Creating a portable virtual server lab

Presentation for the Singapore PowerShell User Group  
8. April 2017

💻 First

Image from my last PowerShell presentation in 2008, and I haven’t done any presentation since then.

What do I mean by portable virtual lab?

I will mostly do demos and will use many custom commands, if I am too fast, please let me know.

Create VMs LAB2 and LAB5, to save time:

New-LabVM -id 2 -OS 2016GUI -NamePostFix CCC

💻 Agenda

quickly going through

💻 Technologies leveraged

 Who is using any of these technologies?

New-LabVM -id 5 -OS 2016GUI -NamePostFix DC1

💻 Motivation

Allows me to plug my USB drive into any capable computer and use my own secure environment.

Could be used to run a server lab at night or weekend on some big hardware servers without touching anything on the servers. (some Server hardware may require additional drivers for the OS to boot up)

Malware analysis, use throwaway OSes, but not VMs.

💻 Around the world

About seven years of travelling, mostly overland, came to Singapore twice from Europe over land.

The dots are not places I visited, they are places I stayed for at least one night.

💻 The host

show the USB drive, and the connector. SSD is much faster than any HDD or memory stick.

 Who knows what Windows to Go is?

 Anybody wants to try it out, plug this into your laptop?

** How many people are using Hyper-V (other virtualization technologies?)**

💻 Using Profiles

 Who is using profiles in PowerShell?

ex, um, dm, vm, ev, ser, n, ise, apps, fire, hosts, iis

Word, vs, sql, su, fm, excel, pdf, code

** What may these commands do?**

💻 Creating new Vms

Custom commands to manage my LAB.

show existing VMs:

Get-VM

vm

let’s create or main server first, I call it the CCC (command and control center), we want a GUI server for this:

New-LabVM -id 2 -OS 2016GUI -NamePostFix CCC

Review the output - My script is now creating a new VM based on an sys-prepped Windows Image and applies AND unattend file. This sets the Name, the IP address and some users.

 Who uses sysprep.exe or unattend.xml?

Connect to the VM via Hyper-V manager to see how it is doing.

"C:\Windows\system32\VmConnect.exe" "KNIGHT" "LAB4-2016GUI" -G "B9469941-2A5C-4868-A0D3-C831CCCF933F" -C "0"

we can connect to it:

LAB 2

 Why using RDP over Hyper-V Connection?

Much better clipboard, support \\tsclient, sound etc.

create another server for domain controller demo:

New-LabVM -id 5 -OS 2016GUI -NamePostFix DC1

let’s create a few more machines:

New-vLab -OS 2016Core -count 5

most of our servers don’t need a full GUI, so I am using Server Core.

 Who is using Windows Server core or Nano?

see what happened to our VMs?

Before we start changing things, it is a good idea to make a checkpoint.

 What is a checkpoint / or snapshot?

# CheckPoint-vLab.ps1

show commands but don’t execute them:

CheckPoint-vLab.ps1 -remove

to remove the last existing checkpoint or apply it / rollback / restore:

CheckPoint-vLab.ps1 -apply

go back to LAB 2

Run setup icon, because each user needs some settings after first login (this could be done via logon scripts in you are using a domain)

Connect to a core one:

LAB 3

run setup-user rather than click an icon.

LAB3 > setup-user

 Anybody knows why we are an elevated admin even though we didn’t get a UAC prompt?

Because on Server Core / Nano there is no UAC.

If we haven’t done it, run checkpoint:

CheckPoint-vLab.ps1

so, we now started four VMs, each VM has usually a pretty big hard drive footprint, several dozens of Gigabyte. Let’s look at this:

zoom

open R:\Vms in xplorer and press Ctrl+D, Ctrl+1

we can see Bob is 43+ GB but LAB\* are 2.5-4 GB,

 Anybody knows why these disks are so small?

Because of differential disks:

vmx -show parentdisks

Parent Disks: Create a VM manually, customize it and then sysprep it. Use the VHDX as a parent disk for all future VMs with the same OS.

