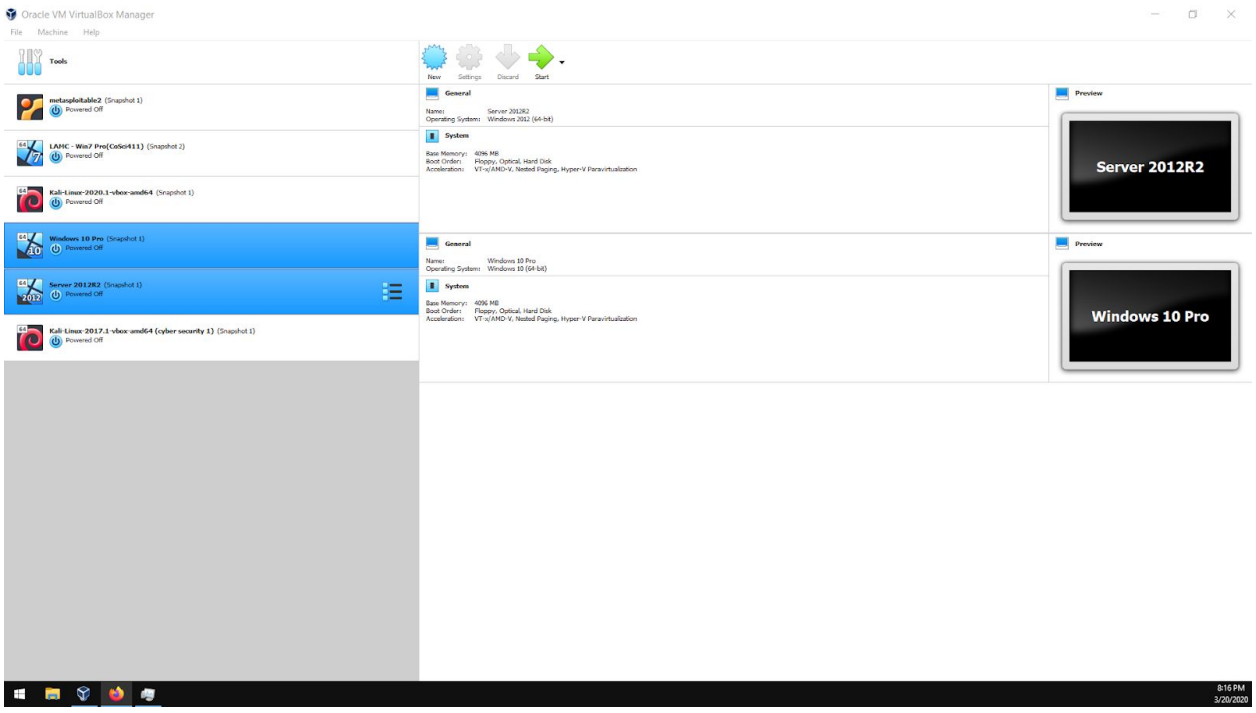
Cyber Report - Create a Domain Controller and Join It

1. Each assignment has a goal. What is the assignment and how will you find the solution?

> The goal of this lab is to create and connect to a domain controller situated on an instance of Server 2012R2 via VirtualBox. Using Windows 10 Professional, a static IP connection will be made to the newly created domain. To provide static IP addressing, virtual network options within VirtualBox will be utilized. A brief demonstration of data storms will be included at the end of this lab.

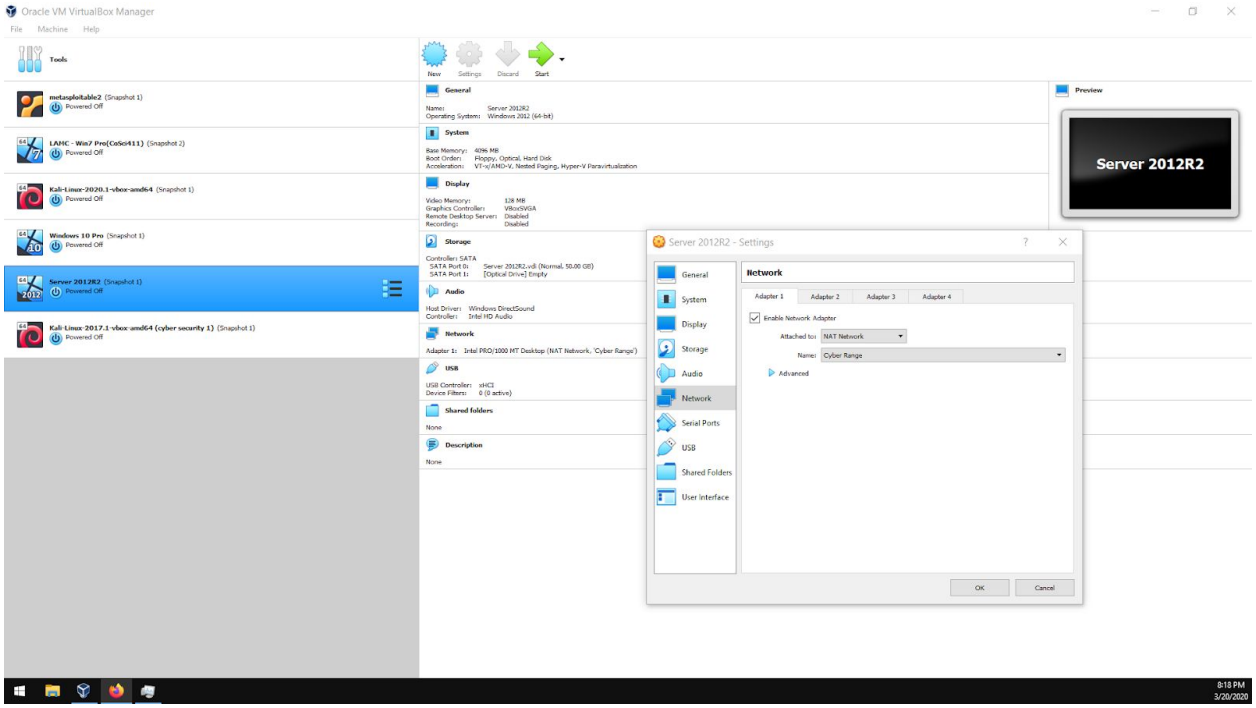
2. Demonstration of the steps taken with screenshots (snipping tool) from your computer. You need to show the steps you took as you took them.

VirtualBox Main menu



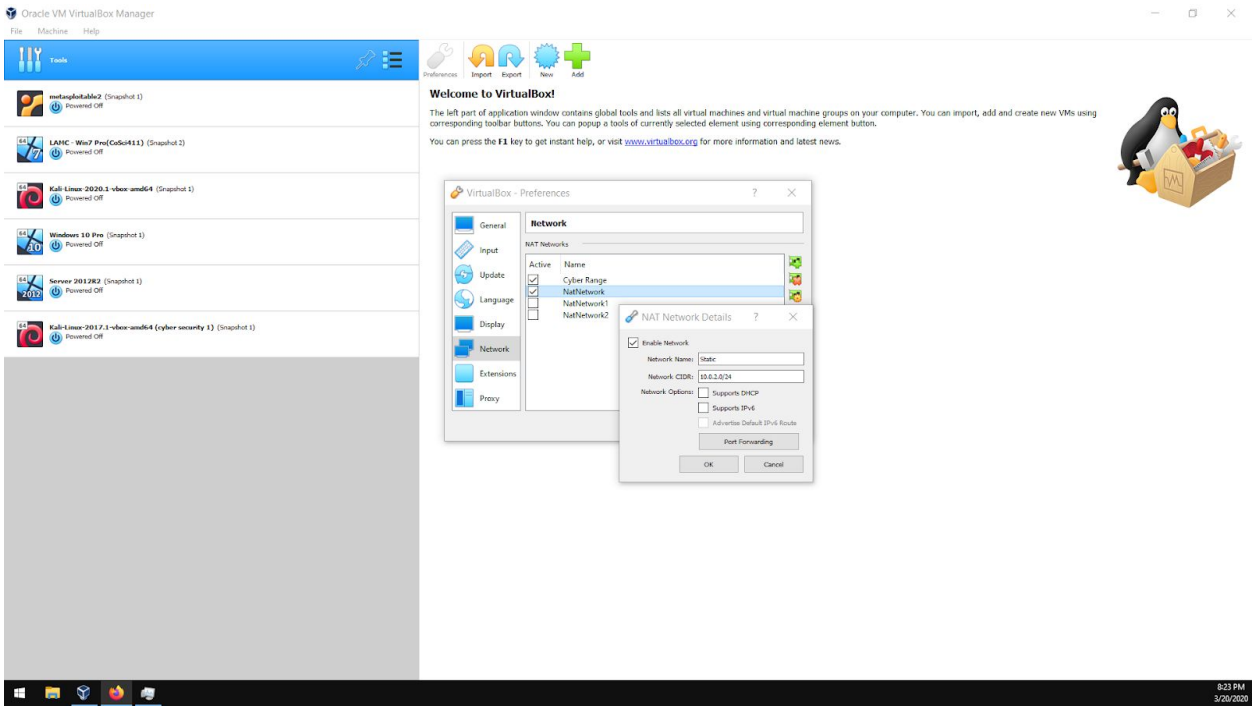
Starting at the VirtualBox main menu, I've selected the two virtual machines that will be focused on in this lab.

Server 2012R2 - Settings



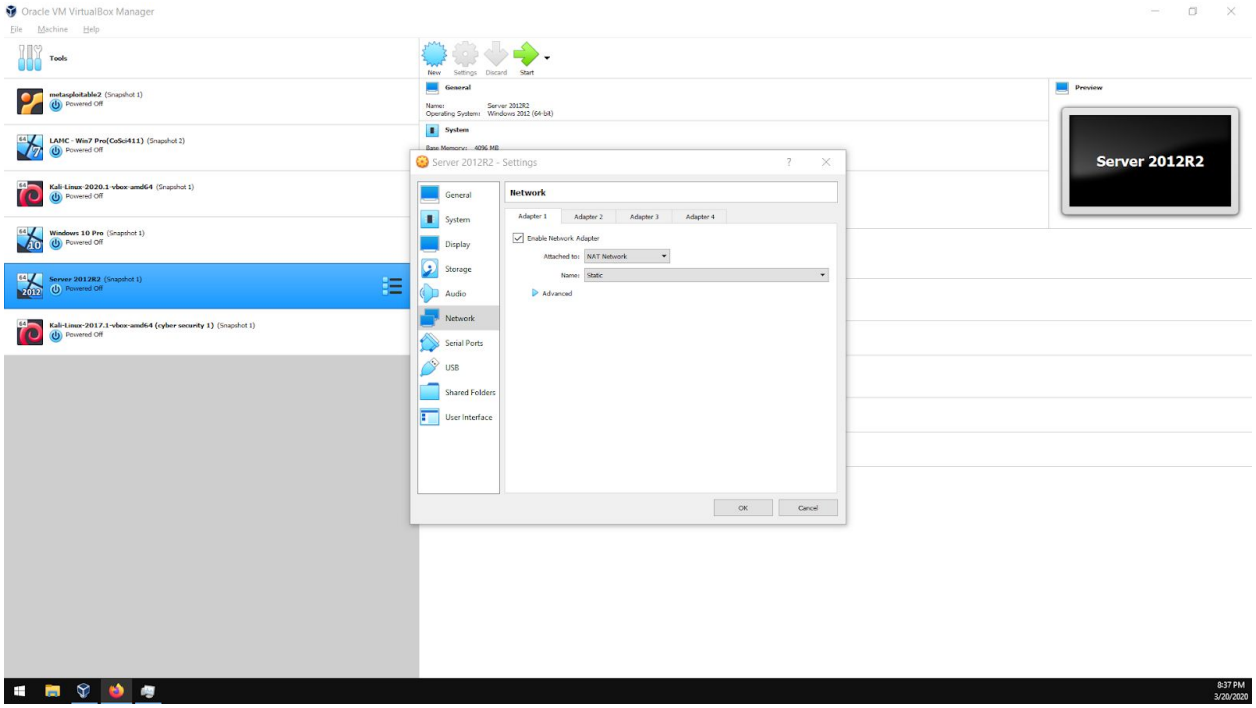
The current Network settings for Server 2012R2 display a NAT Network (Cyber Range) configuration. This setting will not work because Active Directory requires static IP addressing.

VirtualBox - Preferences



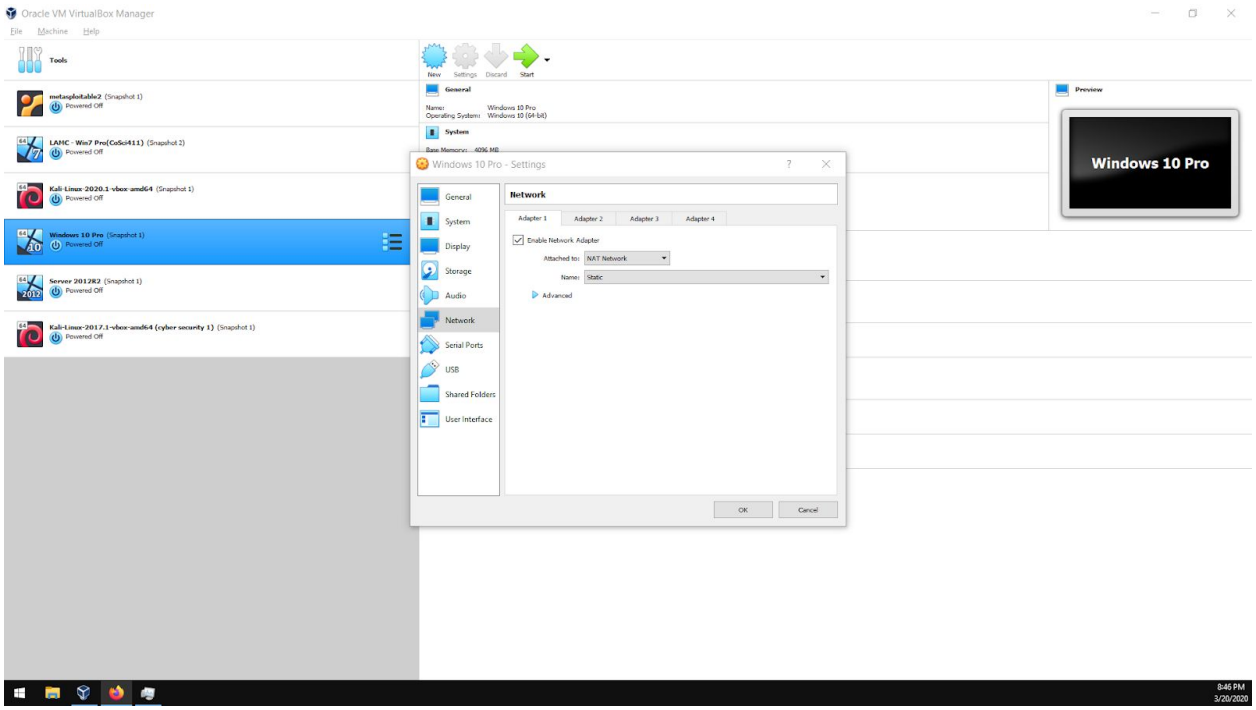
These are application wide settings within VirtualBox, with each virtual image setting its own network setting to choose from the list.

Server 2012R2 - Settings



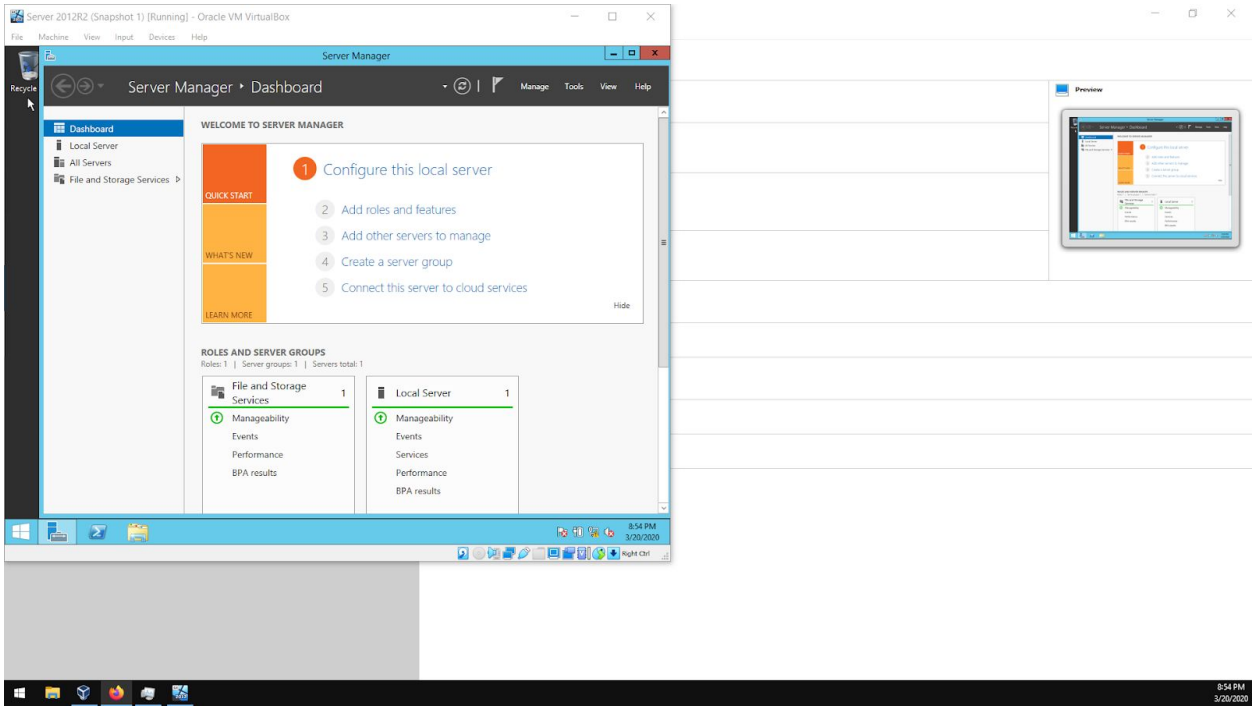
The setting for Server2012R2 is set to Static, meaning that DHCP will not automatically hand out IP addresses, the IP values will need to be configured manually.

Windows 10 Pro - Settings



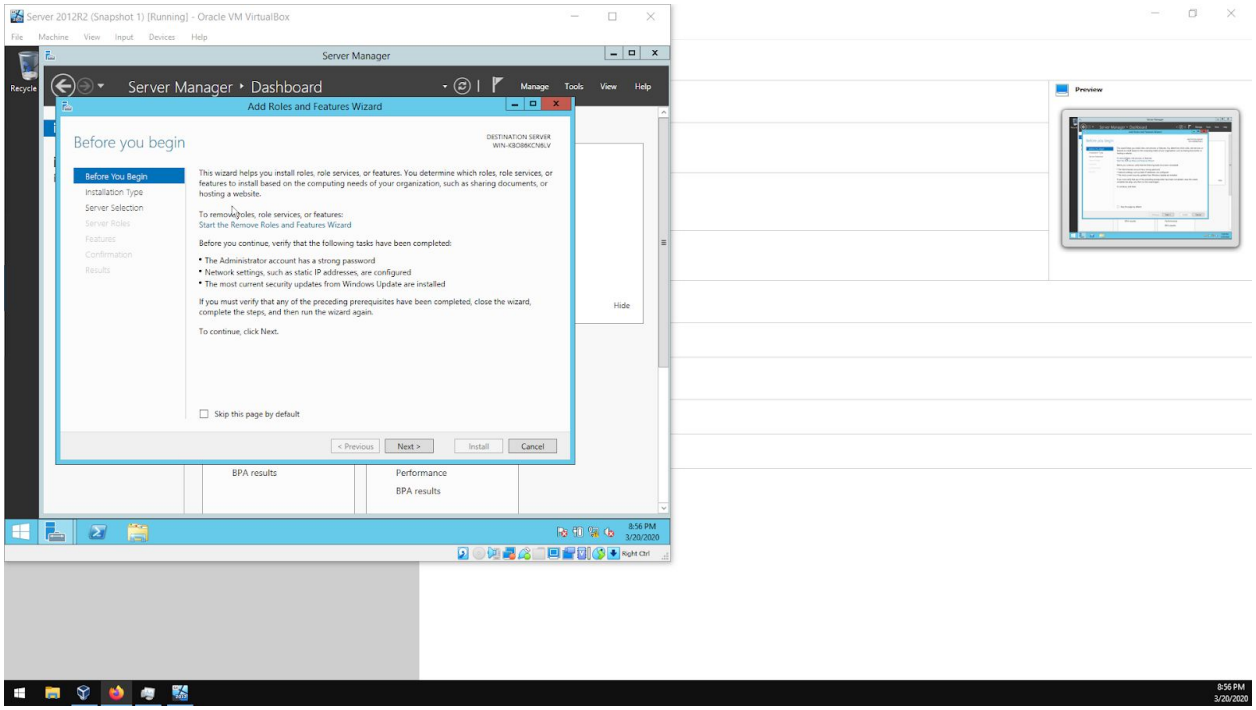
Here the same setting is made for Windows 10 Pro, Network set to Static.

Server 2012R2 - Server Manager



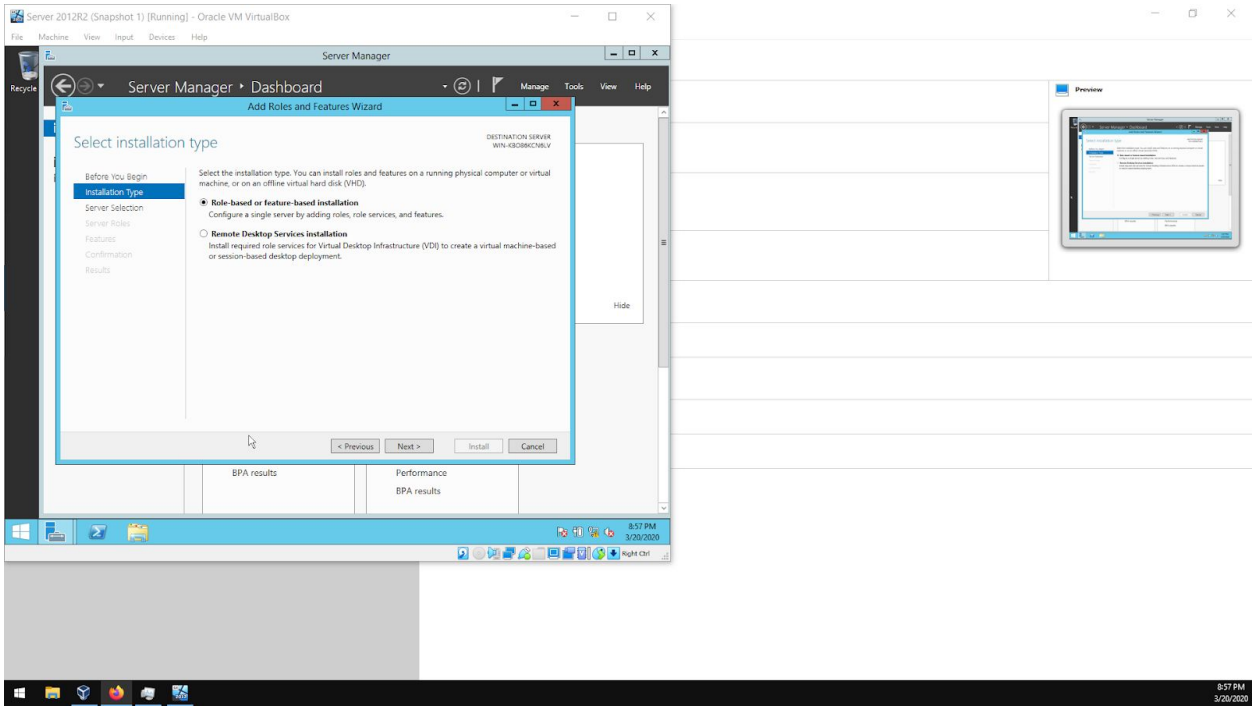
Configuration is done through Server Manager, selecting Configure this local server.

