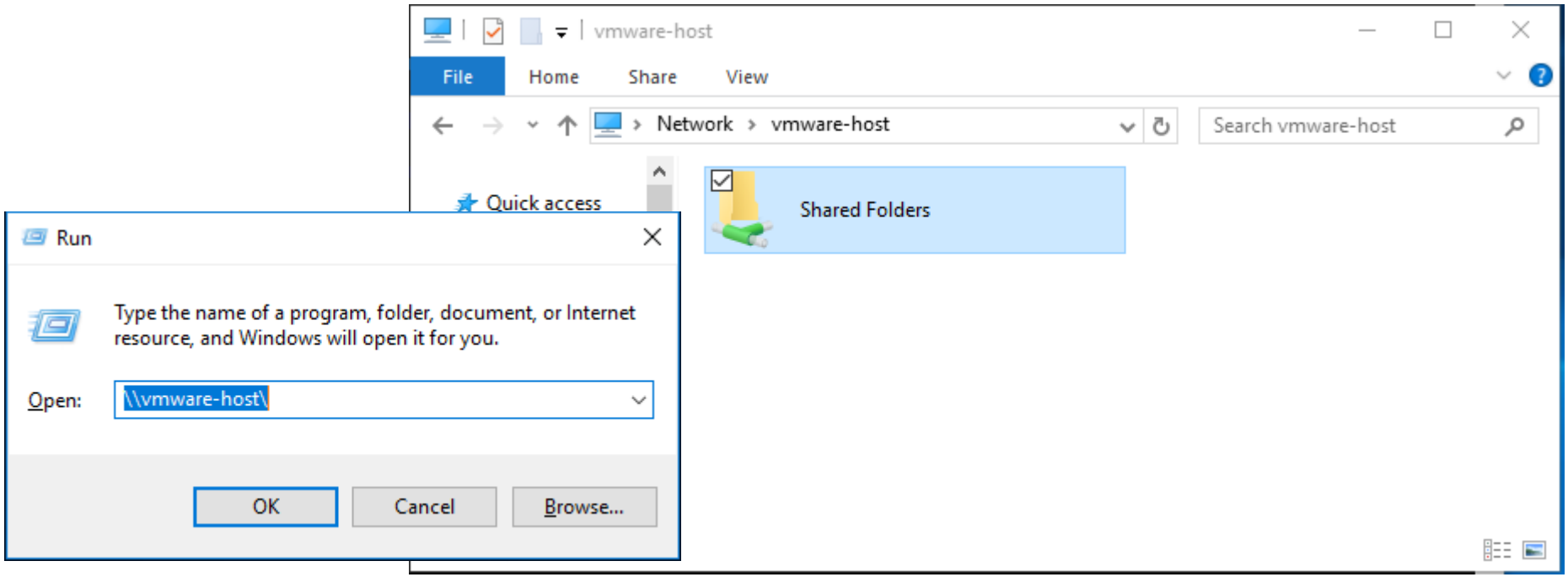
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Shared folders (2)



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Shared Folders (3)



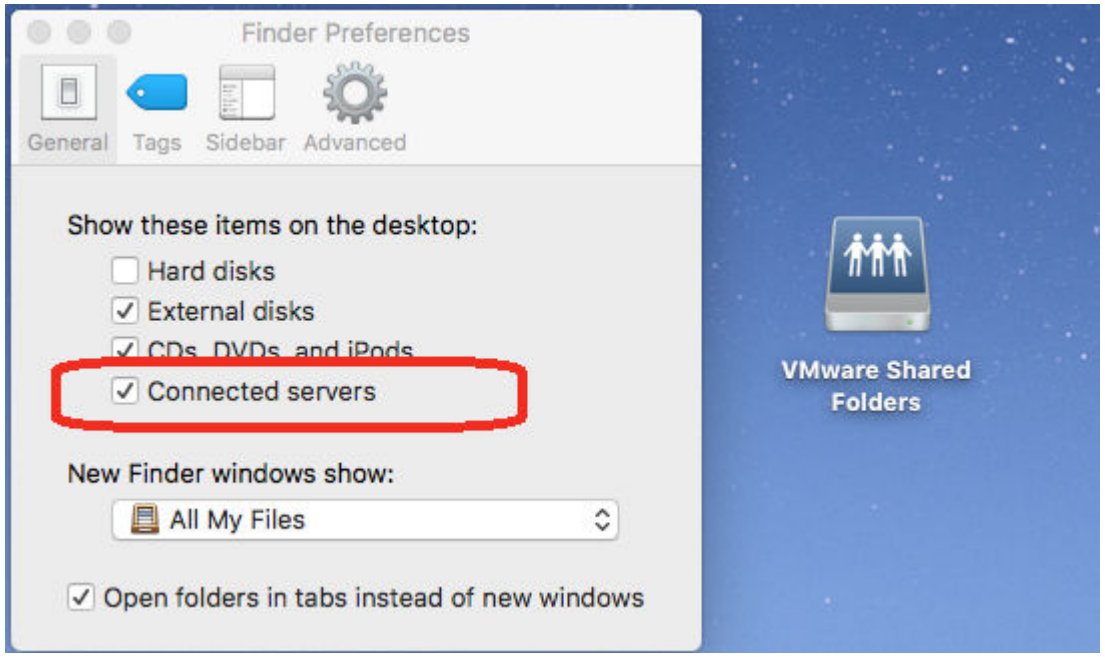
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Shared Folders – Mac and Linux