💻 Using custom scripts

let’s run some custom scripts to setup roles

Start with a new Active Directory with a domain controller on LAB5:

go to LAB 5 and click setup icon.

su

to elevate and:

Setup-AD -prepare -forest

go to LAB 2, we need IIS later

Setup-IIS.ps1 -role

# [z:\dsc.cmd](file:///z:/dsc.cmd)

# setup-vlab.ps1 -cert

dsc.ps1 -PullServer

still on LAB2

sm

to open server manager,

 in Server Manager, connect to a LAB3 PowerShell session,

For better font:

Cz

Enter-PsSession LAB3

Setup-DemoWebServer.ps1 -iis -sites 5

We see a LAB server group; how did this get here?

The setup scripts copied the file

C:\Users\adm\_lab\AppData\Roaming\Microsoft\Windows\ServerManager\ServerList.xml

which has a list of servers.

go to LAB2

iis

to start IIS Manager, connect to LAB3.hahndorf.eu as adm\_lab, show the new sites created.

In Server Manager connect to LAB4 via PowerShell remoting, or Computer Management.

Open a browser to navigate to http://lab3.hahndorf.eu:8003

 Check for LAB5, it may have rebooted, when it is back up, connect to it:

LAB 5

and run the second phase of the AD setup, login as hacon\administrator, setup icon.

Setup-AD.ps1 -setup -gpo

to create an OU, groups and users and to import some prepared Group Policy objects,

Next open Active Directory tools:

adum

and show haconOrg – Management - Users

gpmc

to show Domains - hacon.local – haconOrg, there is our GPO.

We could now run scripts to have our LAB machine, join the new domain.

We are having a virtual LAB up and running, how long did this take?

Talk about Mysore and why it may not be worth it to use scripts for small scale installations.

💻 Desired State Configuration

Anybody using DSC? What for?

Explain high level what it is.

💻 DSC Resources

You are using resources in your configuration, examples are:

Show some resources

Get-DscResource | Select Name,Modulename

Microsoft is trying to get anything configurable in Windows into the resource kit.

💻 Using DSC locally

<https://msdn.microsoft.com/en-us/powershell/dsc/overview>

https://msdn.microsoft.com/en-us/powershell/dsc/quickstart

Get-WinEvent -LogName "Microsoft-Windows-Dsc/Operational"

Copy a prepared configuration:

Copy-Item $env:bindir\scripts\setup\labwebserver.ps1 -Destination $env:newsdir\LabWebServer.ps1

Prepare a file:

"<head></head><body><p>Hello World!</p></body>" | Out-File $env:newsdir\test.html

Look at the file:

ise $env:newsdir\LabWebServer.ps1

compile it:

news

. .\LabWebServer.ps1

LabWebServer -NodeName localhost

Lets look at the compiled file using xPlorer2, also show c:\inetpub

Execute it:

Start-DscConfiguration .\LabWebServer -force -wait -verbose

Check for directory and files and

Change 2ndSiteRootFolder to Absent, we have to compile and run it again, I automated this:

dsc -source LabWebServer -run

if an error, try manual.

Take file and run it remotely

dsc -source LabWebServer -node LAB3 -build

now we have to copy the file over to another server:

Start-DscConfiguration -wait -Path .\LabWebServer -Force -verbose -computername LAB3

We get an error, on LAB3:

"<head></head><body><p>Hello World!</p></body>" | Out-File $env:newsdir\test.html

Try again:

ls c:\inetpub\wwwroot

💻 Using a DSC Pull Server

But that’s a bit of a pain, so let’s use PULL instead:

For pull, we set up a central repository and our servers pull the configuration information from that repository. If some configuration changes, all servers will pull the new configuration and make changes to the server’s settings automatically.

<https://msdn.microsoft.com/en-us/powershell/dsc/pullserver>

https://msdn.microsoft.com/en-us/powershell/dsc/pullclientconfignames

prepare the pull server

# setup-iis.ps1 -role

if cert is required:

# setup-vlab.ps1 -cert

show the new cert:

certs

make sure we have required components:

installing nuget and xPSDesiredStateConfiguration, or run:

# [z:\dsc.cmd](file:///z:/dsc.cmd)

then setup the pull-server which consists of a few steps, which I combined:

dsc -EnableLogs

dsc -pullserver

open: <https://lab2.hahndorf.eu:8080/PSDSCPullServer.svc> in Firefox (ff)

Now we should tell the other server to use the pull server, on LAB3

Get-DscLocalConfigurationManager

We can see it is in PUSH mode

Again there are a few steps involved change the mode, we use a DSC and my own script again to make it easy, on the Pull Server:

dsc -PullClient LAB3

Get-DscLocalConfigurationManager

dsc -PullClient LAB2

Now LAB3 is configured to pull configuration changes from LAB2.

