ScriptDotS

We are all in a void. A pointer to something that doesn't exist…

You are here: Home › Active Directory Pentesting › Active Directory Penetration Dojo – Setup of AD Penetration Lab : Part 1

ACTIVE DIRECTORY PENTESTING BLOGS WINDOWS PENTESTING

Winsaaf Man

June 9, 2018 · 5 Comments

Active Directory Penetration Dojo - Setup of AD Penetration Lab : Part 1

The Prologue

Hello everyone, Welcome to the series of Active Directory Penetration Dojo. This series is for people who've used Windows but haven't worked on Active Directory. This blog will be focusing primarily on understanding AD environment so that we can perform AD enumeration and simulate AD attacks as one would do when doing a Red Team Assessment.

Hacker's Paradise, Administrator's Hell

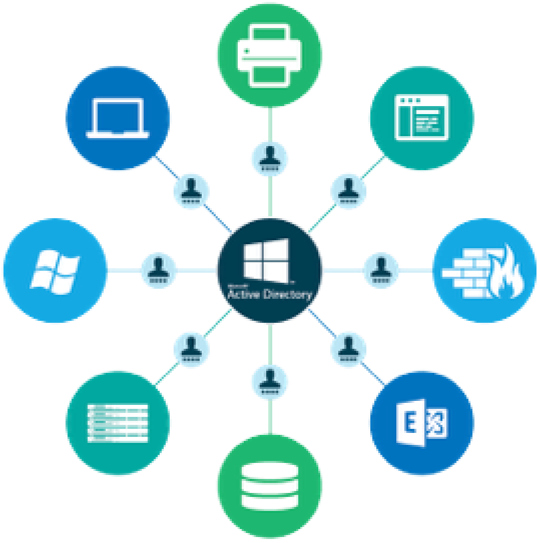
Before joining InfoSec domain, I used to work as a Windows L3 administrator. My job was to manage AD resources, servers and deal with group policies etc. When I came into the Information Security domain a few months back, I started seeing the AD from the view of Red team members who perform different AD attacks and bypass these policies. That motivated me to research more on using the AD resources in an offensive manner.

From this blog series, you will get to know AD from two different point of views i.e. as an Administrator who tries to add security policies to harden the environment and an attacker who tries to bypass that and uses the same policies to manipulate the environment. There are many things that lead to the compromise of AD, like misconfigured settings, poor maintenance procedures, and many other mistakes made by administrators which I learned over time.