Add Roles and Features Wizard



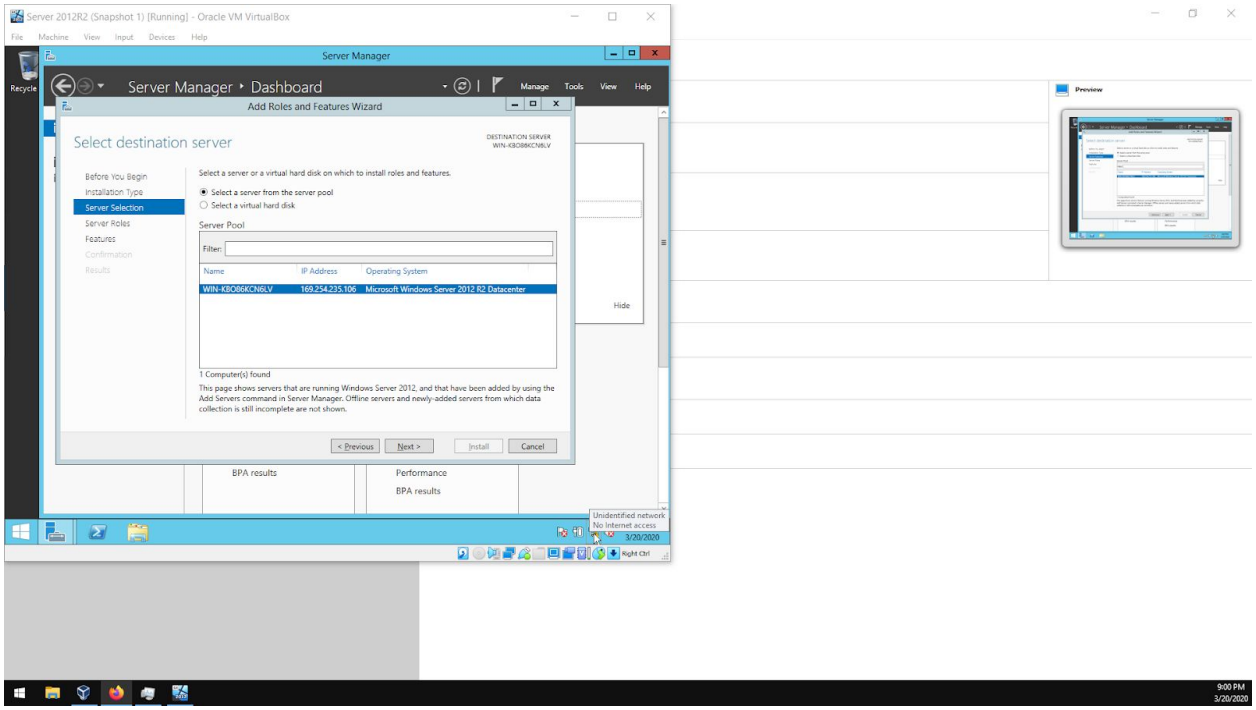
Roles and features are chosen here.

Installation Type



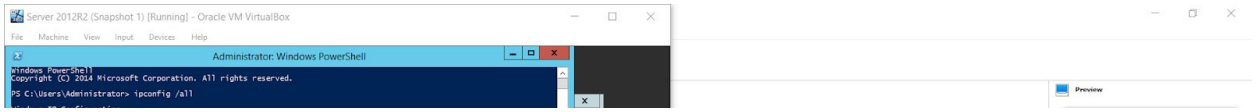
For this lab, Role or feature based installation is selected.

Server Selection



The IP must be configured as Static before continuing.

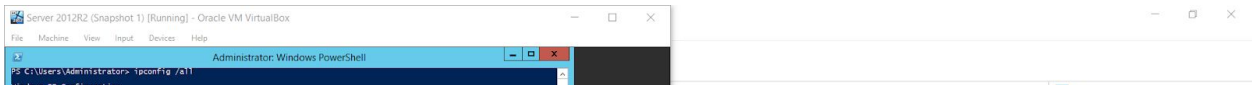
PowerShell - ipconfig /all



ipconfig /all will display all the necessary information for setting up the IP statically. Note there is no Default Gateway listed.

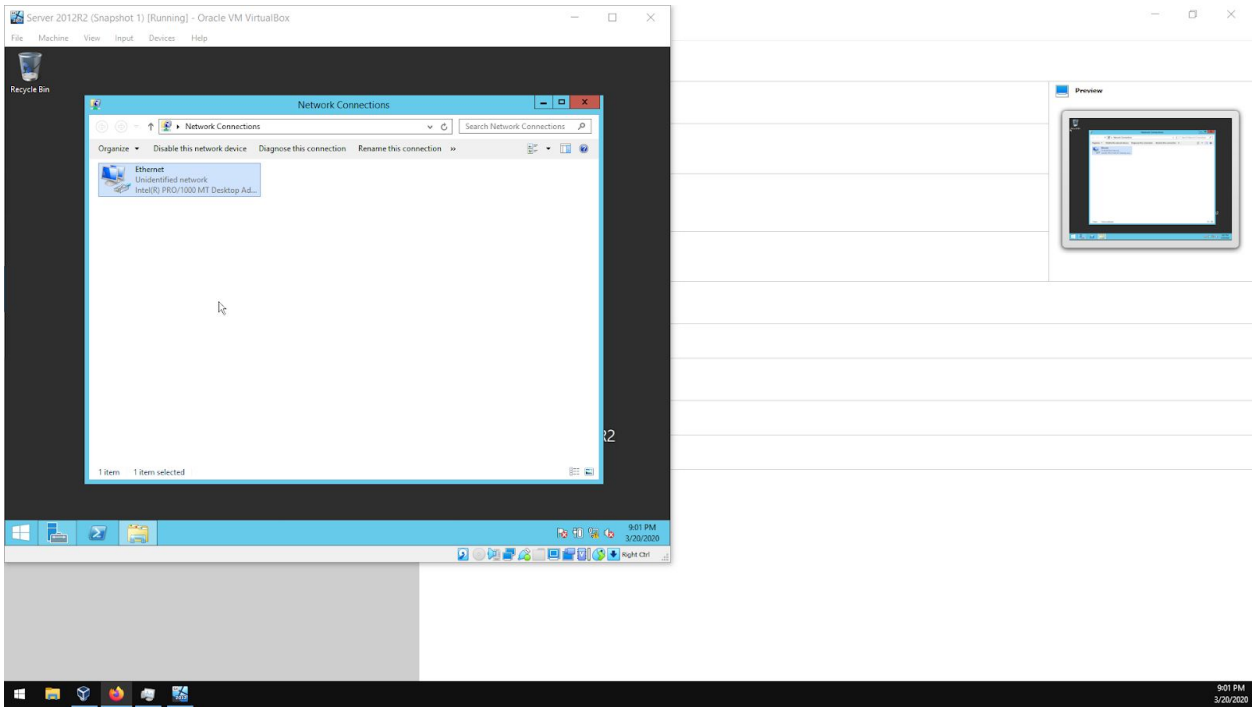
PowerShell - ipconfig /renew

ipconfig /renew should repopulate the Default Gateway field. But according to the error, the DHCP server can't be contacted. That makes sense since I've turned the DHCP option off for Static IP addressing in the VirtualBox settings.



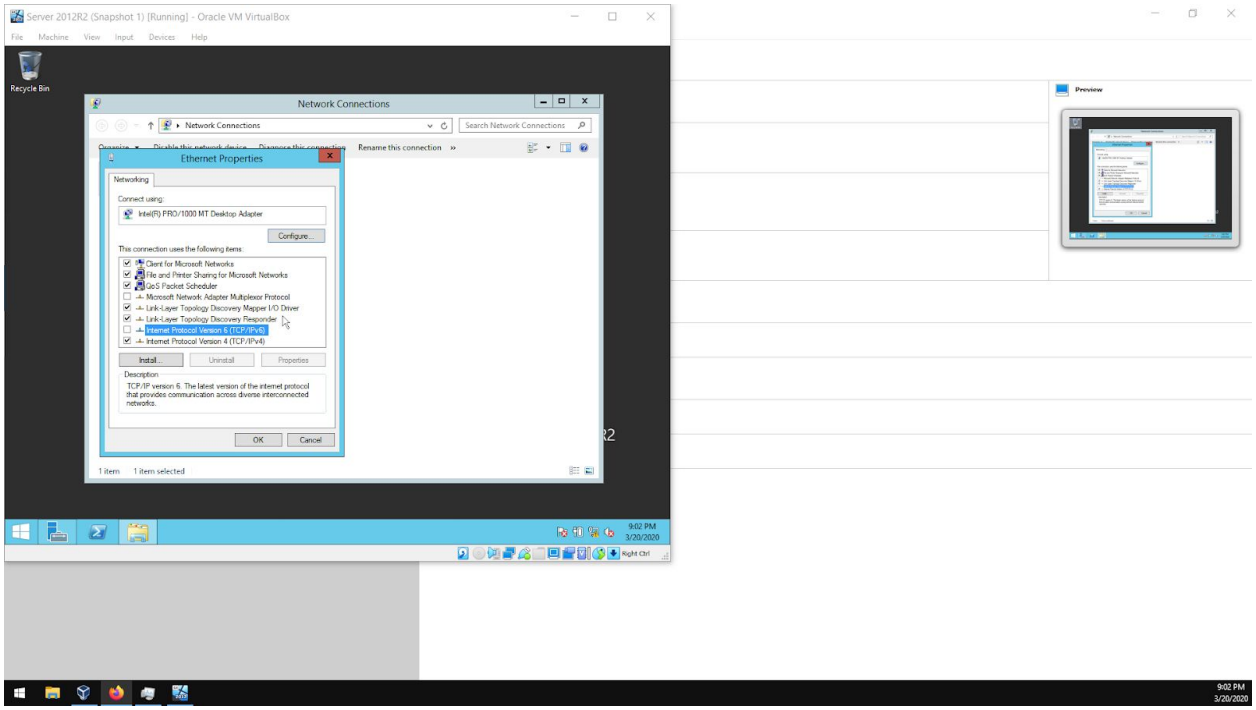
I shut down the VirtualBox Settings and enabled DHCP to observe any changes. Sure enough a Default Gateway has been reestablished. Perhaps there is an order to set up a Static IP address.

Network Connections



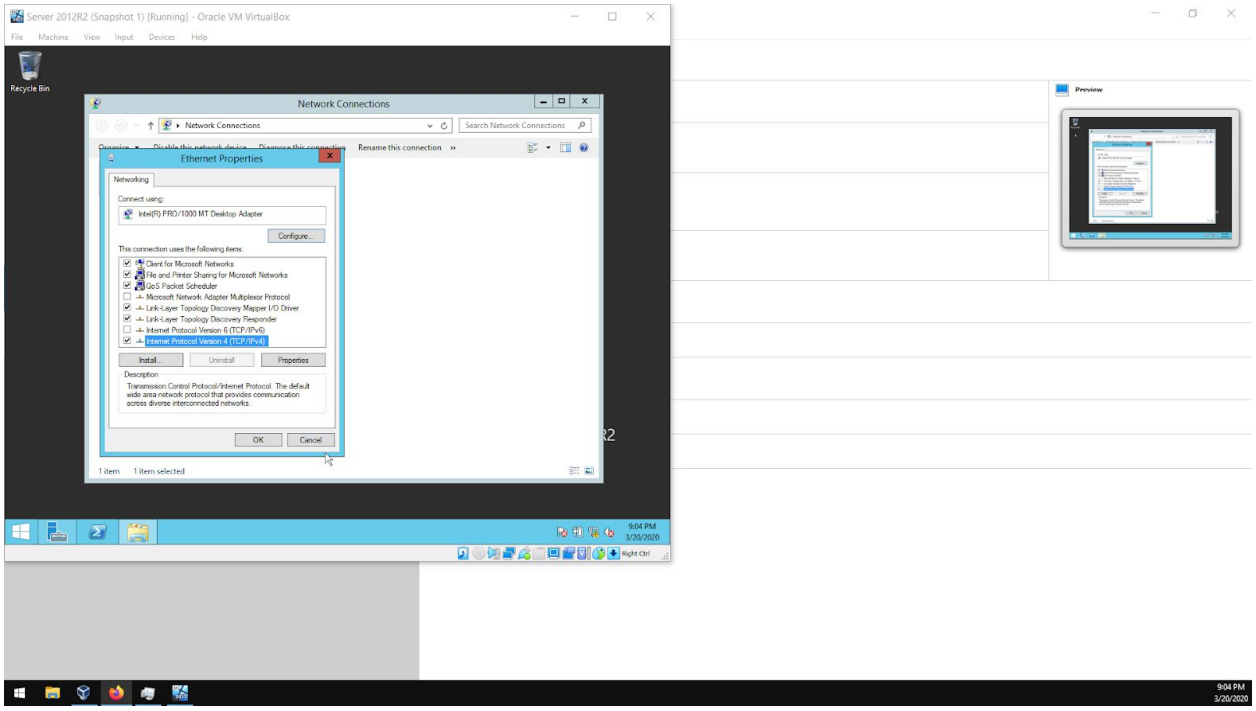
Right-Click on Ethernet to select properties.

Ethernet Properties



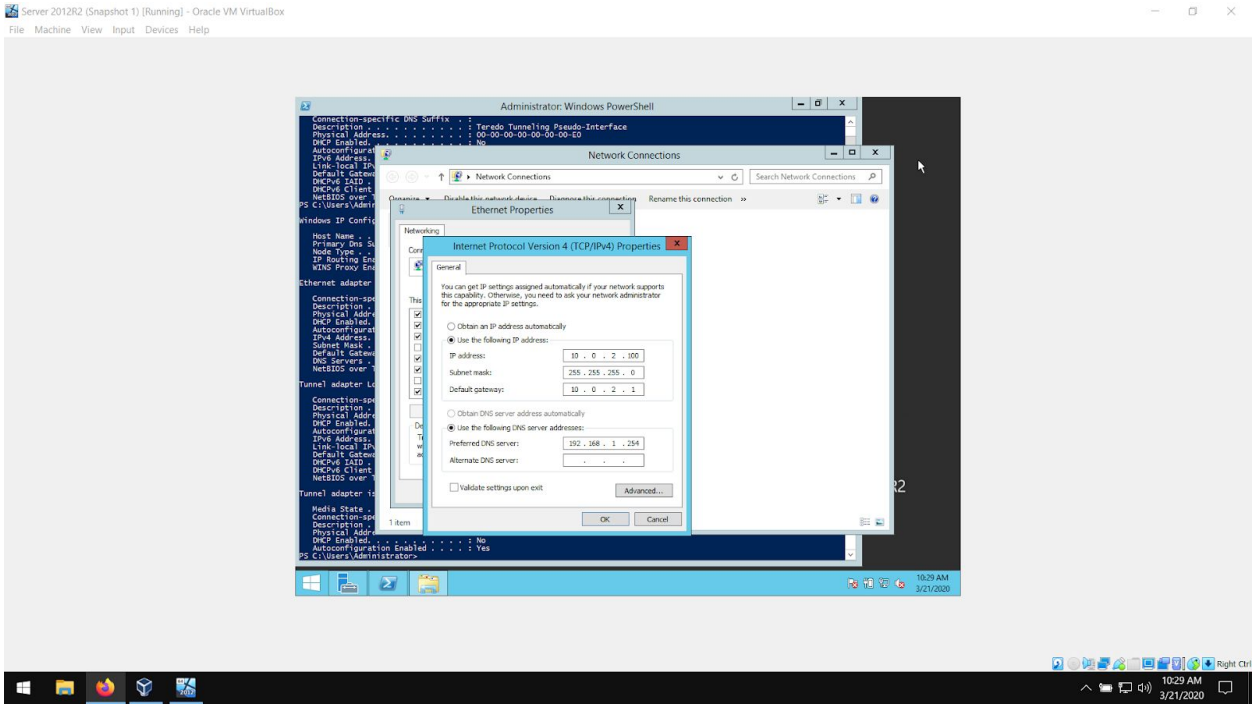
Since this is a IPv4 network, IPv6 is disabled. Select Configure to continue.

Ethernet Properties



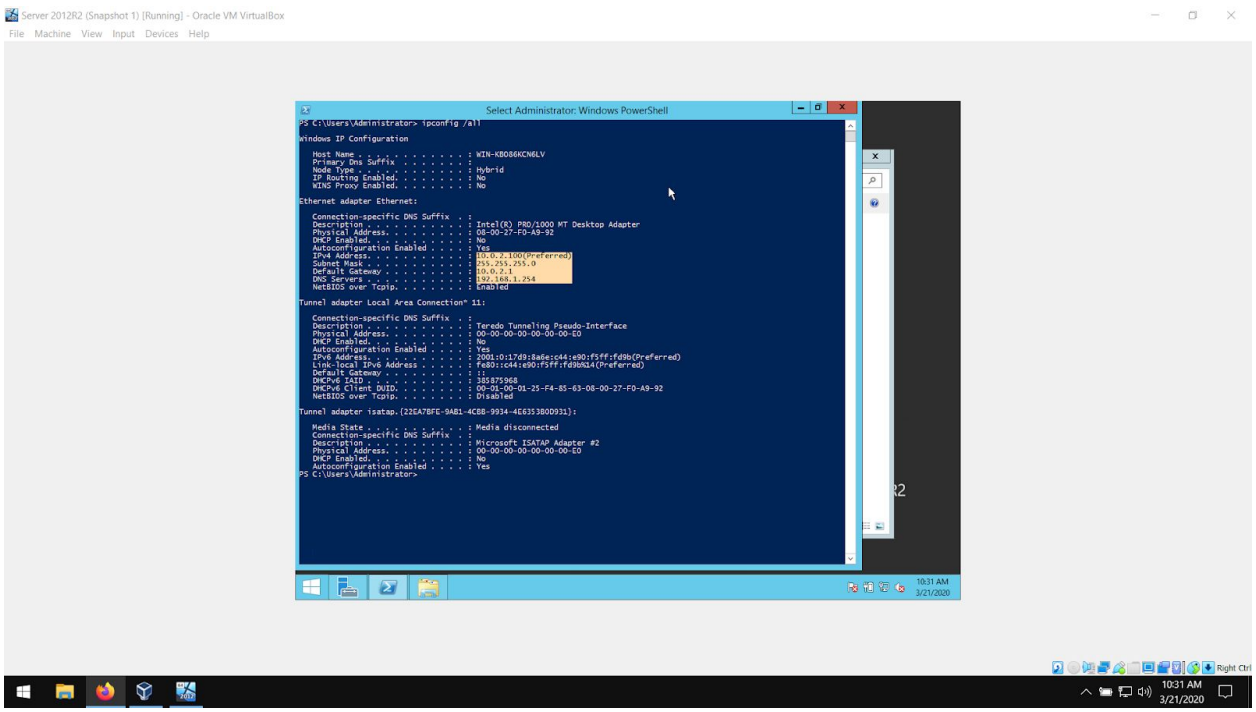
Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties.

Internet Protocol Version 4 (TCP/IPv4) Properties



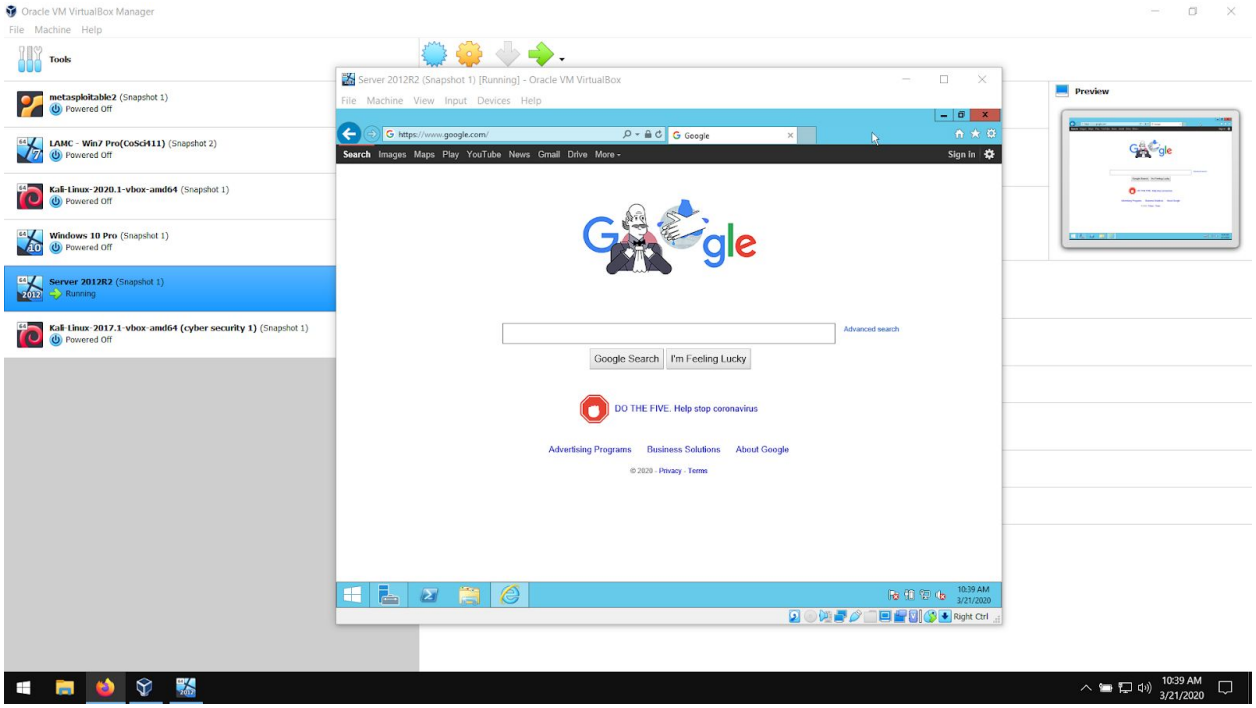
Select Use the following IP address. This is the step that corresponds to addressing an IP that DHCP would have done automatically.