- Mac: Shared folders will be mounted at:
  - /Volumes/VMWare Shared Folders
  - Can show on desktop in Finder (next slide)
- Linux: use ".host" as the hostname
  - mount -t vmhgfs .host:/foo/bar /var/lib/bar

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Mac –Shared Folders on Desktop



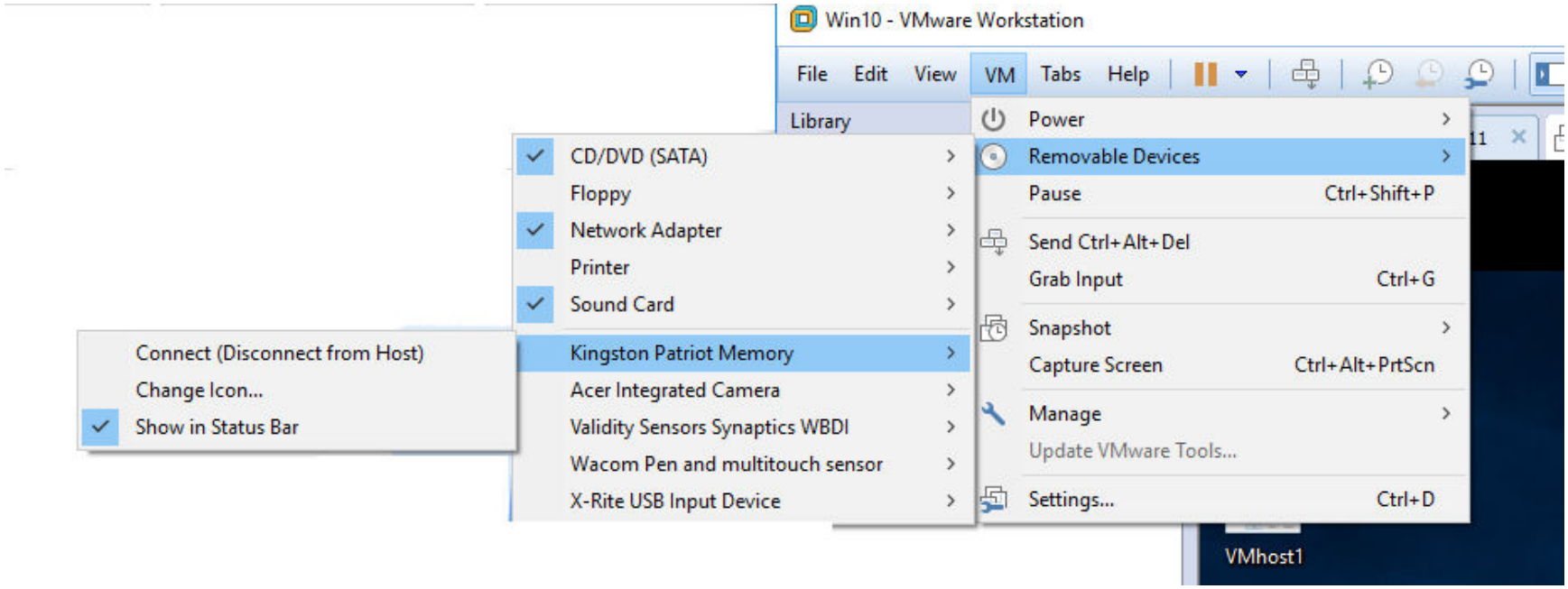
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

USB Devices

- Host can “pass through” USB devices to the guest
- Useful for flash drives and wireless cards

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

USB Devices (2)