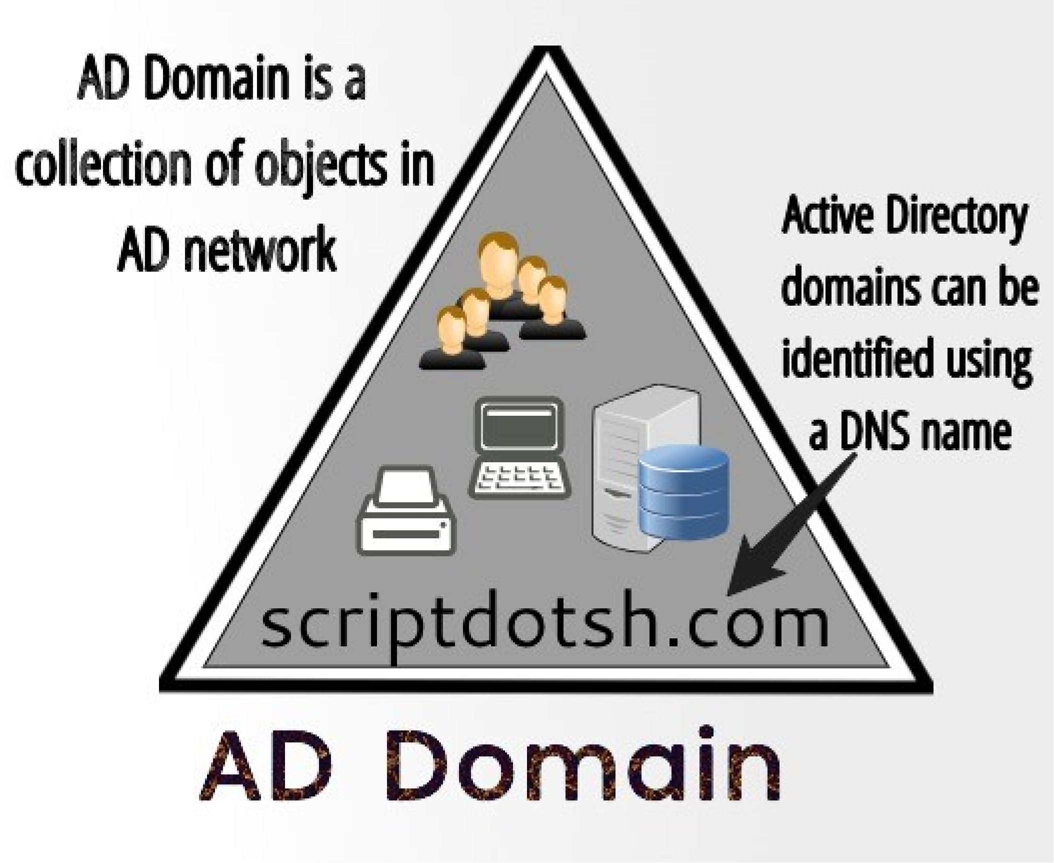
This blog series may be little lengthy covering the ADDC setup and attacks, reason being to understand the concepts of Active Directory, we must first understand the basics. It's gonna be more interesting after understanding how the things work and when we setup a Virtual lab to test out the different attacks.

Hello Windows!

Active Directory is Microsoft's Directory service which acts as a centralized repository that holds all the data related to users, computers, servers, resources etc. of an organization and it makes administration & management very easy for System administrators. Using AD, workstations can be updated, configured and maintained remotely. It is a single management interface that is accessible from anywhere on the network.

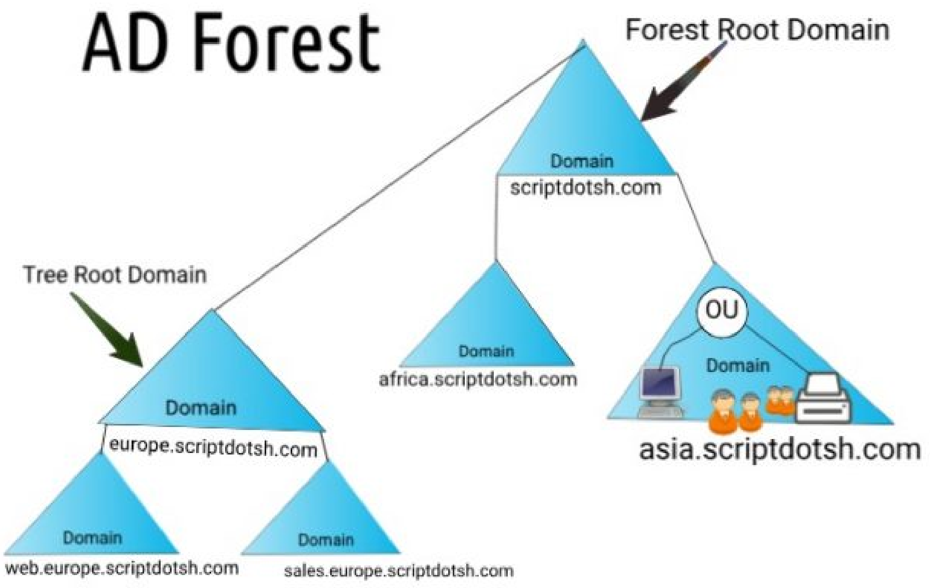


And this collection of all objects falls under a **domain**. Domains represent logical partitions within Active Directory for security and directory replication. A domain is always referred to by its unique name and has a proper domain name structure. (like-scriptdotsh.com)