PowerShell - ipconfig



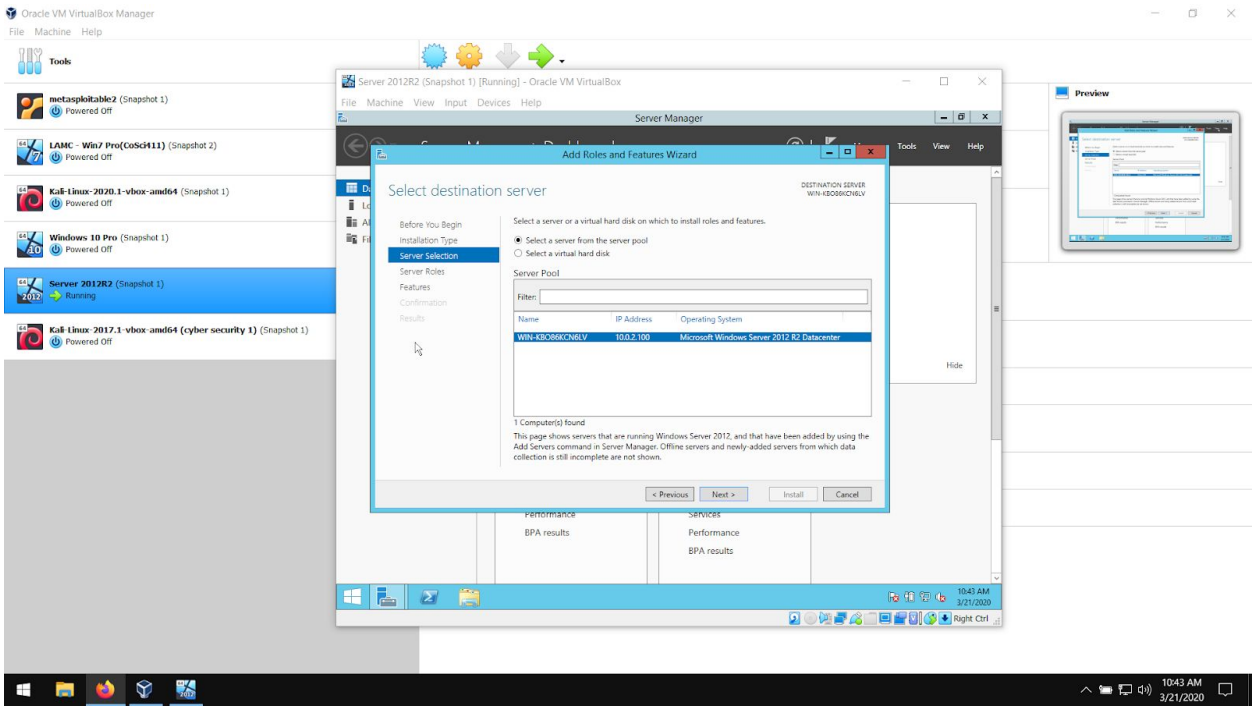
Using ipconfig /all verifies a Static IP address.

Internet Explorer



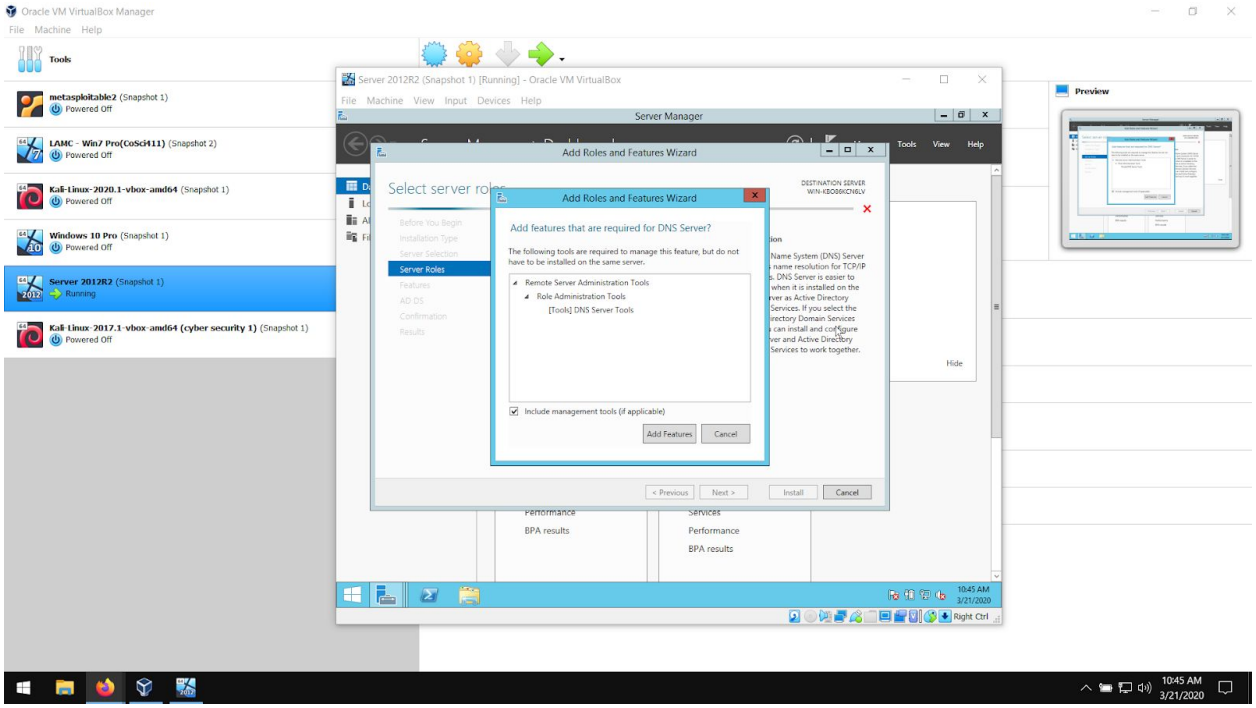
Internet connection verified.

Add Roles and Features Wizard - Server Pool



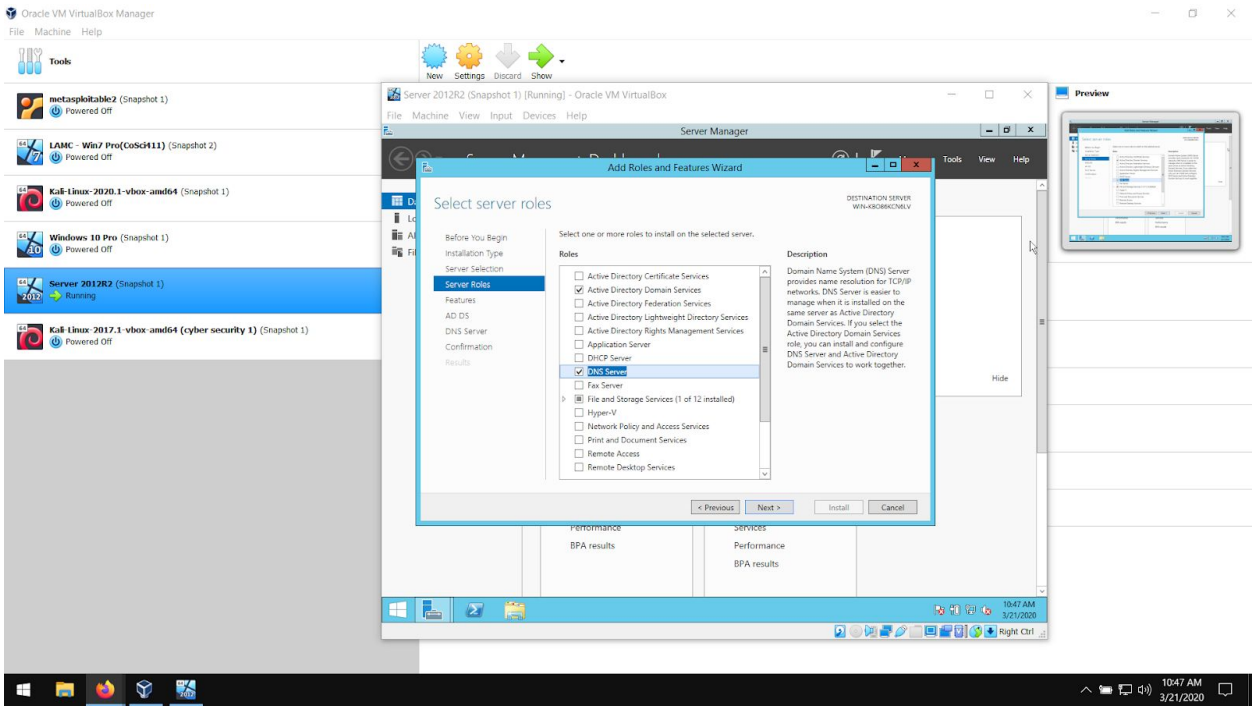
Back at Server manager, note the correct IP Address for the Destination server is displayed, 10.0.2.100

Add Roles and Features Wizard - Server Roles



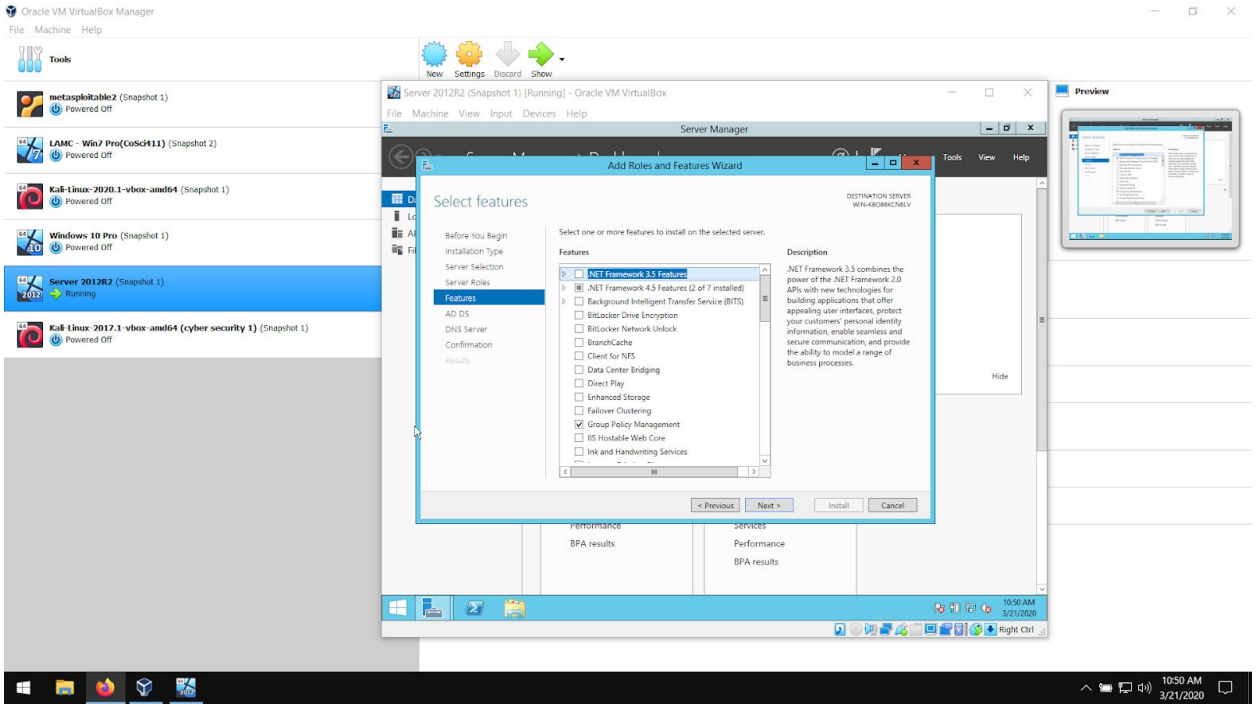
Confirmation box for DNS server. A similar configuration box appeared for Active Directory Domain Services

Add Roles and Features Wizard - Server Roles



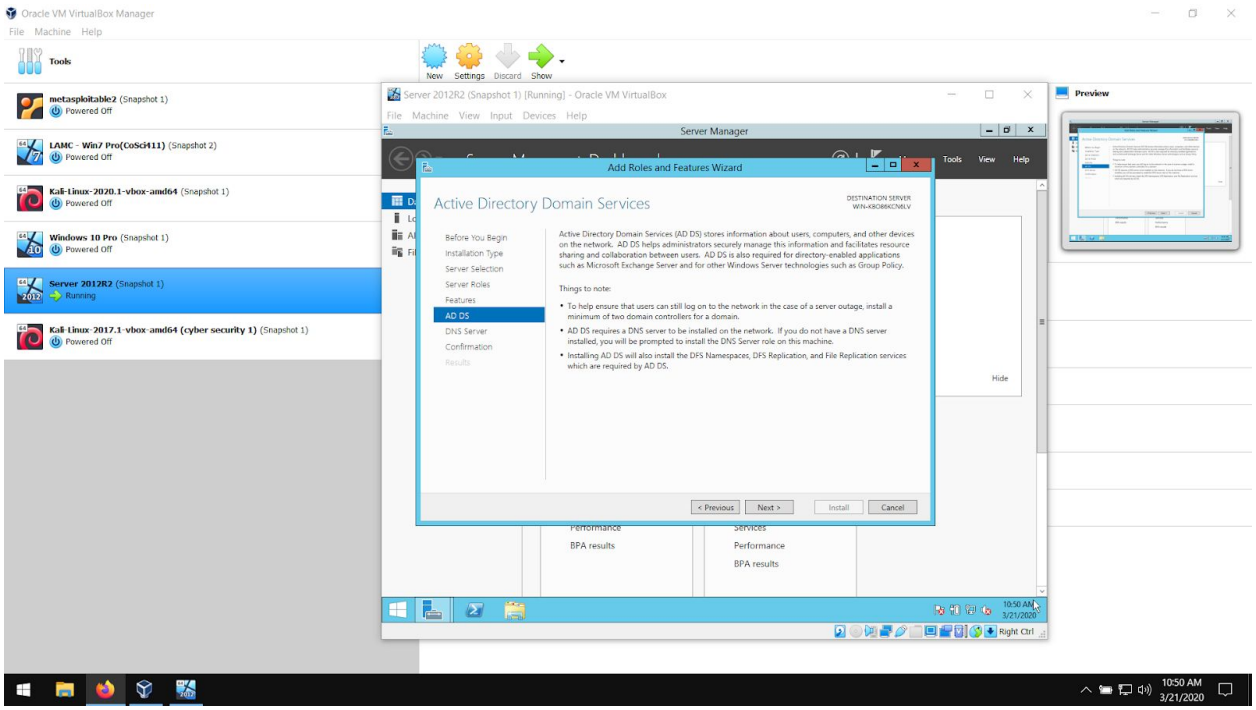
No reboot was required when adding the DNS Server role.

Add Roles and Features Wizard - Features



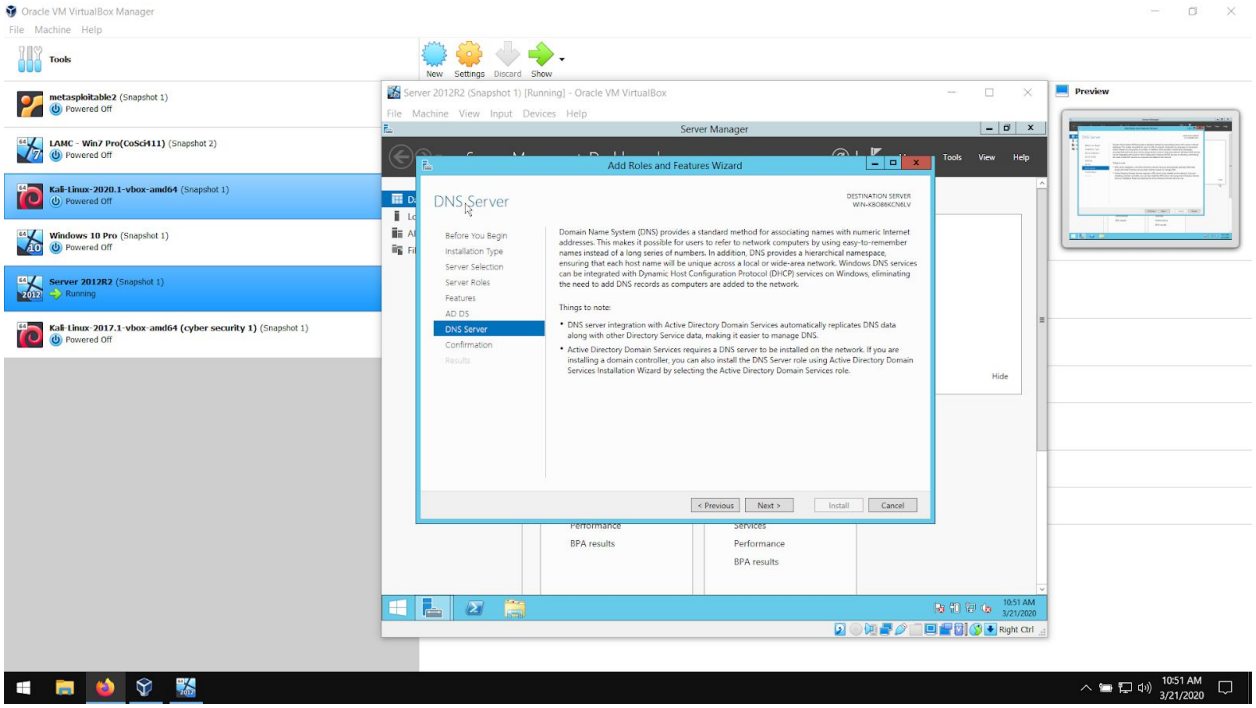
All defaults were selected.

Add Roles and Features Wizard - AD DS



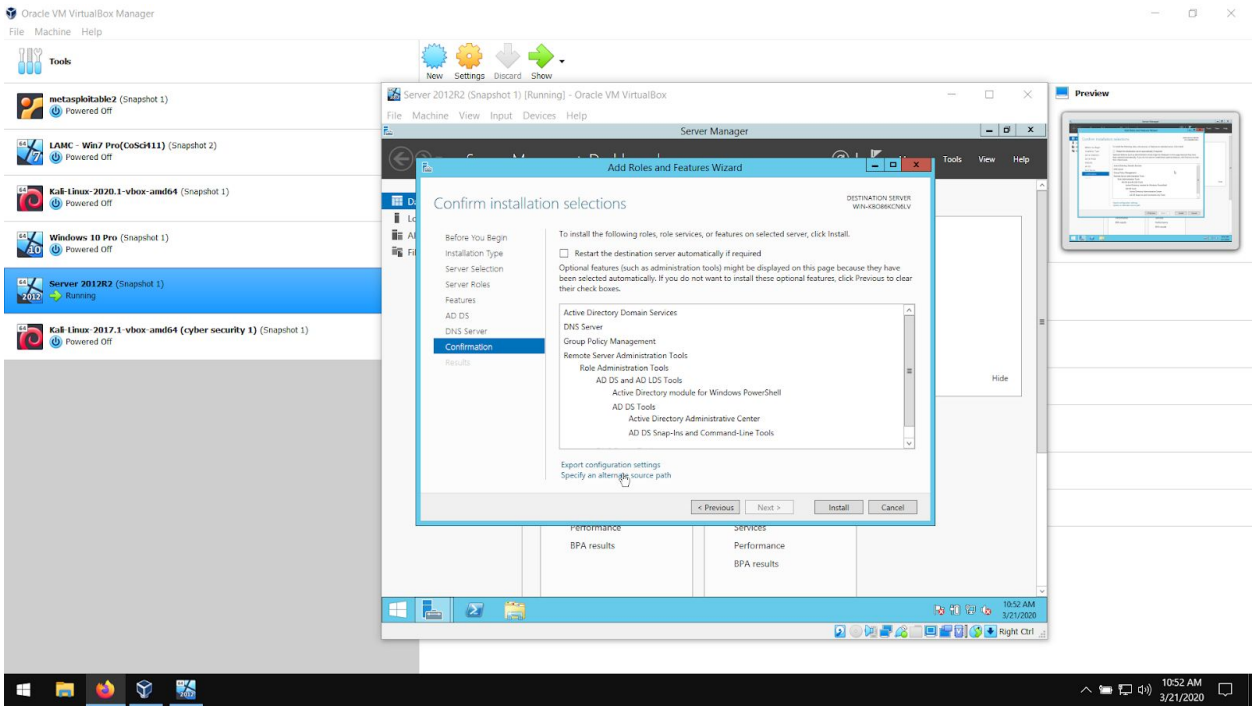
All defaults were selected.

Add Roles and Features Wizard - DNS Server



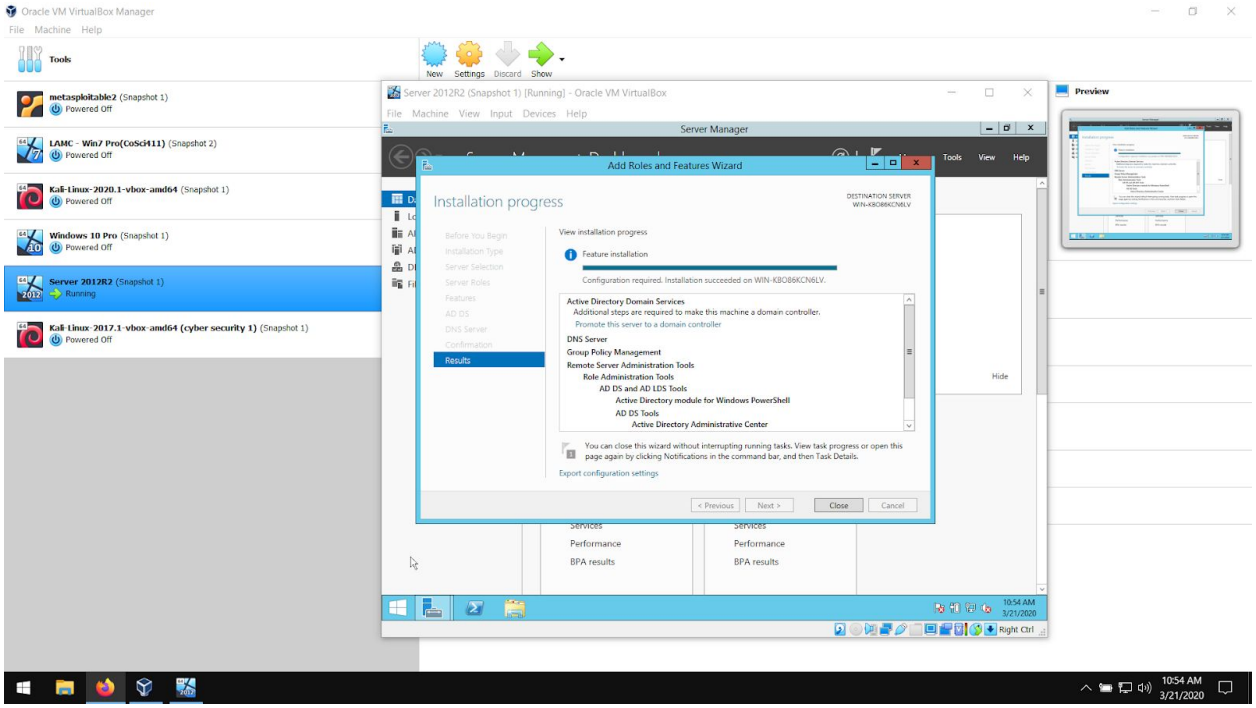
All defaults were selected.