We should be able to see this in the IIS logs:

n (ls C:\inetpub\logs\LogFiles\W3SVC2 | sort LastWriteTime | Select -Last 1).FullName

**Providing configurations on the pull server:**

Tests MOFs locally, then put them into “C:\Program Files\WindowsPowerShell\DscService\Configuration”

Create a new file:

$f="C:\news\LabDSCClients.ps1"; New-Item $f; n $f

**Configuration LabDSCClients {**

**param**

**(**

**[string[]]$NodeName = 'localhost'**

**)**

**Import-DscResource -ModuleName PsDesiredStateConfiguration**

**Node Localhost {**

**File TestFolder**

**{**

**Ensure = "Present"**

**Type = "Directory"**

**DestinationPath = "C:\News\Test1"**

**}**

**File NoSetup1**

**{**

**Ensure = "Absent"**

**DestinationPath = "C:\News\setupcmd.log"**

**}**

**}**

**}**

Dsc -source LabDSCClients -build

Copy it to the correct locations with the correct name.

copy .\LabDSCClients\Localhost.mof -Destination "$env:ProgramFiles\WindowsPowerShell\DscService\Configuration\LabDSCClients.mof" -verbose

let’s look at the file:

& $xplorerSquare 'C:\Program Files\WindowsPowerShell\DscService\Configuration\'

Before they can be distributed, we need to create checksum files for each MOF file:

Dsc -checksum

Now force an update, otherwise it may take some time.

Update-DscConfiguration -wait

Update our config, use a user requested number.

**Registry RegExample**

**{**

**Ensure = "Present"**

**Key = "HKLM:\SOFTWARE\Usergroups\Singapore"**

**ValueName = "IsCool"**

**ValueData = "1"**

**ValueType = "Dword"**

**}**

We can use my -publish command as well

Dsc -source LabDSCClients -publish

Make sure it runs:

Update-DscConfiguration -wait -computername LAB3

Check on LAB3:

Get-ItemProperty -Path "HKLM:\Software\Usergroups\Singapore\"

You can also configure a report server to see exactly what configurations are applied when and where. But I have not done that.

In theory, any configuration changes should now be applied to the pull clients.

**Troubleshooting tools:**

Pull now:

Update-DscConfiguration -wait -computername LAB3

Check for the configuration being applied:

Get-DscConfigurationStatus | fl Status,Mode,Error

Check the event logs:

eventvwr /c:"Microsoft-Windows-Dsc/Operational"

use resource kit module:

Get-xDscOperation

Trace-xDscOperation -SequenceID 93

💻 Alternatives to DSC

I haven’t used any of these, except my own scripts, Chef and Puppet come from the Linux side.

💻 Authoring DSC Resources

I have created some resources, namely IIS resources that are now part of the official DSC resource kit. It’s a whole different topic.

R:\Softlib\current\tools\bin-iso\DSCResourceKit\xWebAdministration\1.17.0.0\DSCResources\MSFT\_xIisMimeTypeMapping

💻 Things DSC can't do!

Explain why this is a problem.

You can request certain things not to be there, but you have to name them. You can not say, never have more than 4 web sites.

💻 Questions?

Any questions?

Extras

**Nano Server:**

prepare disk (takes a while)

New-NanoServer.ps1 -Id 2, or copy from parentdisks

New-LabVM.ps1 -Id 3 -os 2016Nano

**Update Bin-Iso**

Create-BinIso.ps1 -ejectAllDisks

Create-BinIso.ps1

vmx -name lab1,lab2,lab3 -DVD bin

on servers: [z:\update.cmd](file:///z:/update.cmd)

**remote editing**

open ise

connect to box: enter-pssession -computername LAB5

cd \bin\scripts

psedit .\los.ps1

**New Parent Disk:**

* Install new OS or make a copy of an existing ParentDisk.
* Create a new VM, or use SysPrepper.
* Install roles you want to be present on the parent disk
* Update bin directory, maybe clean it.

C:\Windows\System32\Sysprep\sysprep.exe /generalize /shutdown /oobe

* Remove the VM or vhdx, move the vhdx to the parentdisk directory, give it a name with GUI|Core and the OS version.