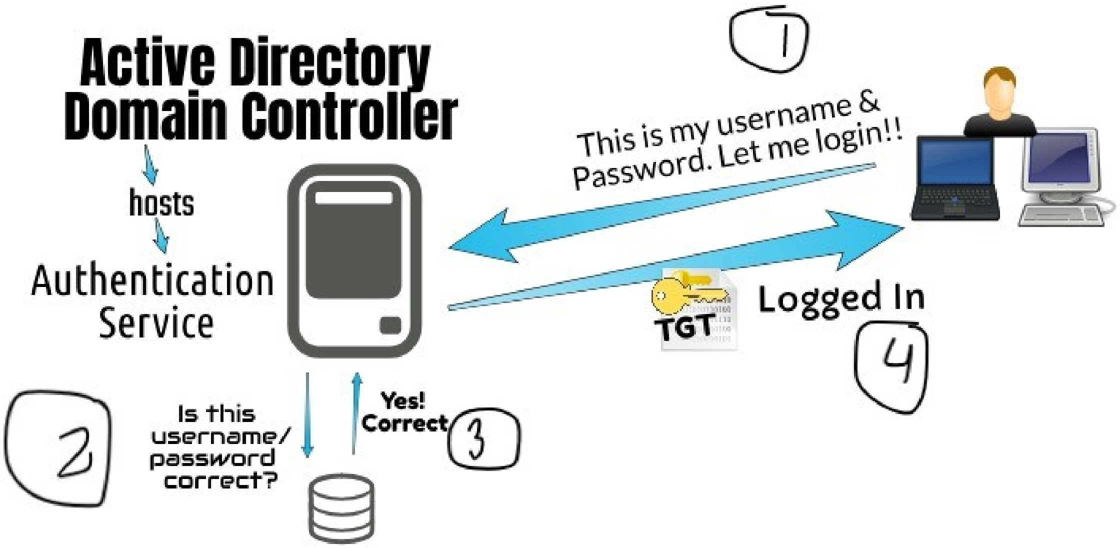

AD Domain is a collection of objects in AD network
Active Directory domains can be identified using a DNS name
scriptdotsh.com
AD Domain

A group of AD domains that share a contiguous namespace is called **AD Tree**. Objects in tree always follow hierarchy. (Example: If in AD Forest scriptdotsh.com, computer1 is in its child domain **europe**, its FQDN would be: ***computer1.europe.scriptdotsh.com***

And a collection of domain trees is called a **Forest**. A domain is always a part of forest even if there is just a single domain. A forest is composed of one or more trees. Unlike a tree, a forest can contain several non-contiguous namespaces.



Active Directory Domain Controller

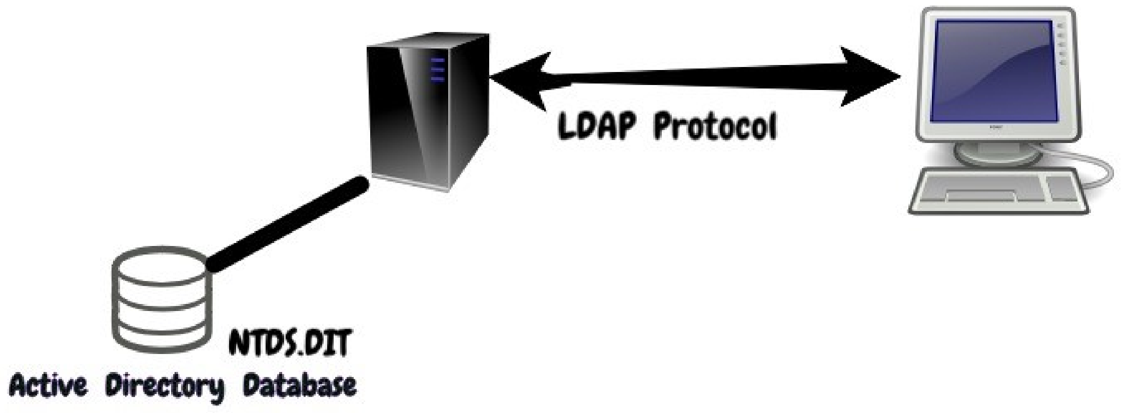

Active Directory Domain Controller
hosts
Authentication Service
1
This is my username & Password. Let me login!!
2
Is this username/ password correct?
Yes! Correct
3
TGT
Logged In
4

AD Domain Controllers host the service that authenticates user and computer accounts when they log on to the domain, so all users and computers must connect to AD DS domain controllers when signing into the network, that's why AD DS is the primary means by which you can configure/manage user and computer accounts on your network. In corporate environment with big infra and lot of users, Microsoft Active Directory is quite famous.