Add Roles and Features Wizard - Confirmation



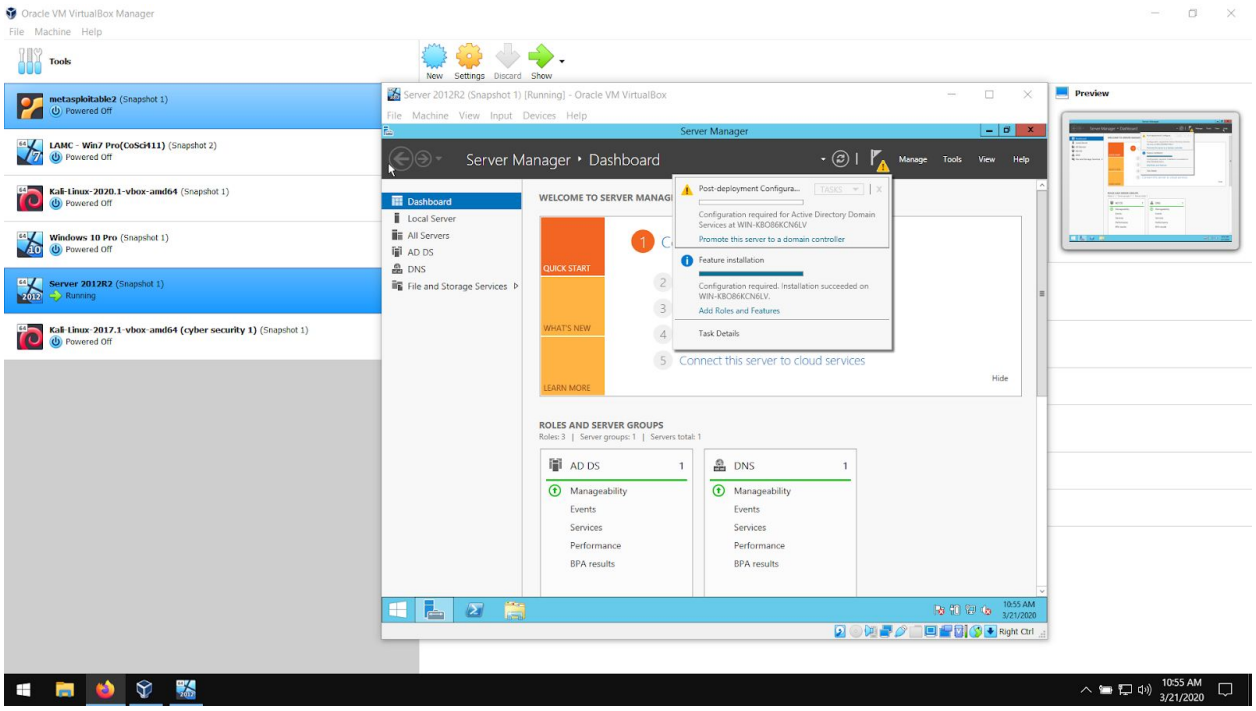
All defaults were selected. Clicking next will begin the installation process.

Add Roles and Features Wizard - Confirmation



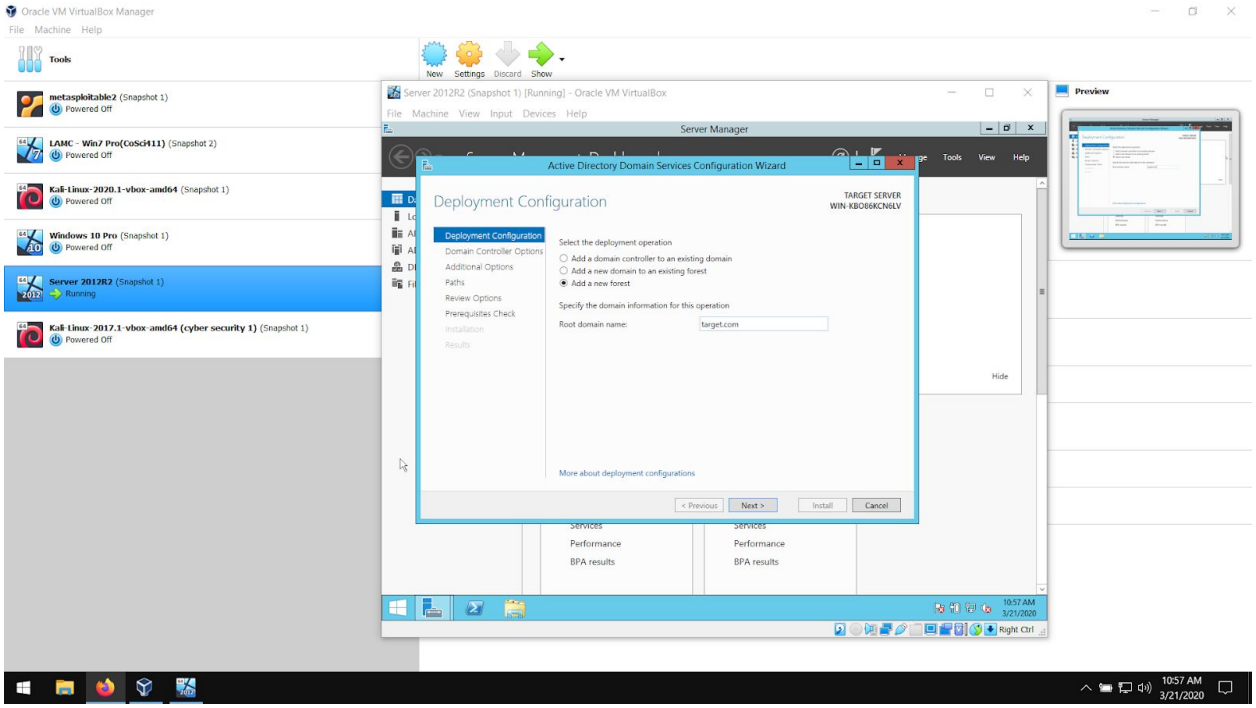
Installation succeeded.

Server Manager - Post Deployment Configuration



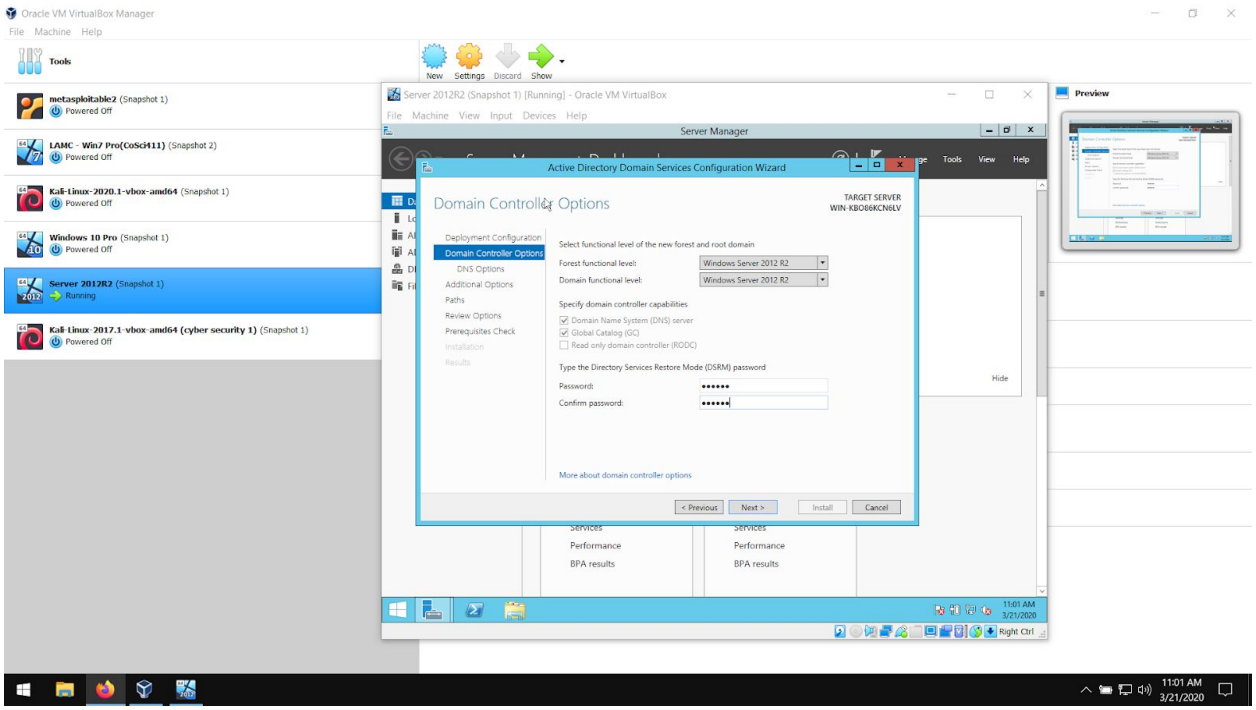
The server needs to be promoted to domain controller.

Deployment Configuration



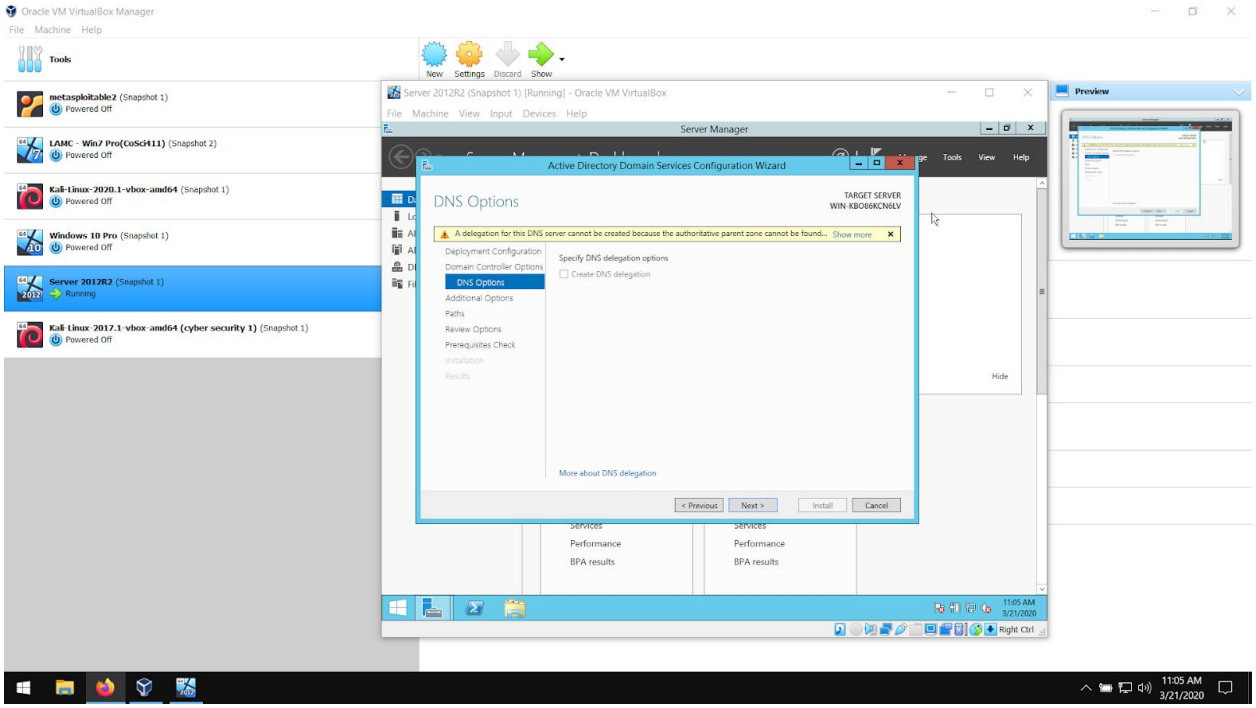
Selecting a forest will configure the Root domain name (target.com). Many domains can exist but only one root within a forest.

Active Directory Domain Services Configuration Wizard



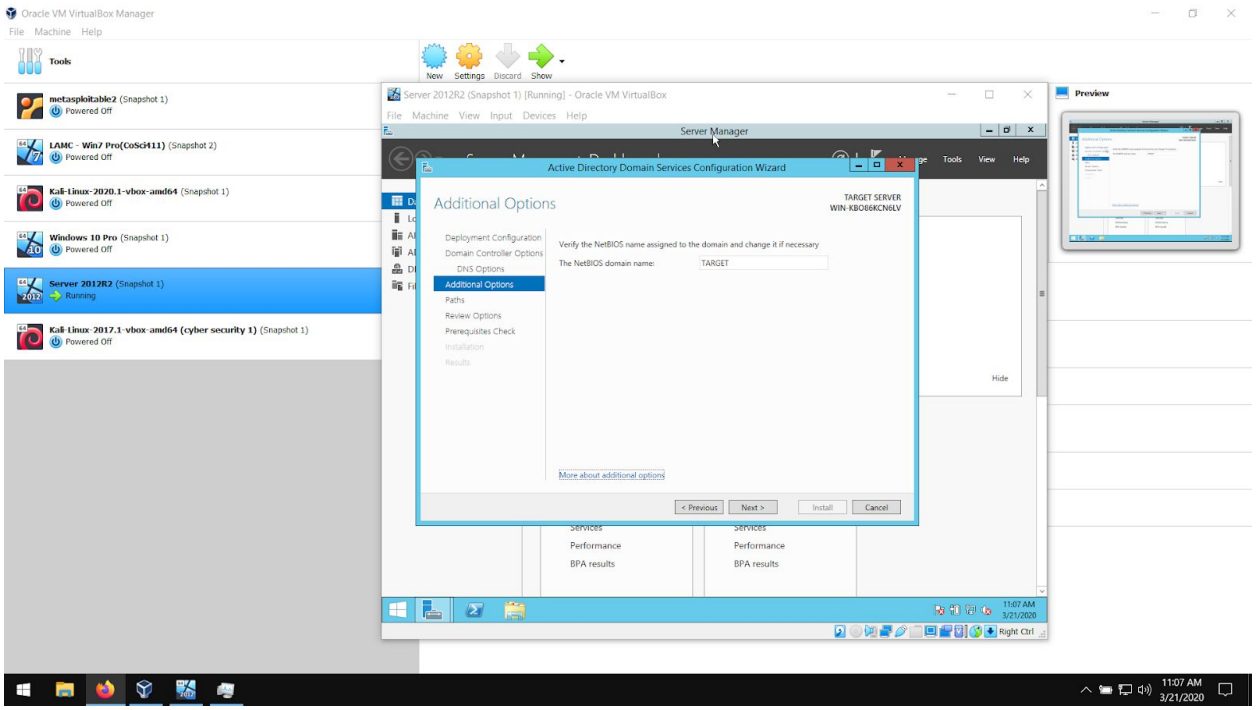
Choosing a password.

Active Directory Domain Services Configuration Wizard - DNS Options



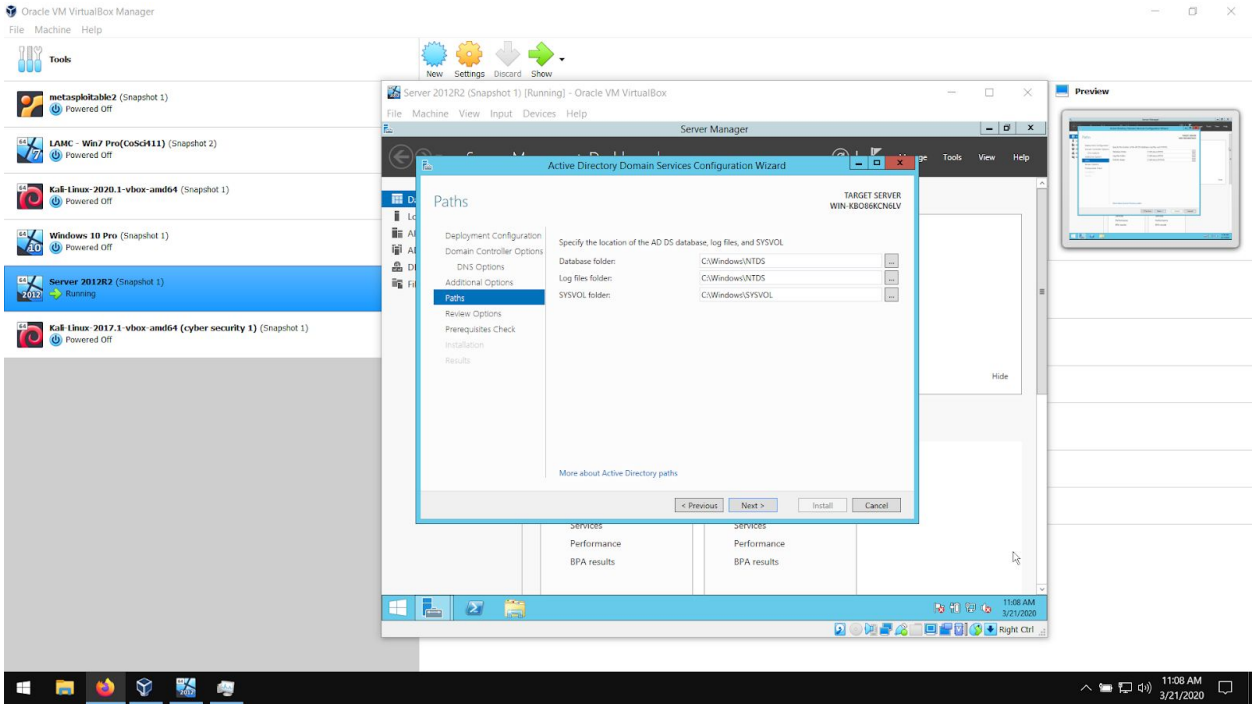
A yellow warning for DNS delegation is displayed.

Active Directory Domain Services Configuration Wizard - Additional Options



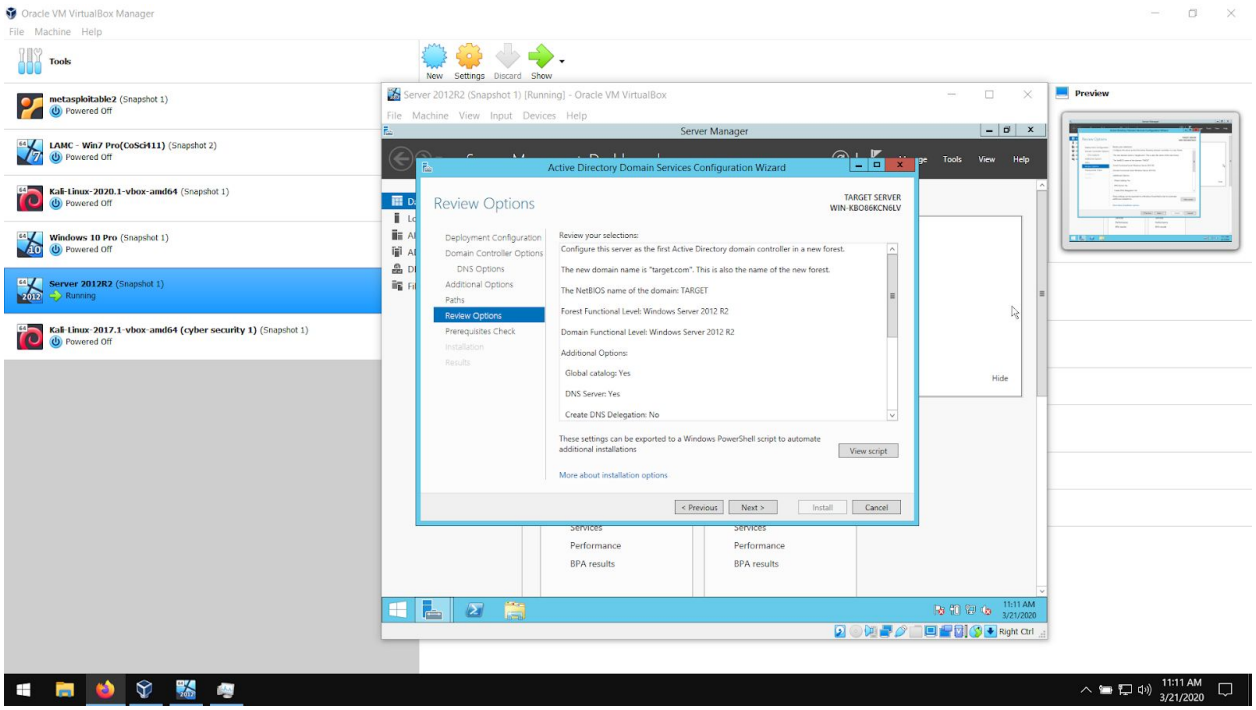
All defaults were selected.