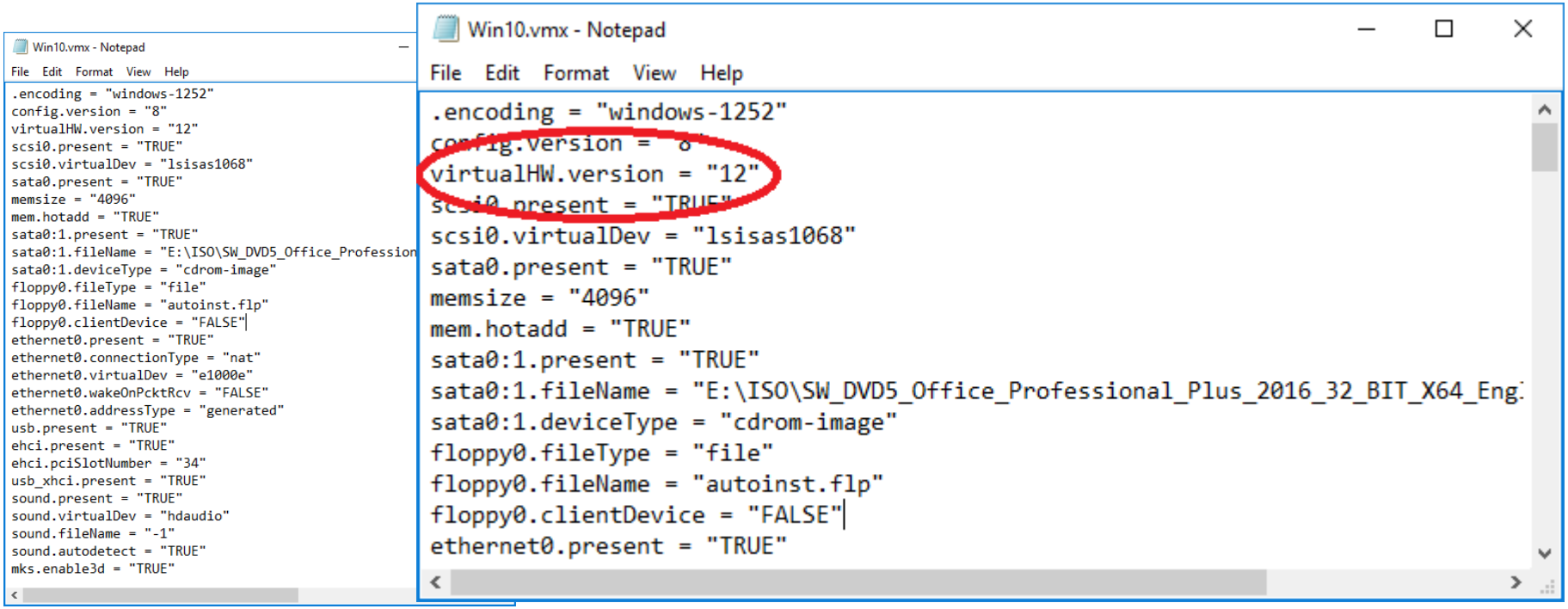
© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Pro-Tip: VM Configuration Files

- .VMX extension
- Just a text file
- Can edit settings not available in GUI
- Can change version compatibility
  - virtualHW.version = "12"

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Pro-Tip: VM Configuration Files (2)



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Useful Links

- VMWare Support
  - http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf
  - http://www.vmware.com/products/fusion/faqs.html
  - https://www.vmware.com/support/fusion.html
  - http://www.vmware.com/products/workstation/faqs.html
  - https://www.vmware.com/support/workstation.html
  - http://www.vmware.com/products/player/faqs.html
  - https://www.vmware.com/support/player.html

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Useful Links (2)

- Virtual Appliances
  - Turnkey Linux
  - https://www.turnkeylinux.org

  - VMWare Virtual Appliance Marketplace:
  - https://solutionexchange.vmware.com/store/category_groups/virtual-appliances

  - JumpBox (No longer free, but offer a free trial)
  - http://www.jumpbox.com/

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Useful Links (3)

- Kali Linux
- https://www.kali.org/

- Samurai Web Testing Framework:
- http://www.samurai-wtf.org/

- Samurai Security Testing Framework for Utilities
- http://www.samuraistfu.org/

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Useful Links (4)

- OWASP Broken Web Applications Project
- https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

- OWASP Vulnerable Web Applications Directory Project
- https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project

- OWASP Web Testing Environment Project
- https://www.owasp.org/index.php/OWASP_Web_Testing_Environment_Project

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Useful Links (5)

- Metasploitable
- https://sourceforge.net/projects/metasploitable/

- MS Evaluation Products (ISO files and Hyper-V files)
- https://www.microsoft.com/en-us/evalcenter/

© 2016, Risenhoover Consulting, Inc. All Rights Reserved