Note: AD DS stands for "Active Directory Domain Services"

AD Database

The information on user identity, computers, groups, services and resources etc. is stored in Active Directory database which is made up of a single file named **ntds.dit**. By default, it is stored in the %SYSTEMROOT%\NTDS folder.



LDAP

LDAP stands for Lightweight Directory Access Protocol. This service is responsible for keeping track of what is on the network.

AD integrated DNS

DNS is important for Active Directory to work. There are several DNS records that AD requires to determine what services are available on the domain and who provides what. These records are managed automatically when you configure DNS in AD.

Kerberos

Kerberos is the services that allows you to use one username and password to log into multiple computers throughout the domain. It basically handles Single Sign On throughout the domain.

Group Policies

Group Policy is used to define user, security and networking policies at the machine level. Administrators can apply group policies from a centralized location to the whole domain or few computers/users. There are still many security professionals who aren't very familiar with AD and many concepts of AD. So, I decided to discuss a few concepts of AD before explaining the setup part. Let's get started with setup.

Active Directory Domain Controller Lab Setup

For this lab setup, I will setup a small environment because of limited resources but this environment is enough to simulate AD Attacks:

- **Domain controller** (Windows Server 2012 R2)

In production environment, there are multiple domain controllers like ADC (Additional Domain Controller), RODC (Read-Only Domain controller), CDC (Child Domain Controller).

- **Client machine** (windows 7, windows 10)
- **Member Servers** like SQL server, File Server, FTP Server, IIS Server, Proxy Server, Antivirus Server etc.

There are two ways to set up the lab:

- Graphical User Interface way
- Command Line Interface way

The Administrator's Way

Let' get started with the first one. Download Oracle VirtualBox from here. Download the Server 2012 R2 ISO file which is evaluation version for 180 days which is good for testing from here.

Note– Always download the evaluation copy of server OS ISO files from Microsoft's website.

Creating a VM for Domain Controller

Hardware Requirements:

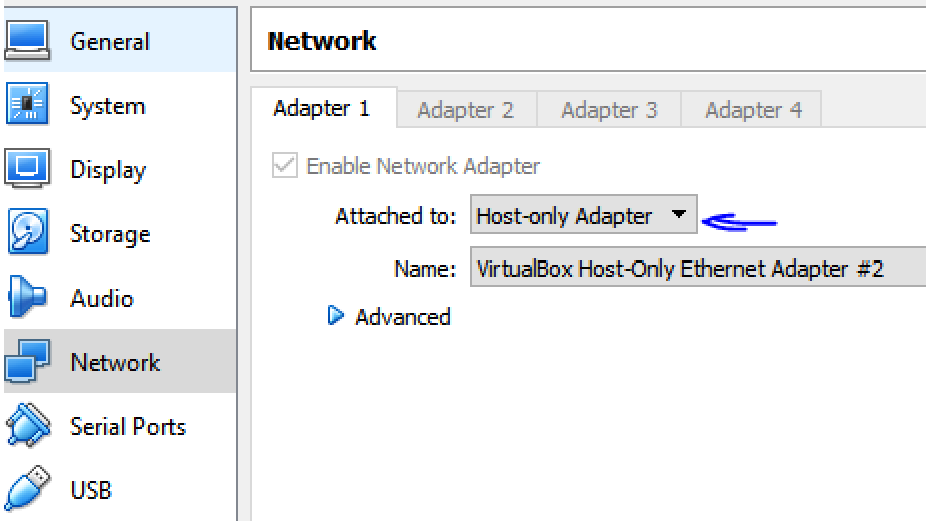
I will create the DC with the below configuration:

- 1 vCPU
- 2GB RAM
- 25-30gb storage

In VirtualBox, Select New Virtual Machine, enter the required details and click on Create. Remember, that your machines will be a part of host-only virtual network and will be segregated from the real environment but will be able to communicate with each other. To set this up, follow the steps:

- Right click your newly created VM and select "Settings"
- Go to Network and select "Host-Only network".