Active Directory Domain Services Configuration Wizard - Paths



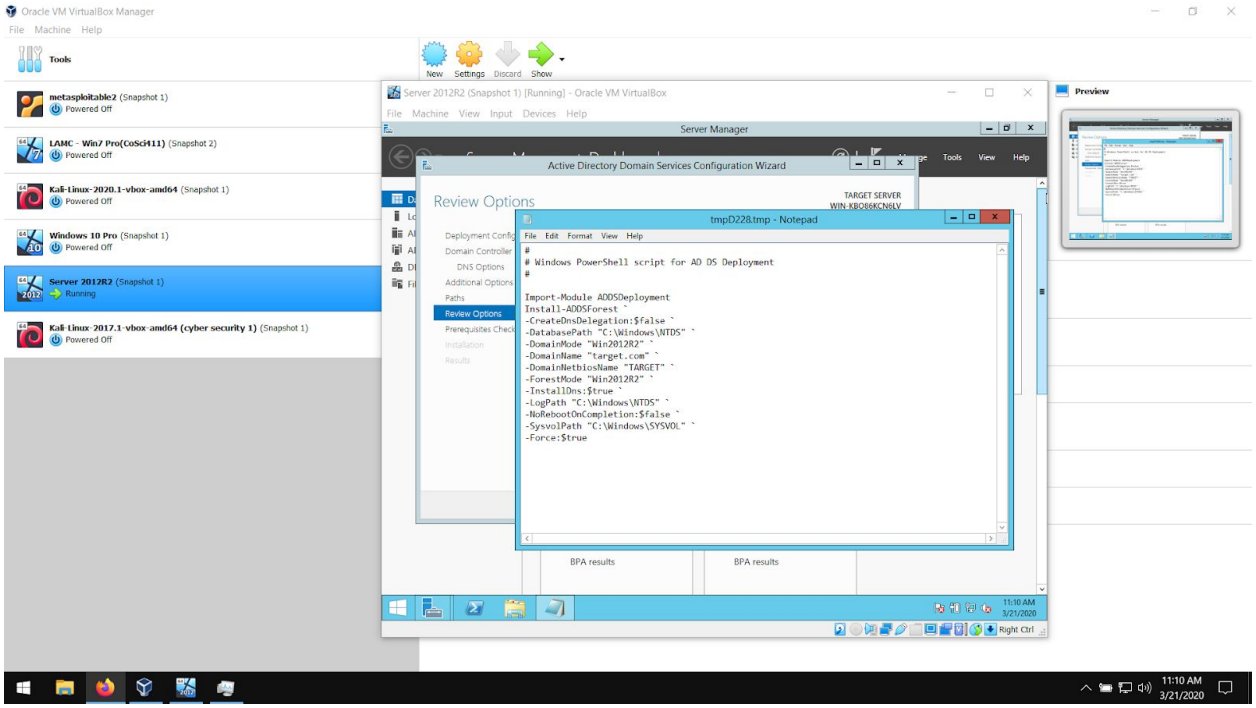
These are important file paths to be aware of. All defaults were selected.

Active Directory Domain Services Configuration Wizard - Review Options



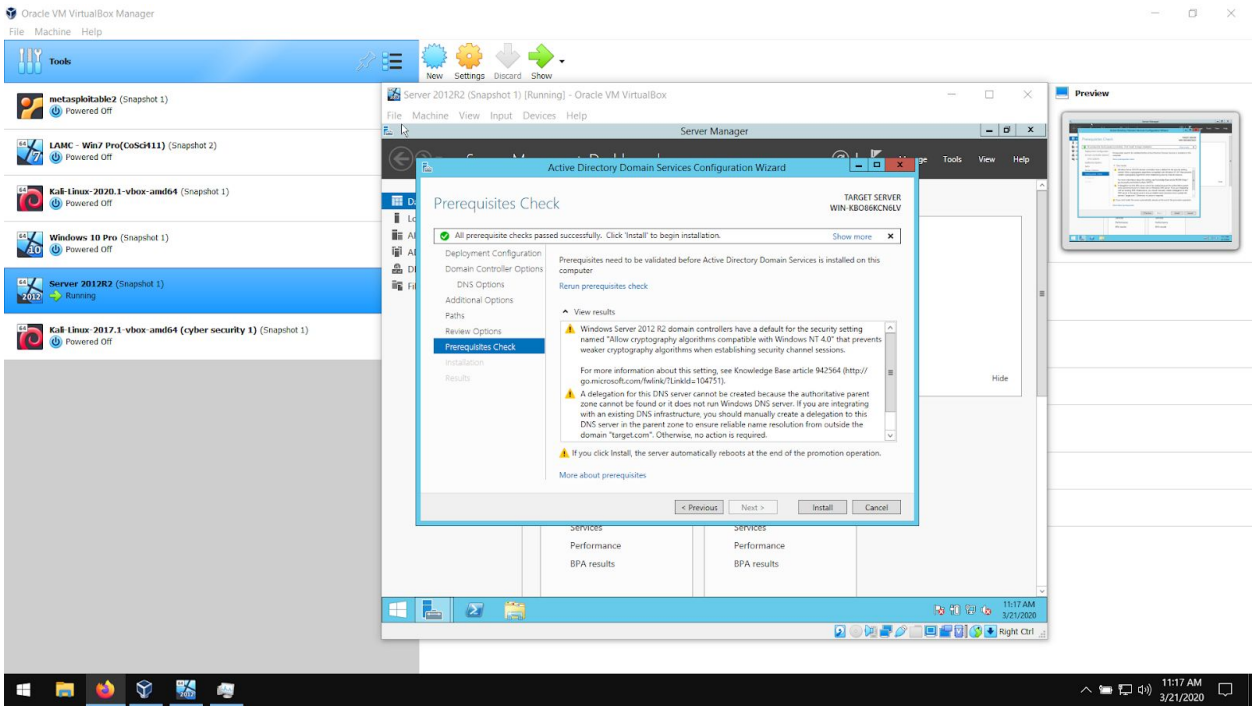
A summary of selections made during the Deployment configuration.

Active Directory Domain Services Configuration Wizard - Review Options



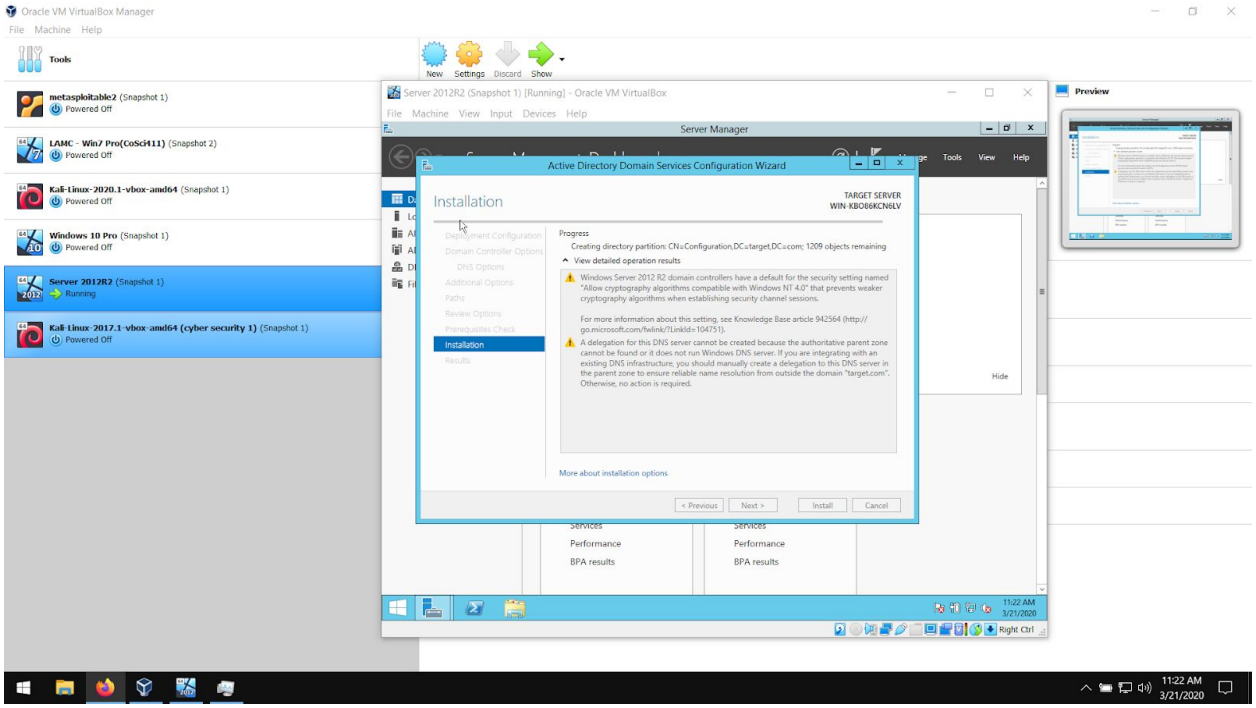
A PowerShell script has been generated for future use on other systems.

Active Directory Domain Services Configuration Wizard - Prerequisite Check



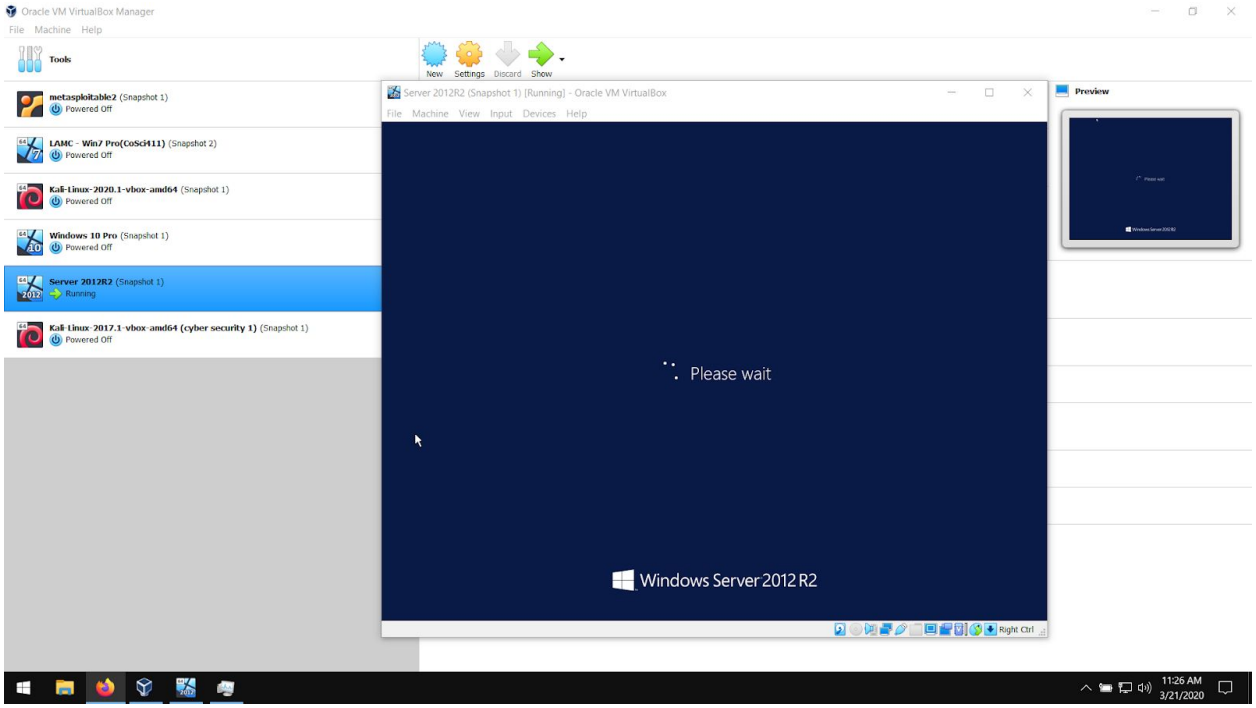
All prerequisites checks have passed, next step is installation.

Active Directory Domain Services Configuration Wizard - Installation



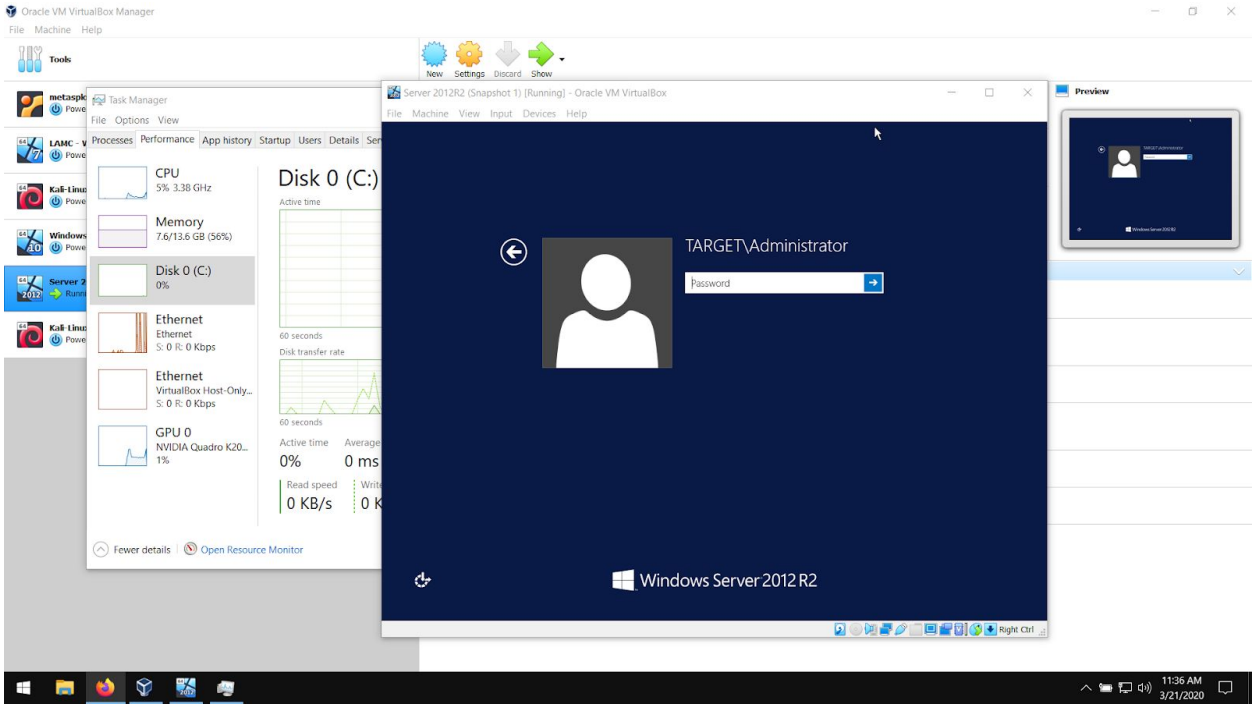
Installation has begun and may take a while.

Active Directory Domain Services Configuration Wizard - Installation



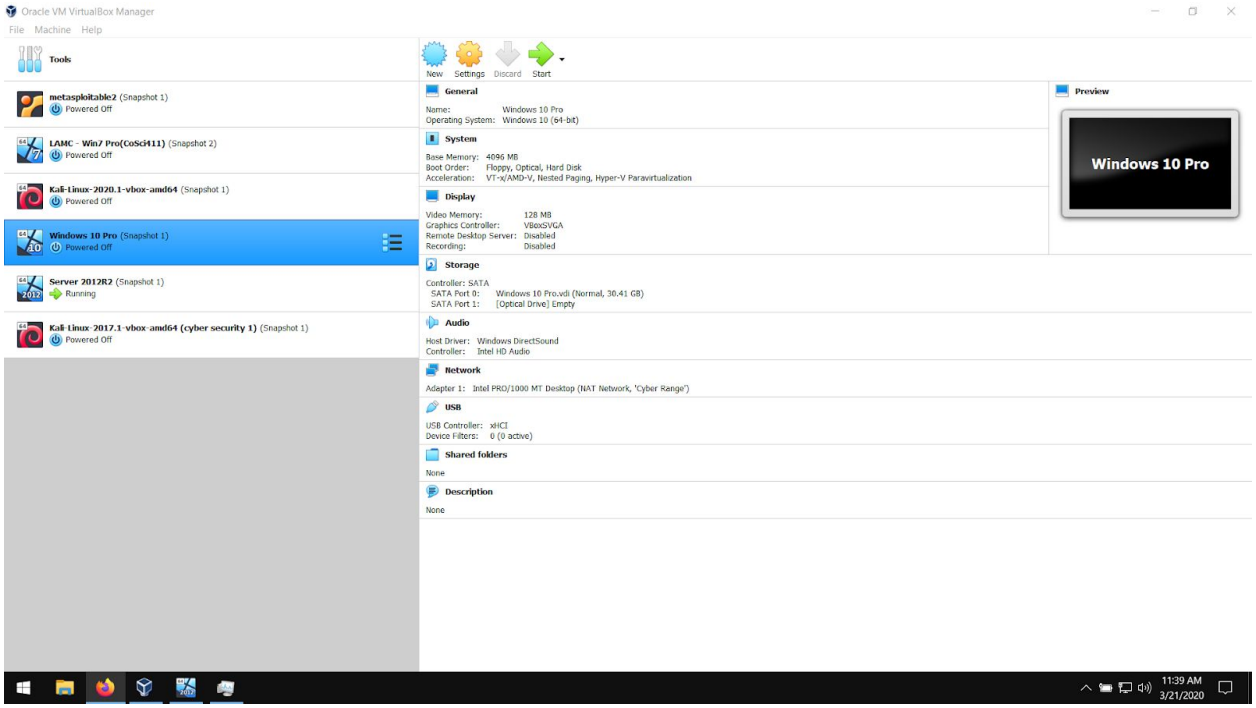
The VirtualBox restarted and is finishing up the installation of the deployment.

Login



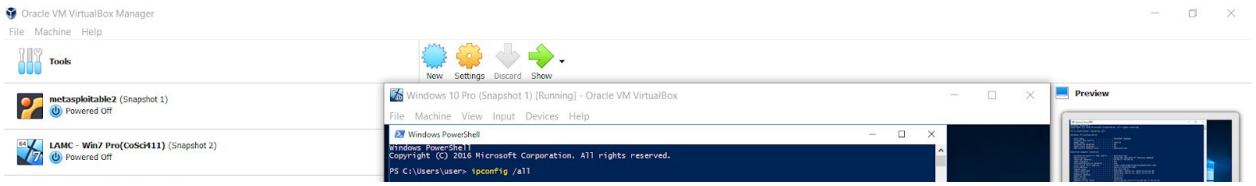
TARGET/Administrator verifies a domain administrator account has been provisioned.

VirtualBox - main menu



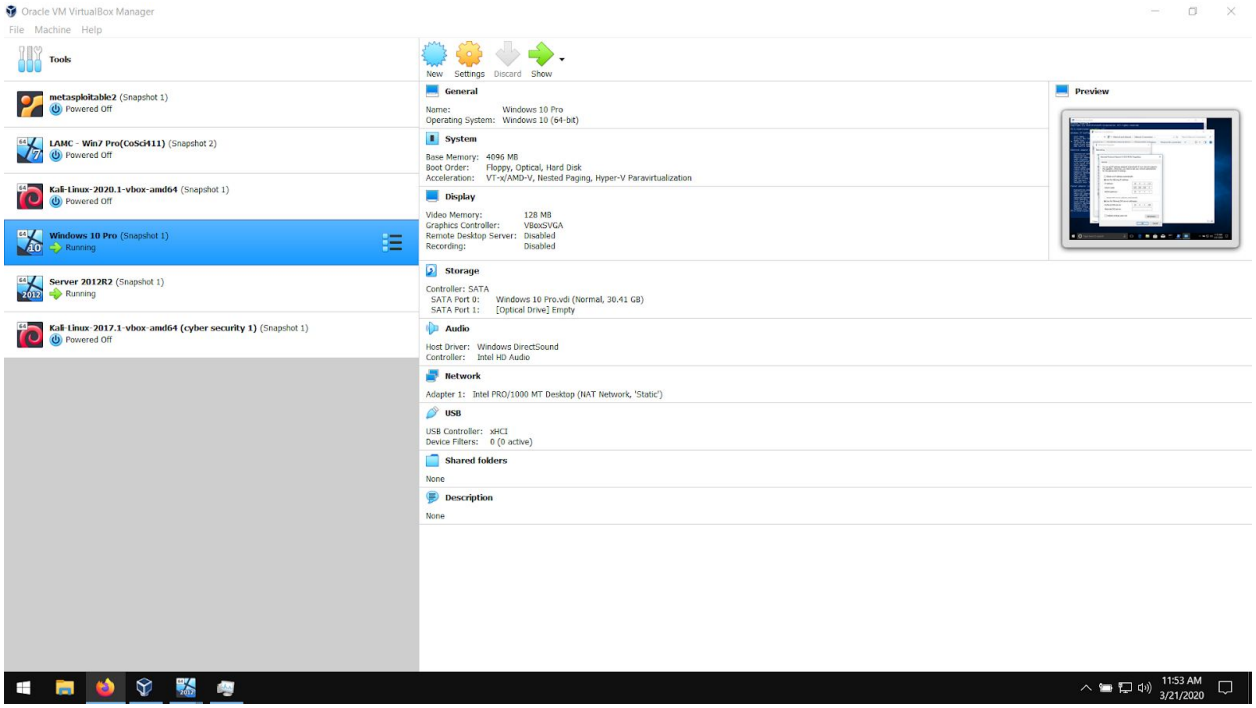
Back at the VirtualBox main menu, Windows 10 Pro will be started with it's network set to DHCP enabled. Windows 10 Pro will verify if the domain controller server is working.

Windows 10 Pro - ipconfig



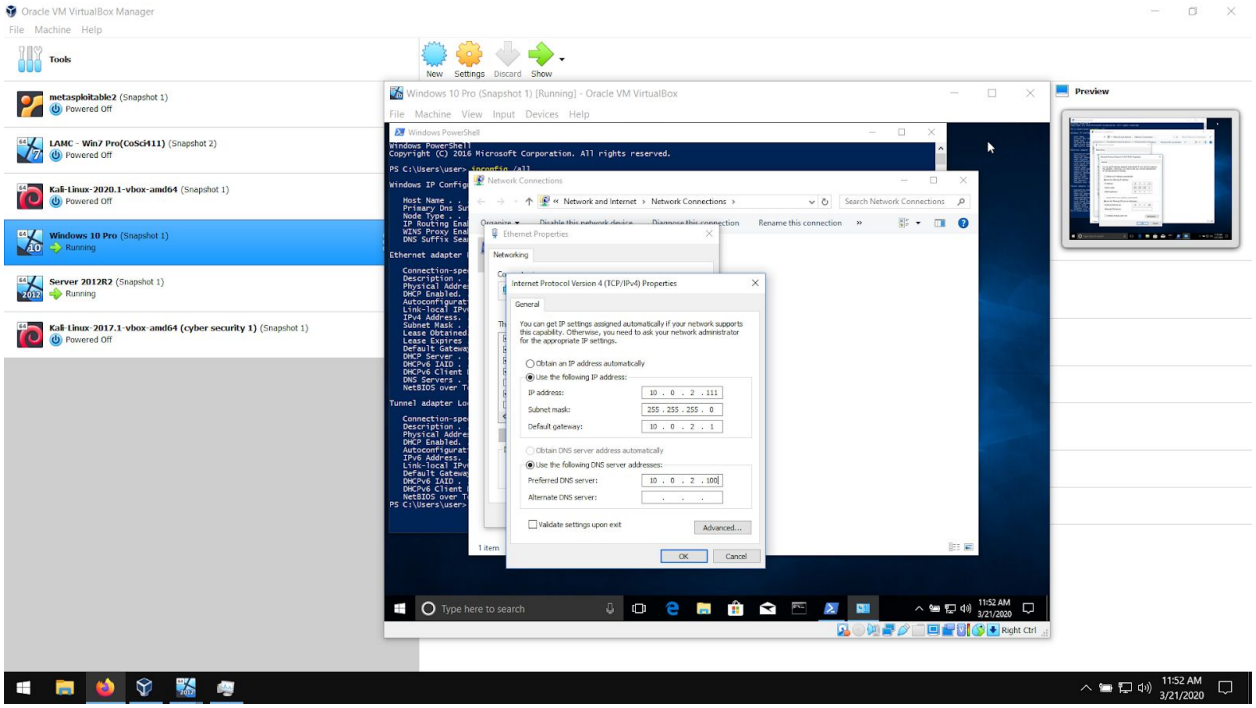
ipconfig /all is used to verify the incorrect IP addressing.