I'm setting internal network so that only DC and Proxy server gets access to internet. Other clients will access internet via proxy server so we could gather logs as well.



☑ Enable Network Adapter

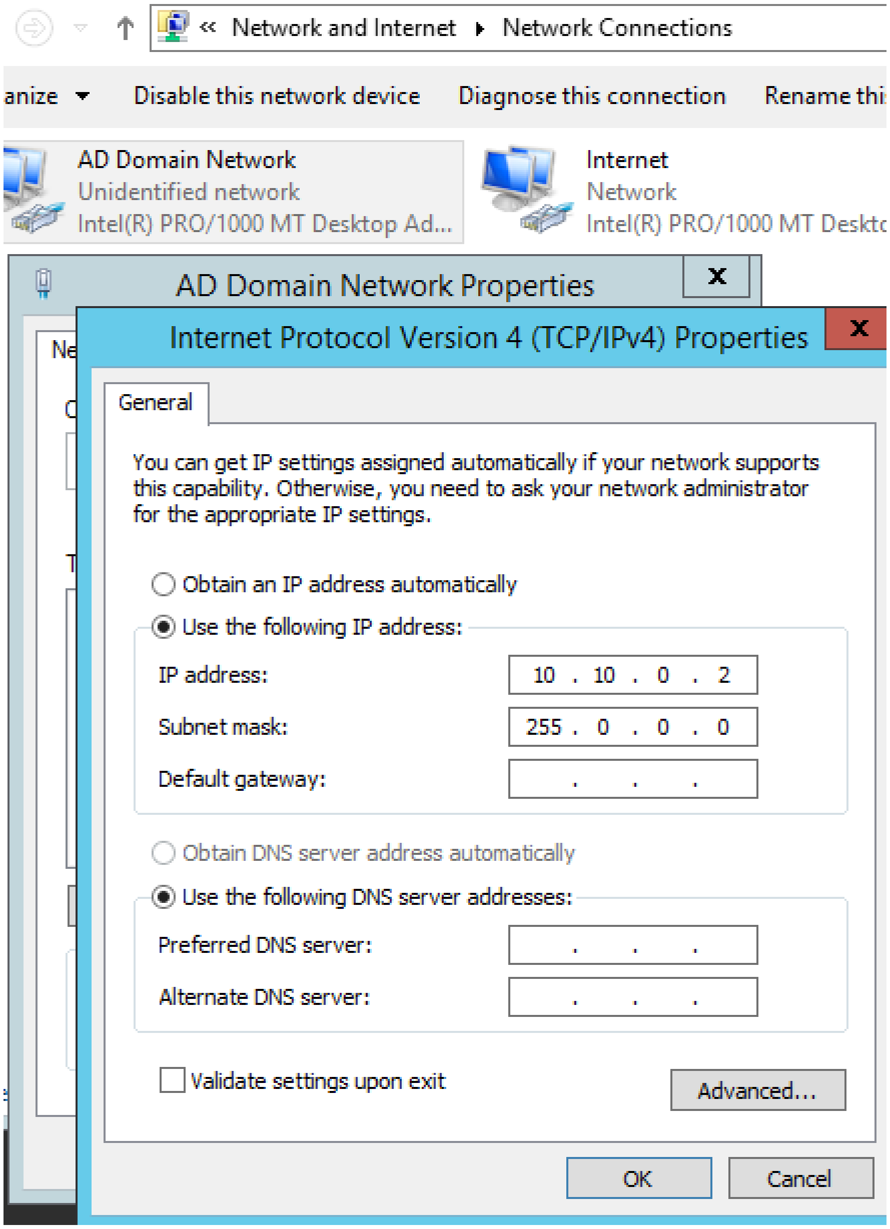
Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #2

I will also set up another NAT adapter later for internet access. For now, let's configure only one adapter (Host-Only). Click to run it and browse the ISO file. It'll boot and come up with normal steps to install windows. Click "Install now" and select partition and begin installation. Once installation finishes, power on the machine and assign a static IP address to it. That will be the address of your AD domain controller and DNS.