VirtualBox - main menu



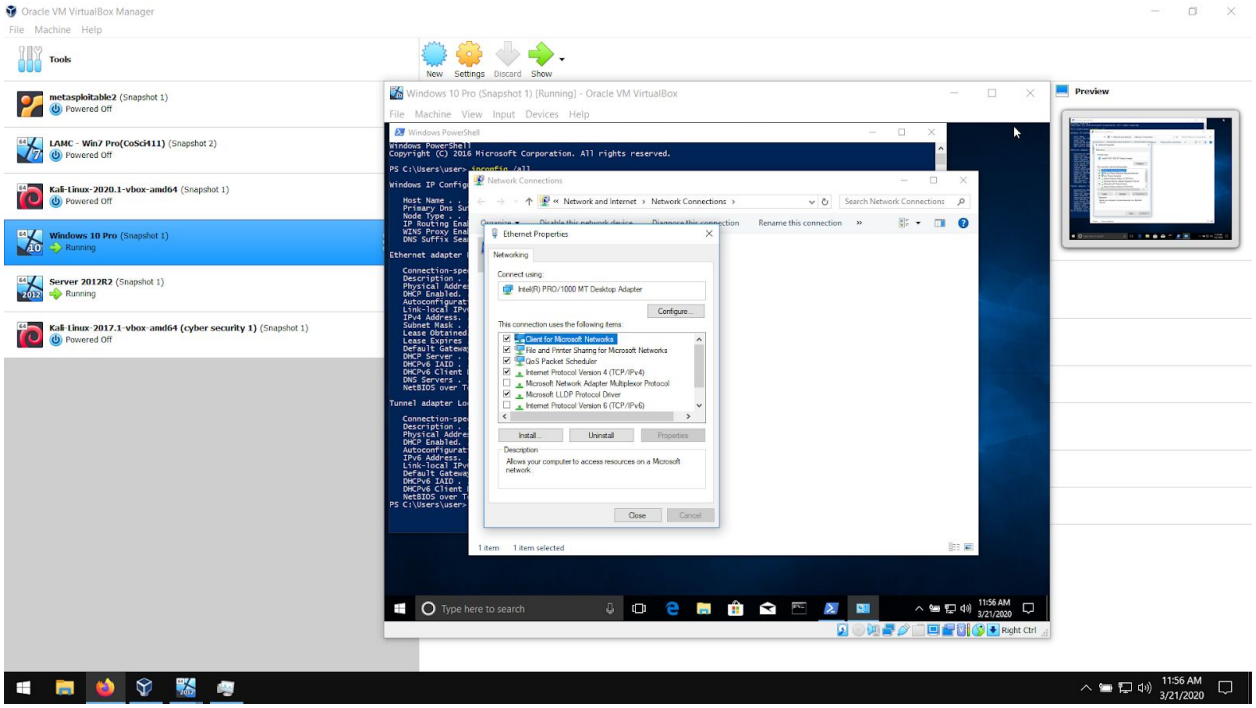
With Windows 10 Pro still running, the network was changed to a Static one.

Network Connections - IPv4 properties



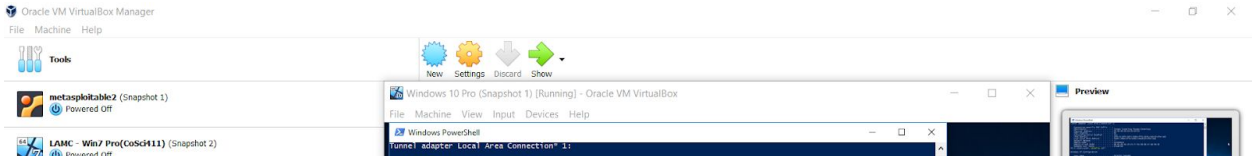
The connection needs to be set as static. The IP address will be an increment of the original 10.0.2.100. The preferred DNS server will be the IP of the domain controller running on Server 2012R2.

Network Connections - Ethernet Properties



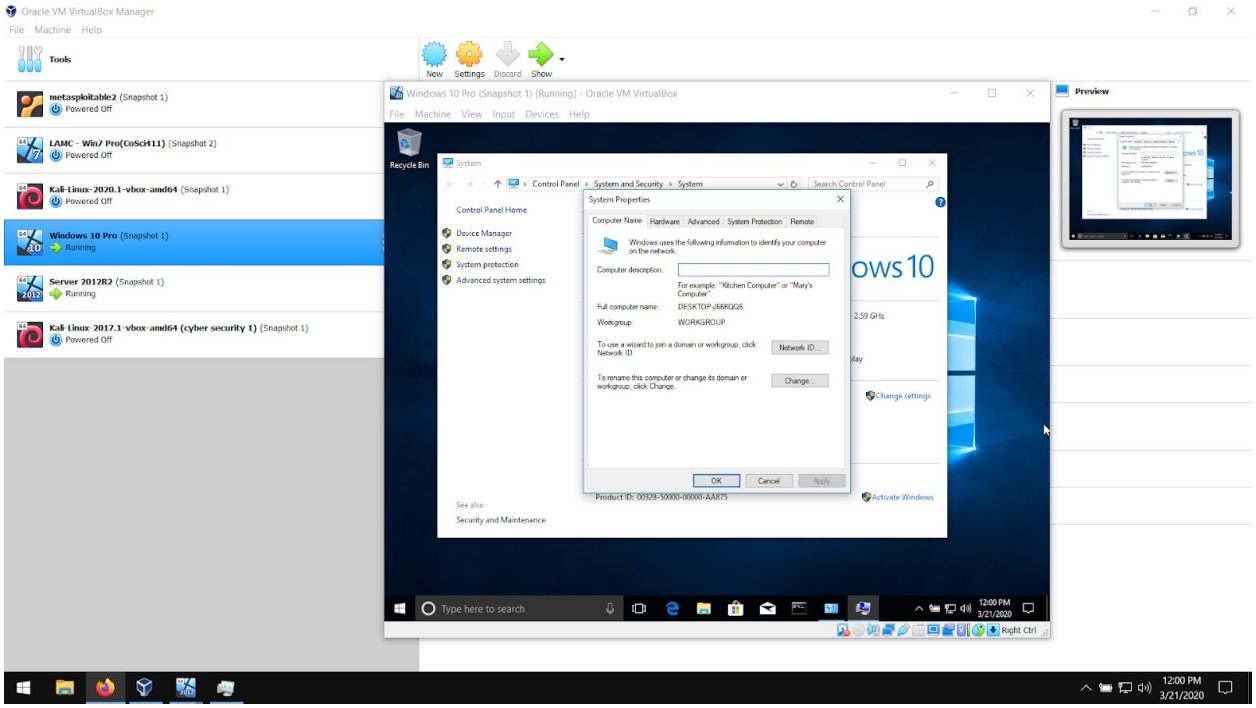
Note that IPv6 has been turned off.

PowerShell - ipconig



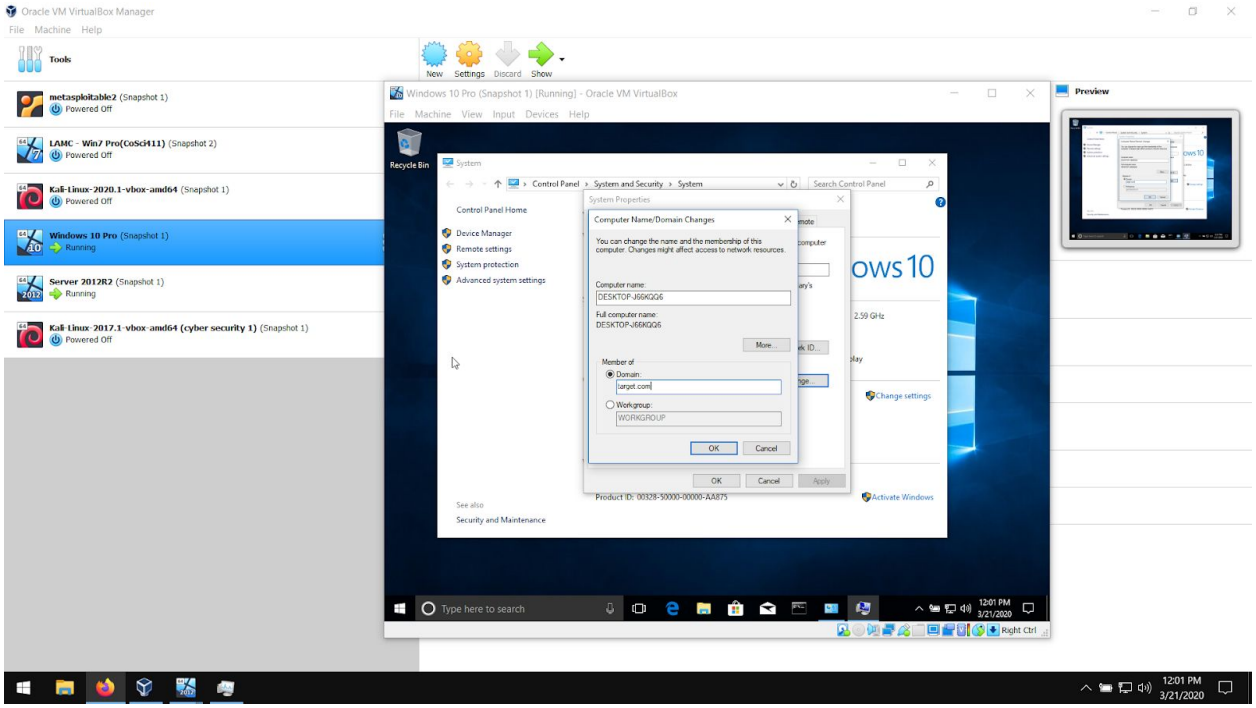
To verify the correct settings, ipconfig /all is used again.

System - System Properties

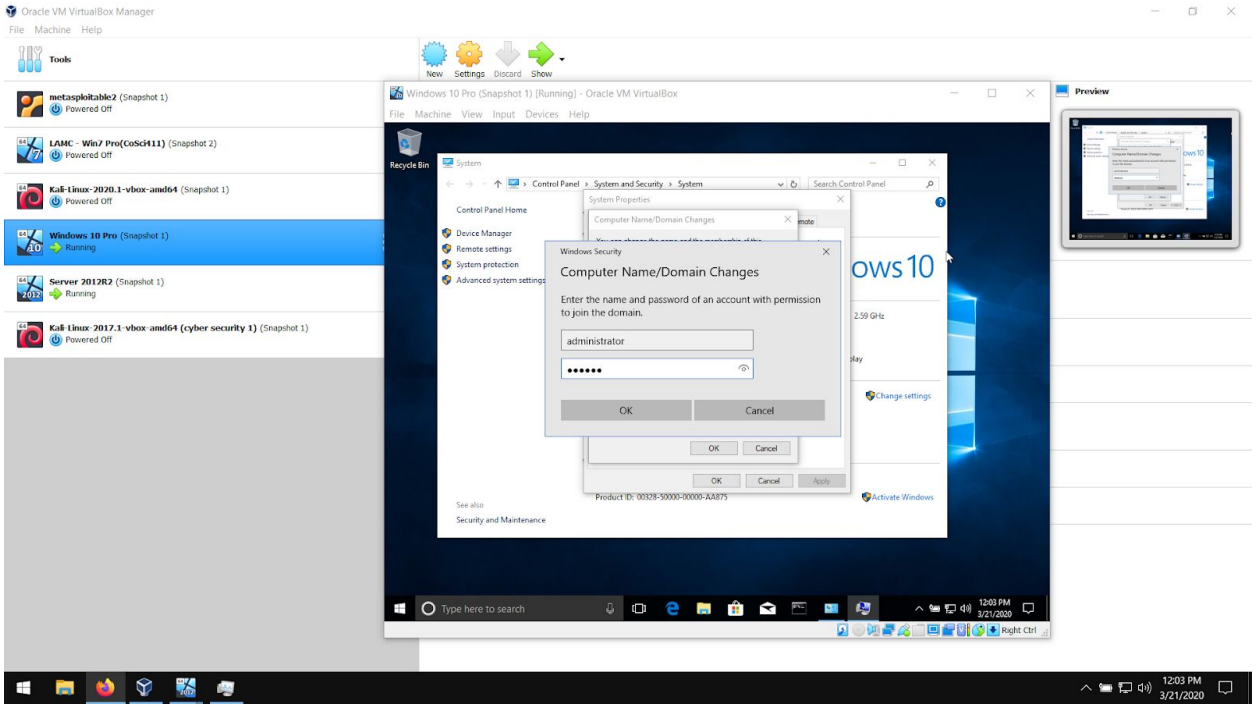


The system needs to now join the target domain.

System - Computer Name/Domain Changes

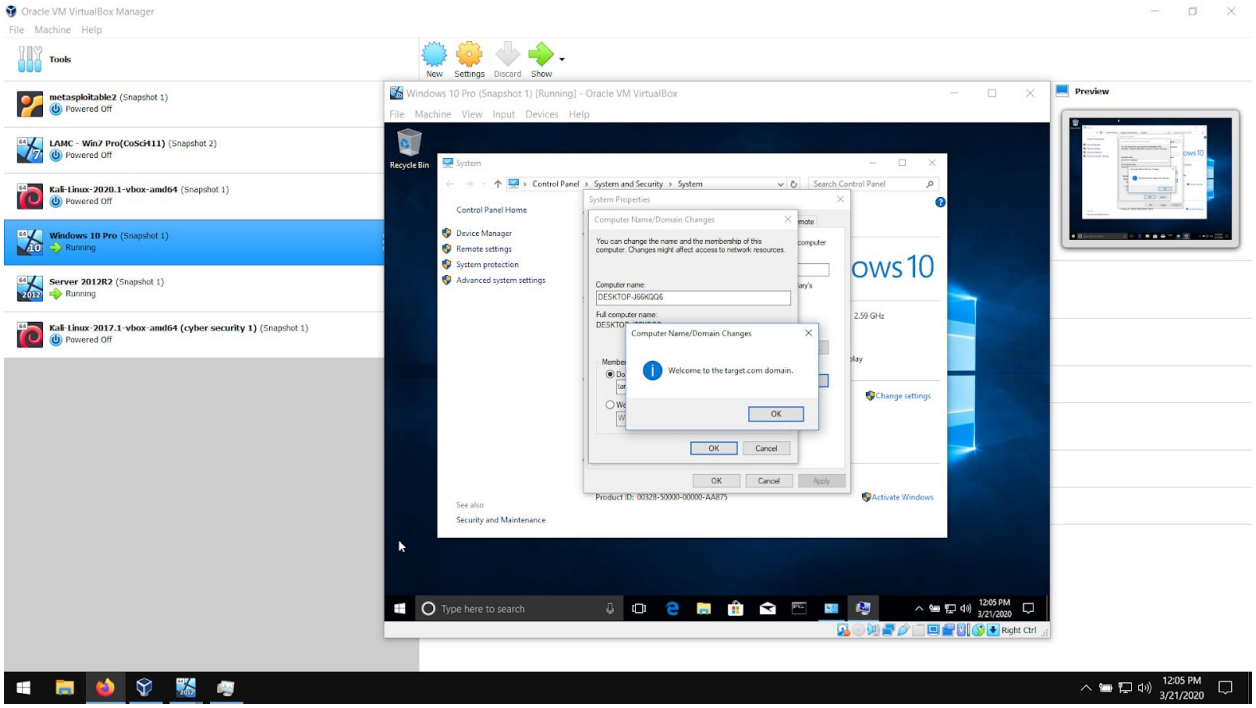


Note the change to member of domain: target.com



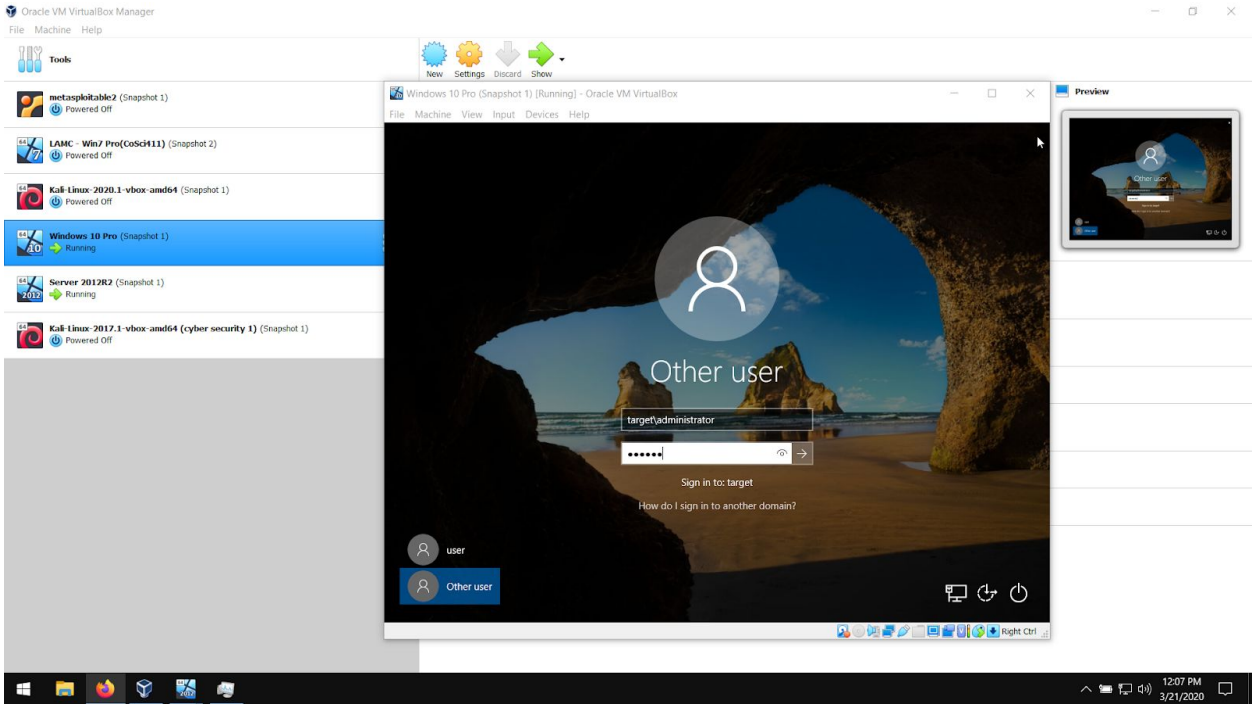
After OK, administrator and the password from the set up in the domain controller deployment is used.

Computer Name/Domain Changes



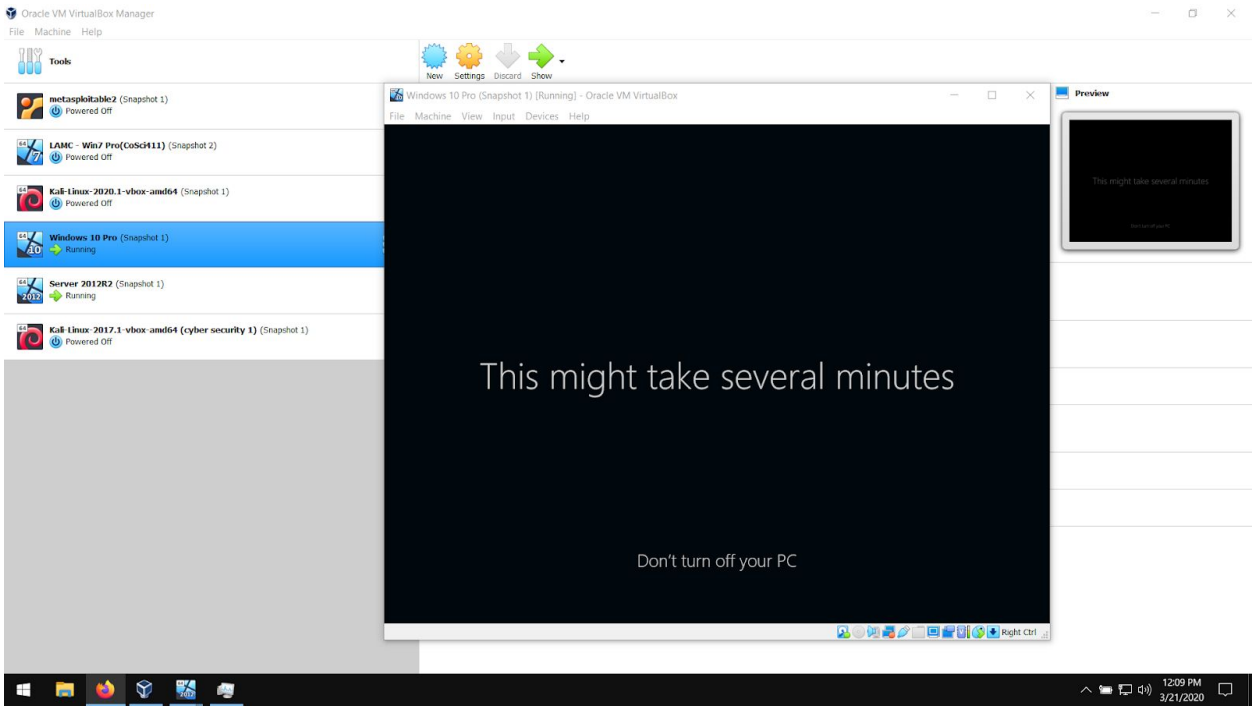
Success! The domain was found and connected.

Login - Other user



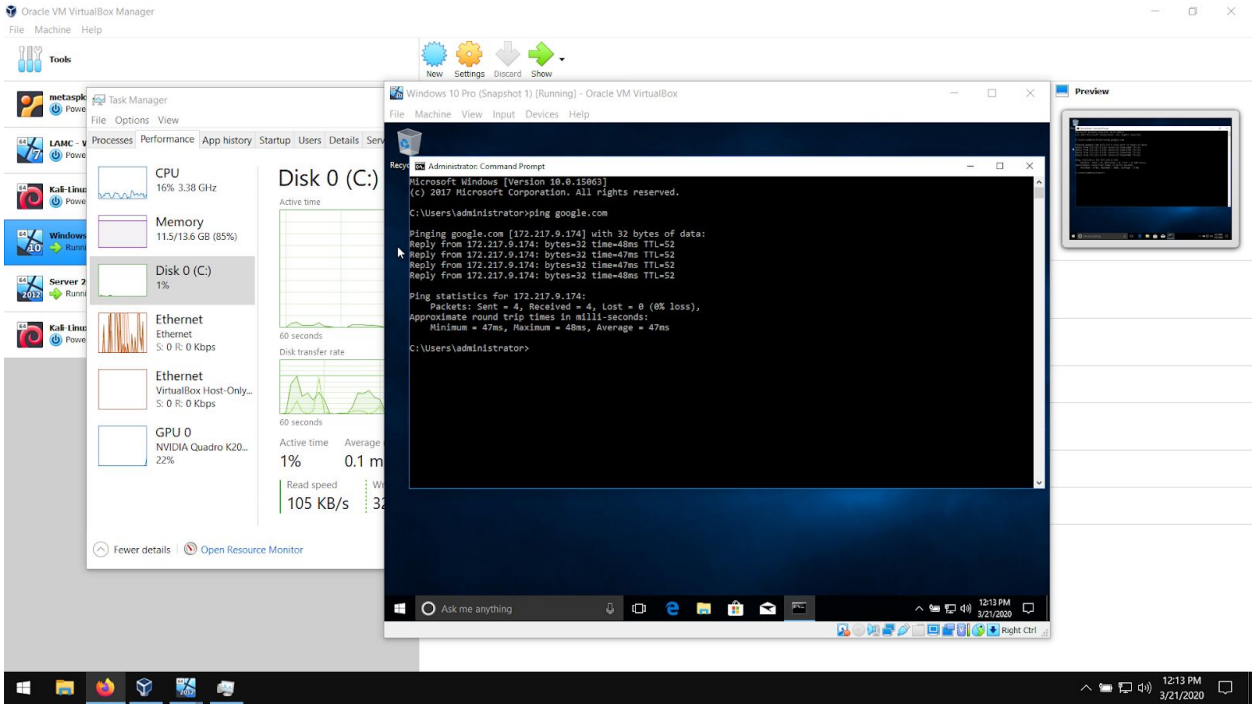
Note that you have to use “other user” to sign into the new domain. The deployment domain password is used.

Login - initial domain login



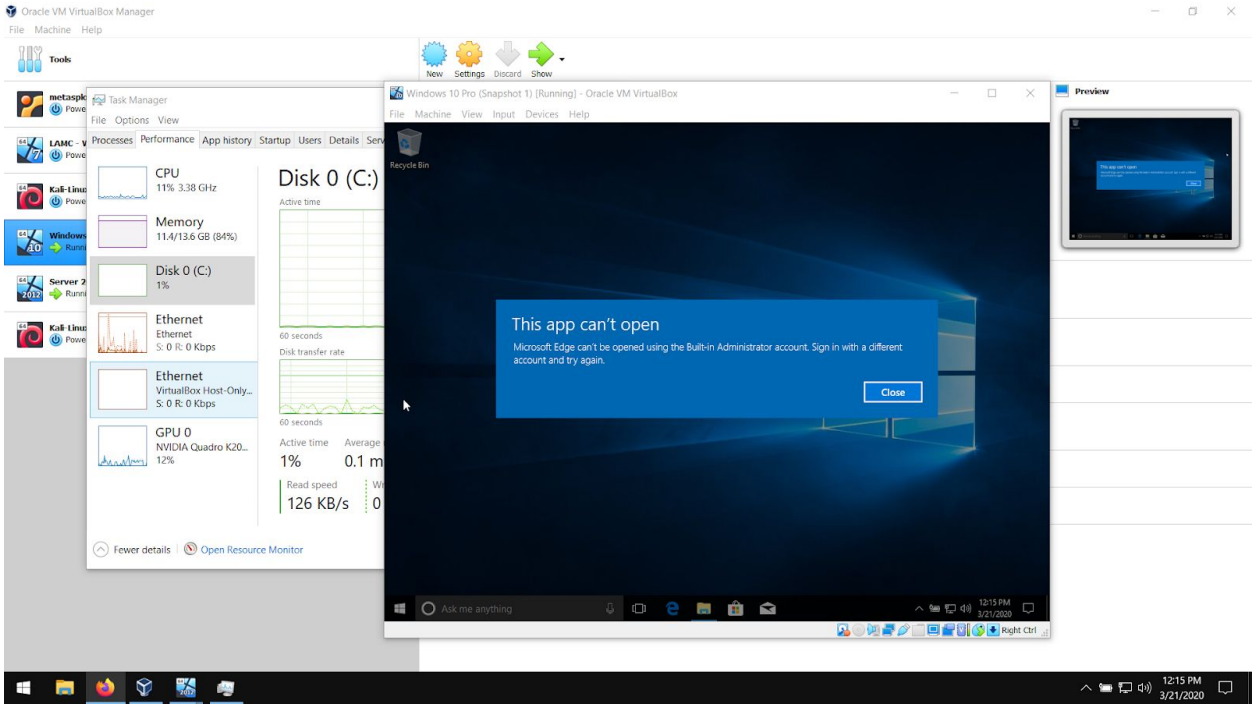
Initial boot into the new domain took less than one minute.

Command Line - ping



To verify network connectivity ping google.com was used.

Microsoft Edge - security policy



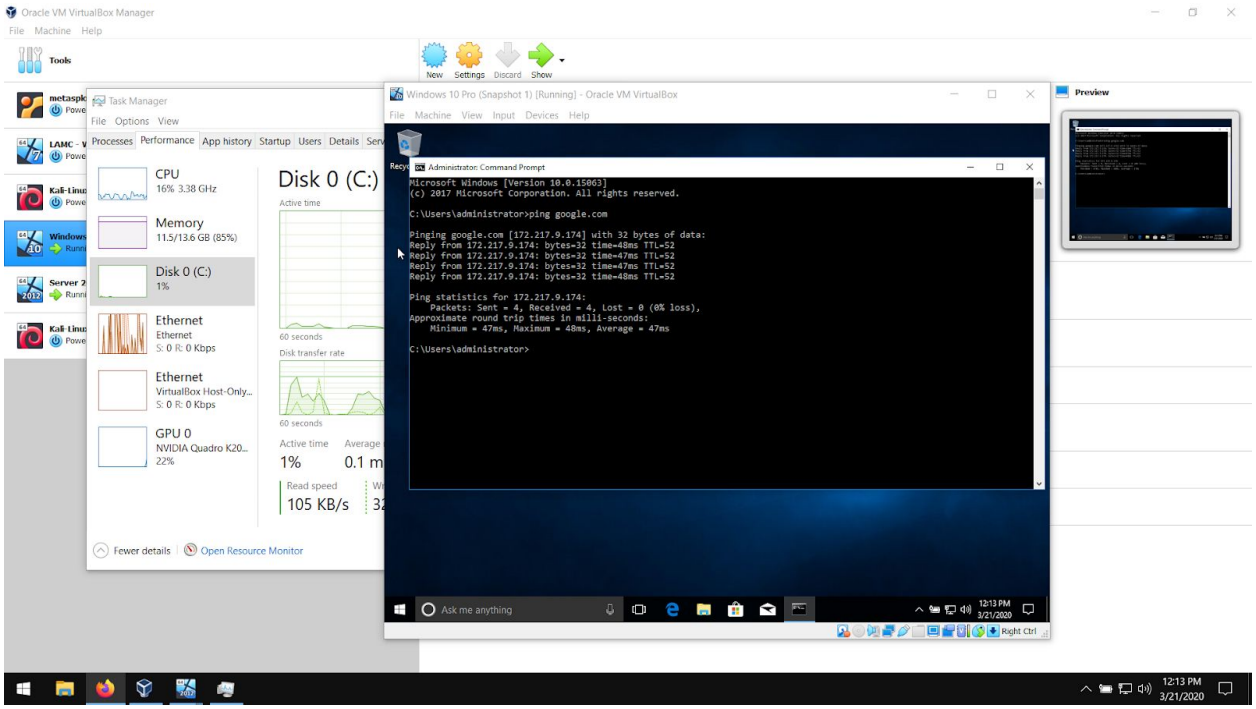
The domain's security policy does not allow Microsoft Edge use. Other applications fall under this policy.

3. Surprises. Things rarely go as planned. Include this in your report. If things aren't working, documenting the problem can help you to find the solution.

> Initially I had planned to set up the VirtualBox networks as a static network before booting any virtual machines. But doing so doesn't set up a gateway that's required since by default DHCP is not configured to run. To get around this there are few steps to take. First, having the virtual image boot in a DHCP environment will allow the configuration of the static IP settings in Windows network settings. After that, disabling DHCP within VirtualBox will ensure the IP correctly is assigned within the Windows image.

4. A screenshot of the final result of the assignment.

Windows 10 Pro - Target domain and PING



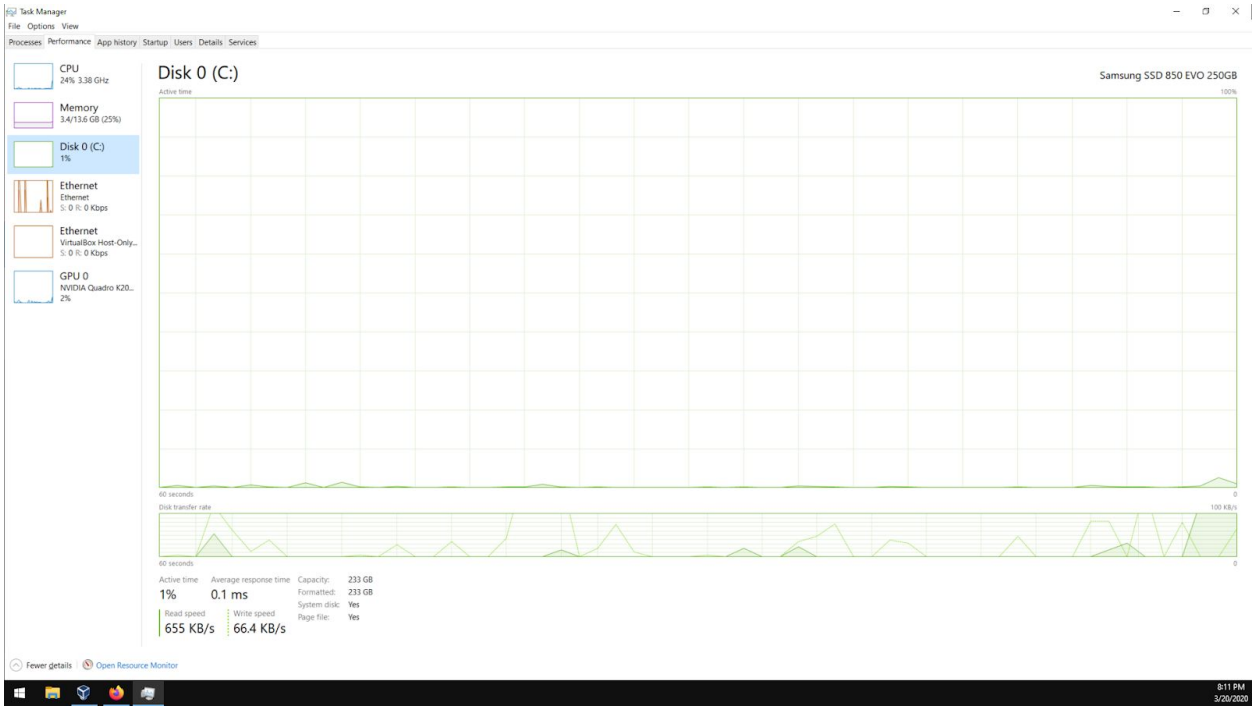
To verify the domain and connection is active, ping google.com was used on an administrator client.

5. Summary. Did it work as expected? Did you need more research?

> The Windows Target domain was successfully deployed and verified using a Windows 10 Pro administrator account. The procedure was long but produced expected results including the security policy disallowing some application execution. Being aware of the security policy will be crucial in knowing what is allowed on the client machine prior to logging into the domain. This could prevent confusion as to why some features or applications don't work. Furthermore, enabling multiple security role deployments in an organization will provide an expanded infrastructural defense in depth platform to be leveraged. More research on proven established security roles may help organizations adapt to meet customer needs and security responsibilities.

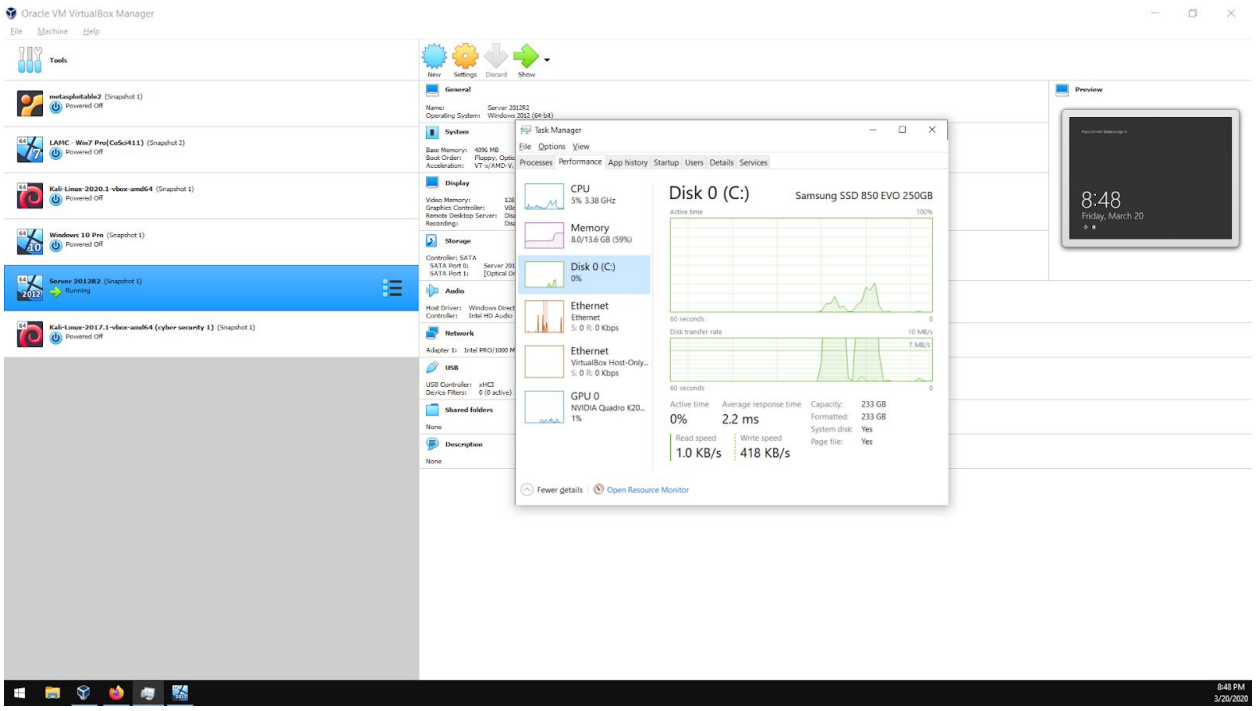
6. Disk Storms

Task Manager - Disk 0: SSD 250 GiB



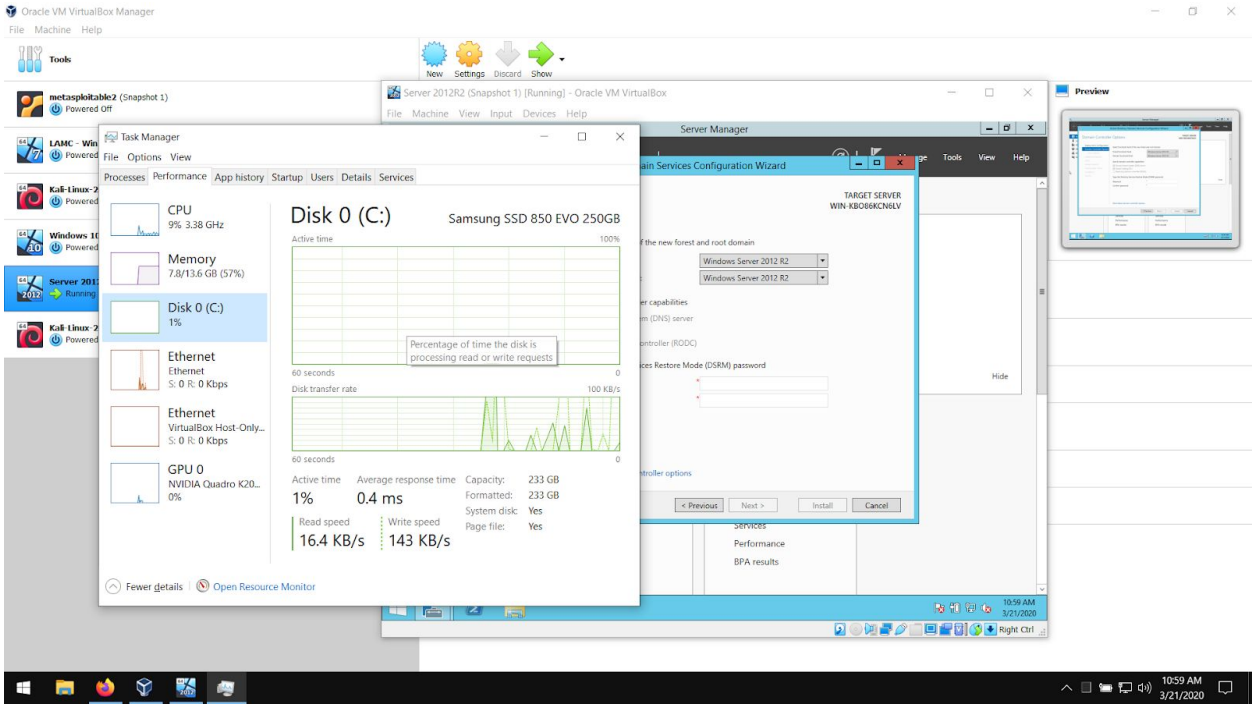
At rest before any virtual machine has started. The sharp rise is due to the screen snip tool.

Task Manager - Server 2012R2 Start up



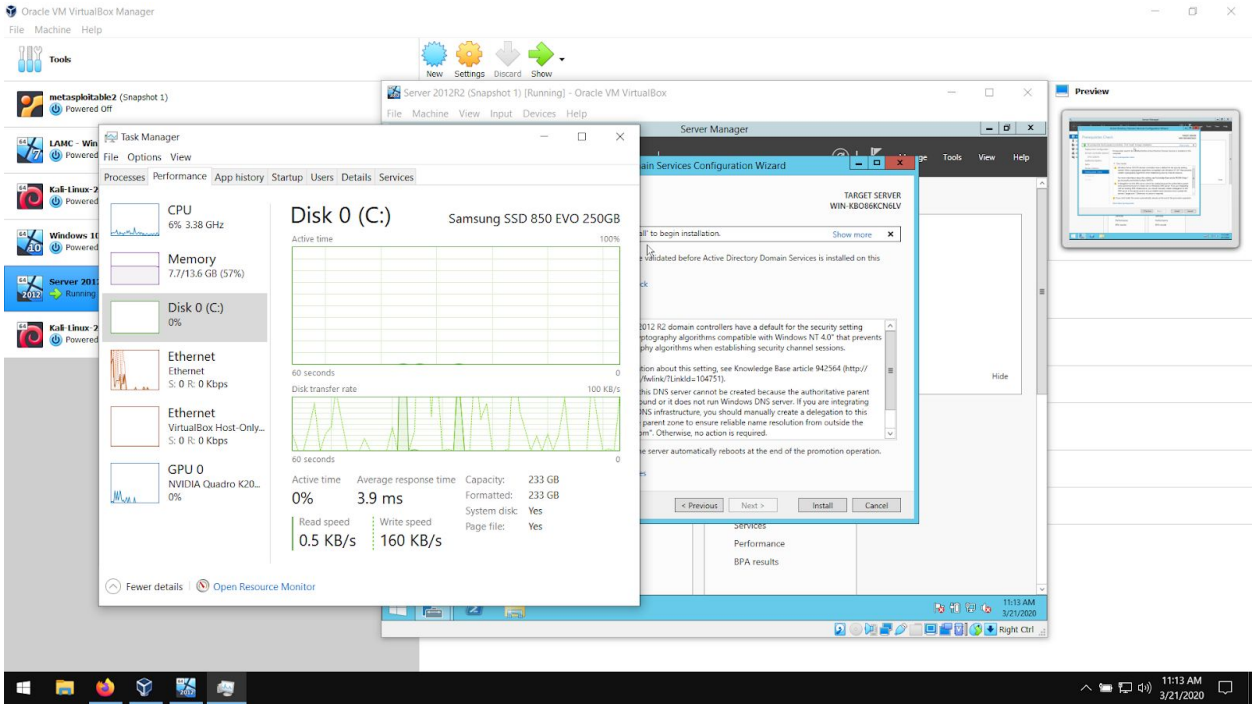
The Average response time range was between .02 ms and 2.2 ms

Deployment Configuration - Domain Controller Options



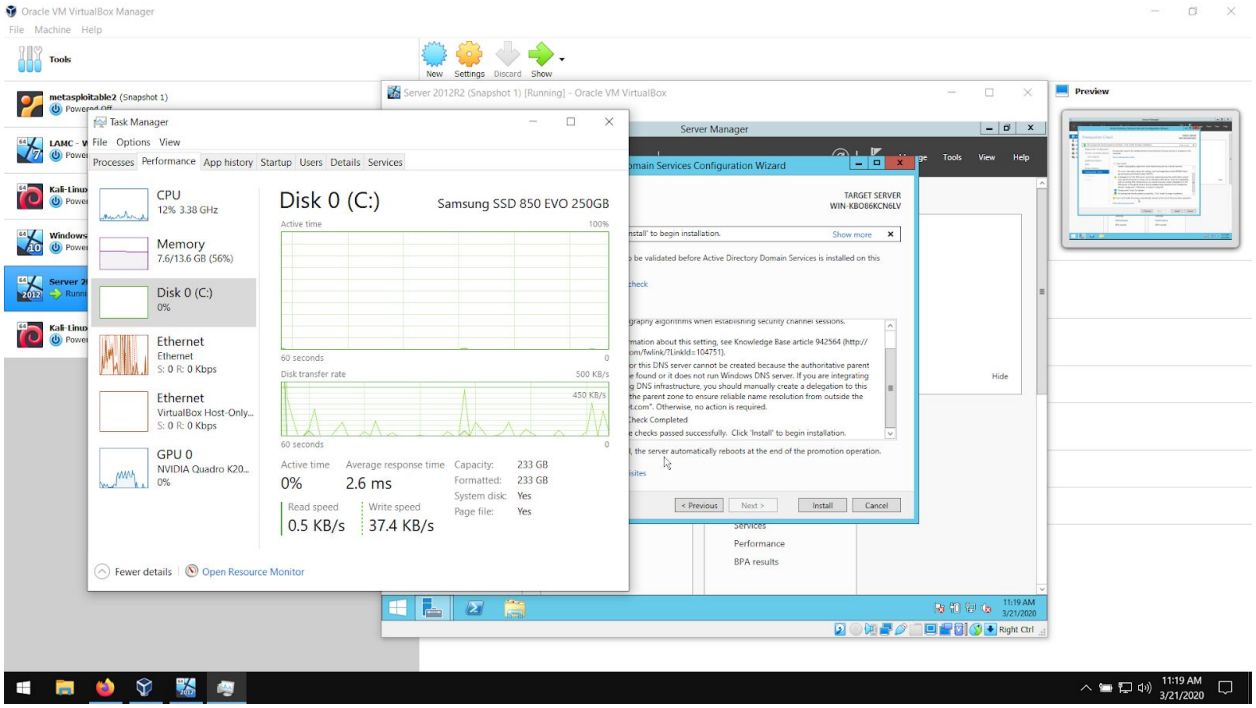
As noted in the video, at this step a processing surge may occur.

Active Directory Domain Services Configuration Wizard - Prerequisite Check



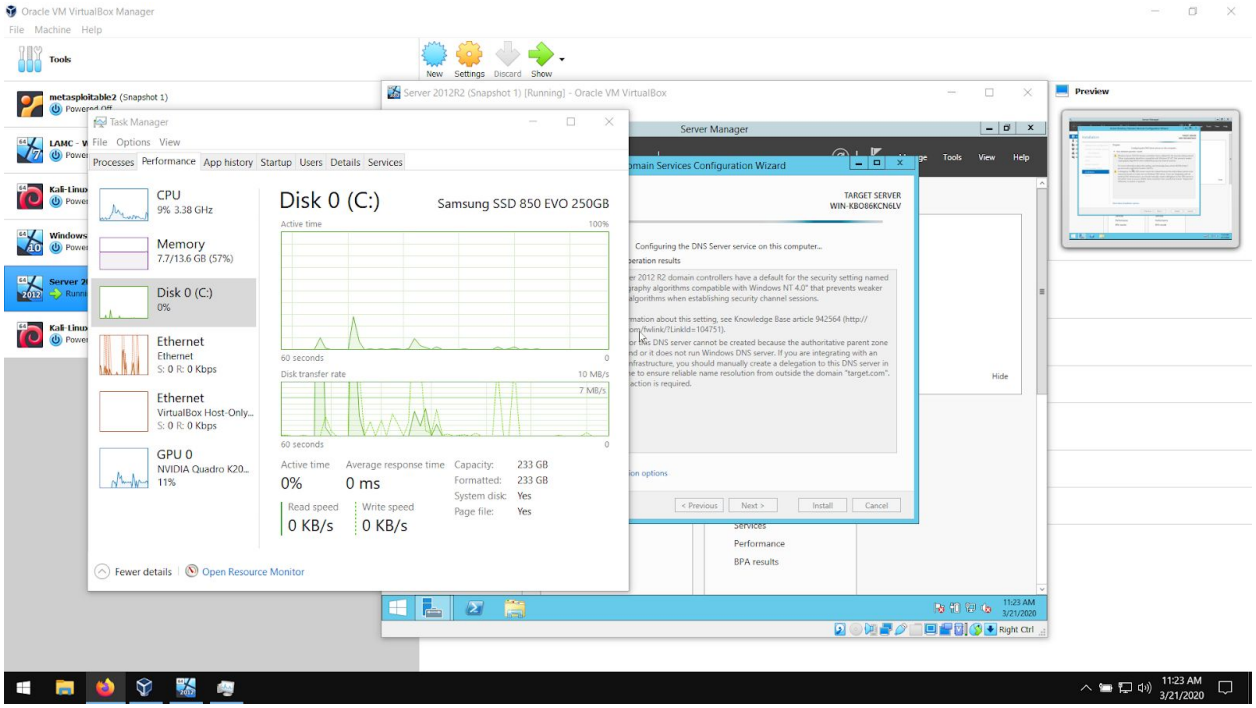
A noticeable disk storm occurred during the Prerequisite Check.

Active Directory Domain Services Configuration Wizard - Pre-Installation



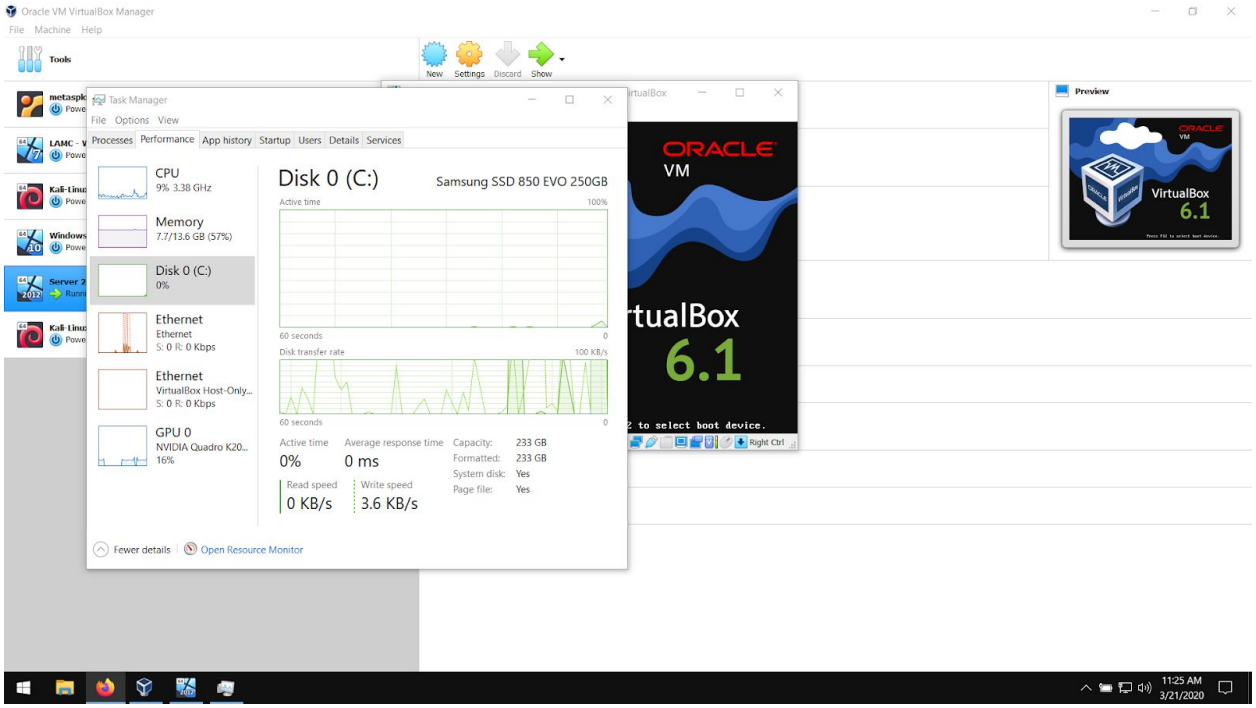
In anticipation of the disk storm for the deployment installation a screen snip was taken of host resources.

Active Directory Domain Services Configuration Wizard - Installation



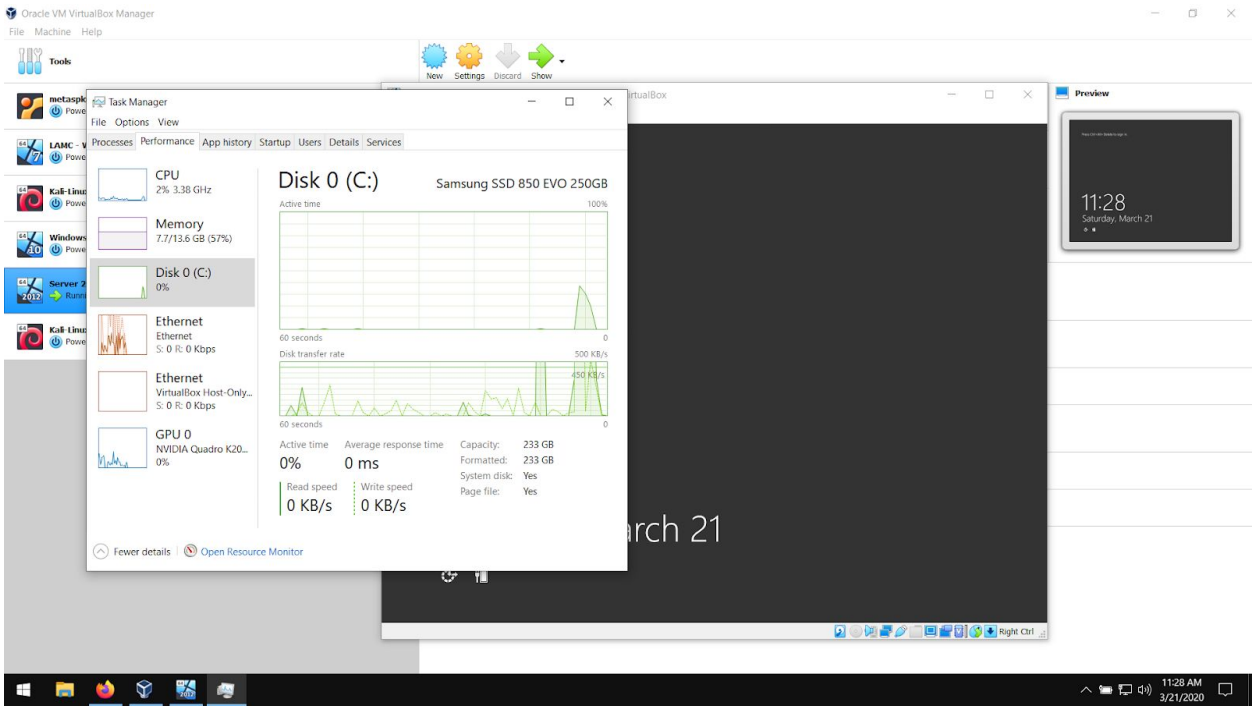
Average response time after one minute came to 12.4 ms

Active Directory Domain Services Configuration Wizard - Installation



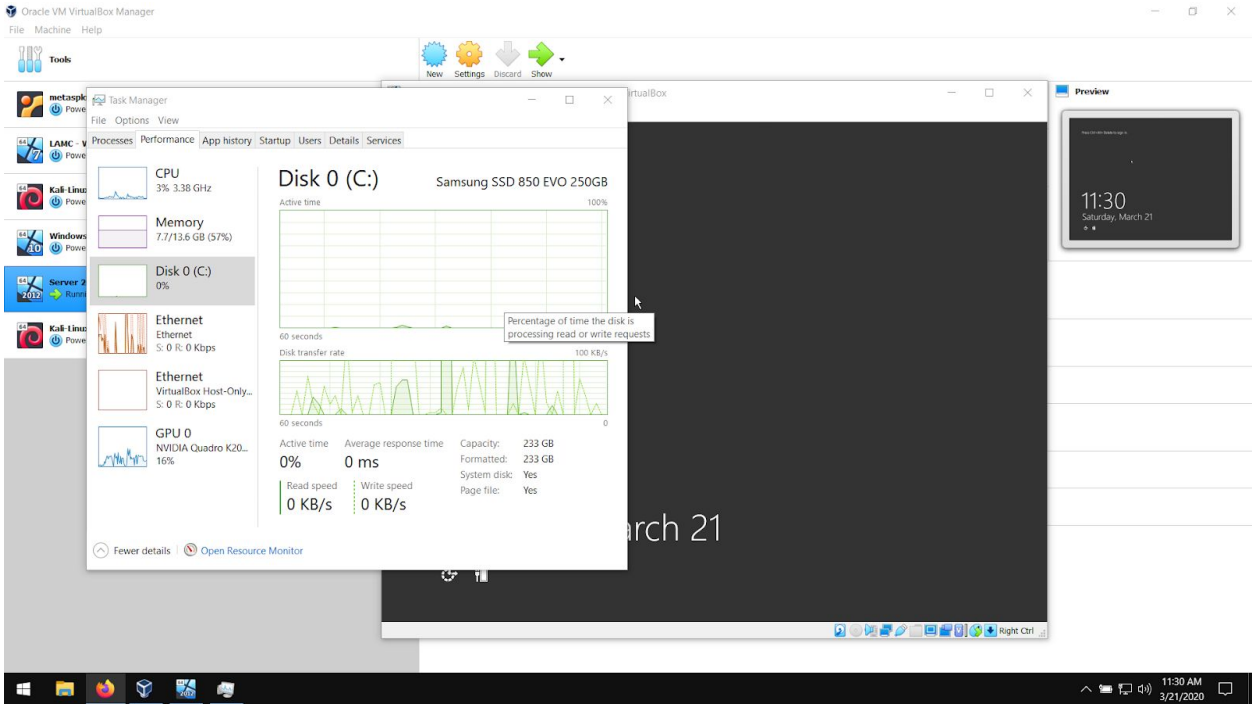
The installation has ended and the virtual box has been reset. This screen snip was taken before rebooting to visualize all disk storms before a reboot one took effect.

Active Directory Domain Services Configuration Wizard - Installation



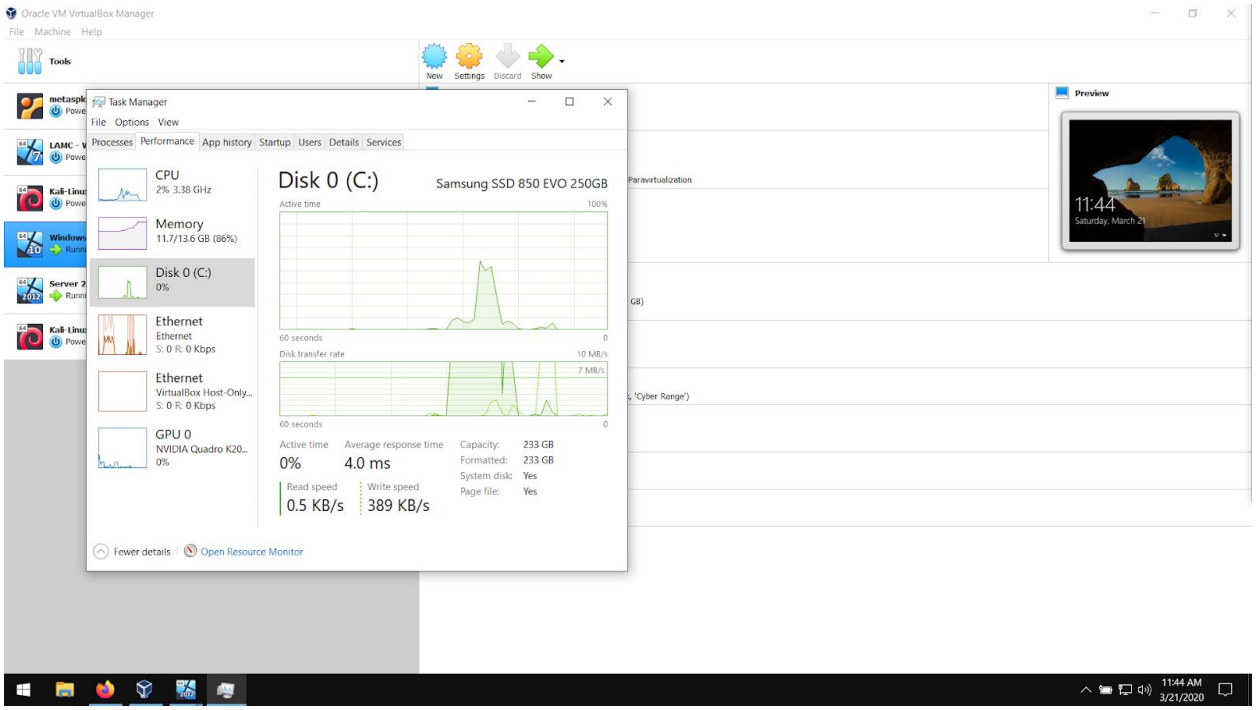
Much more disk usage, with a 12.4 ms peak during the reset.

Login screen Server 2012R2



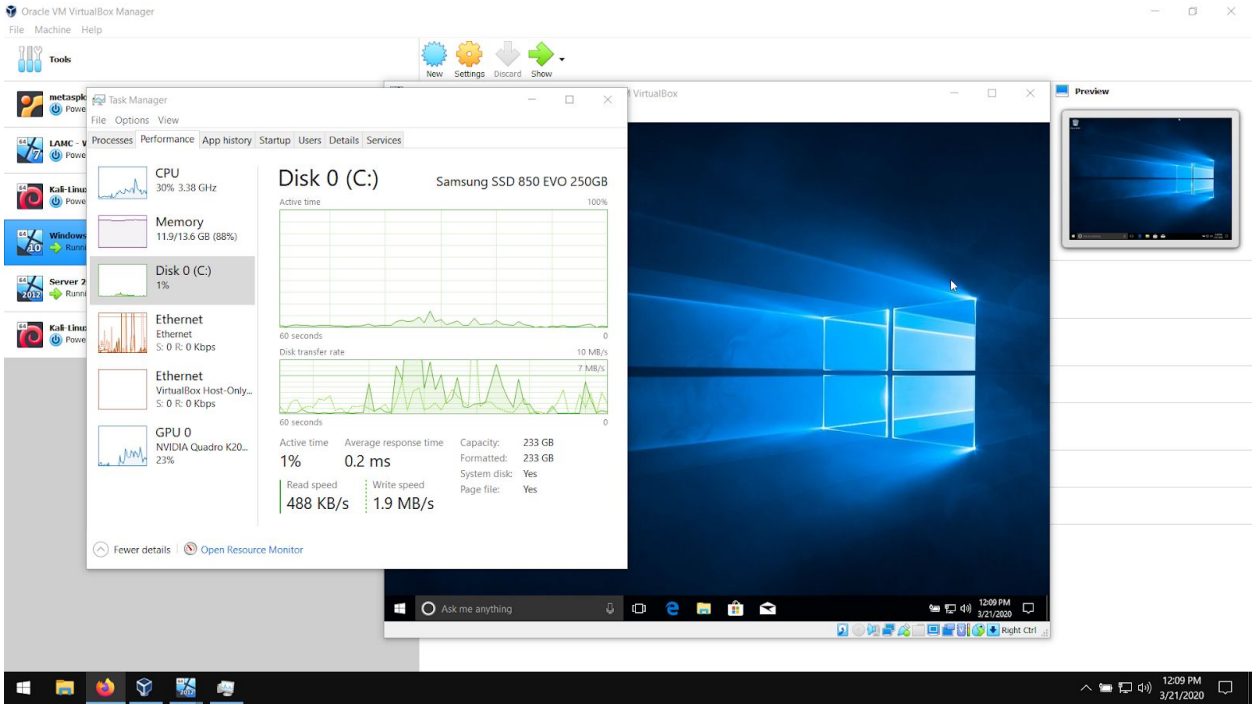
The disk storm continued well after installation and login screen. However, the Average response time was less than 5 ms.

Windows 10 Pro - boot



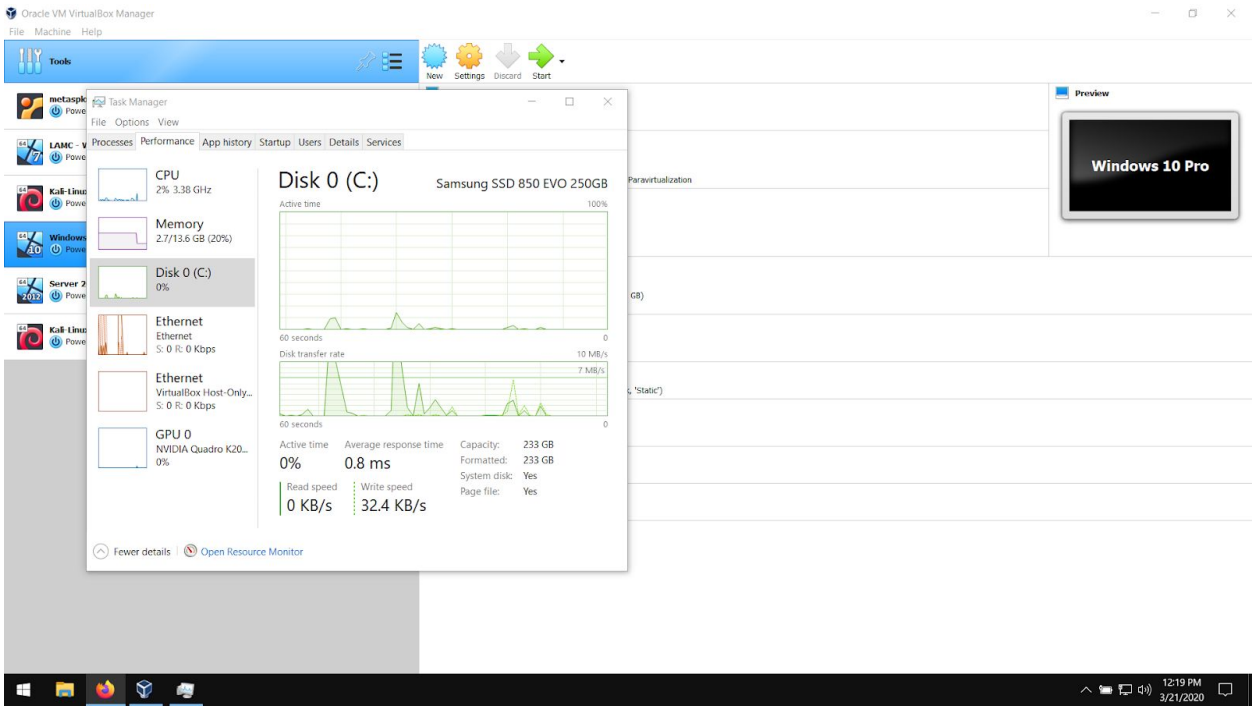
Windows 10 Pro boot screen snip shows a large disk storm with at one point a 20.4 ms average response time.

Windows 10 Pro - initial domain login



This is a screen snip upon entering the domain for the first time. The set up process took less than one minute.

Server 2012R2 - Shut down



Note the step in memory use after Server 2012R2 is shut down.