- **Assign an IP address:**

Go to network properties to assign IP to the machine. Type **ncpa.cpl** in RUN to open network and sharing center. Assign a static IP address to the machine.


« Network and Internet ▸ Network Connections
anize ▾
Disable this network device
Diagnose this connection
Rename thi
AD Domain Network
Unidentified network
Intel(R) PRO/1000 MT Desktop Ad...
Internet
Network
Intel(R) PRO/1000 MT Desktc
AD Domain Network Properties
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Advanced...
OK
Cancel

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 10 . 0 . 2
Subnet mask: 255 . 0 . 0 . 0
Default gateway: . . .

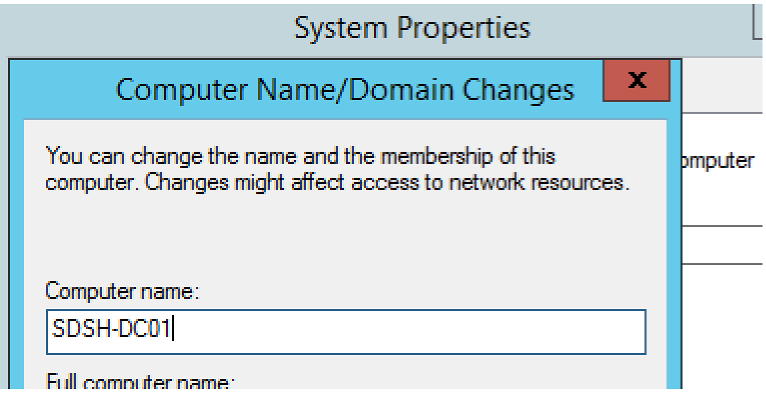
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

- **Change the computer name:**

A meaningful name is required so that administrators can remember which server is DC, File Server, DHCP server etc. Go to system properties and change the computer name. Type **sysdm.cpl** in RUN to open system properties and change computer name.



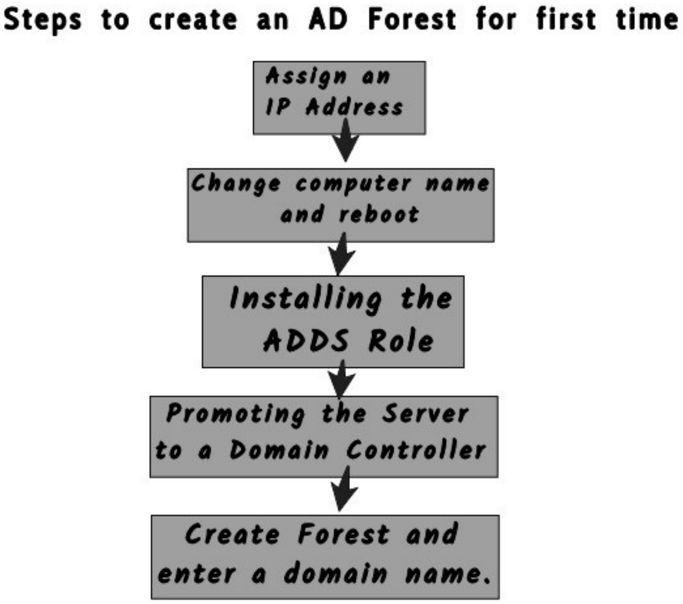
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
SDSH-DC01

Full computer name:

Reboot machine to apply changes.

- **Installing the ADDS Role:**



Steps to create an AD Forest for first time

Assign an IP Address

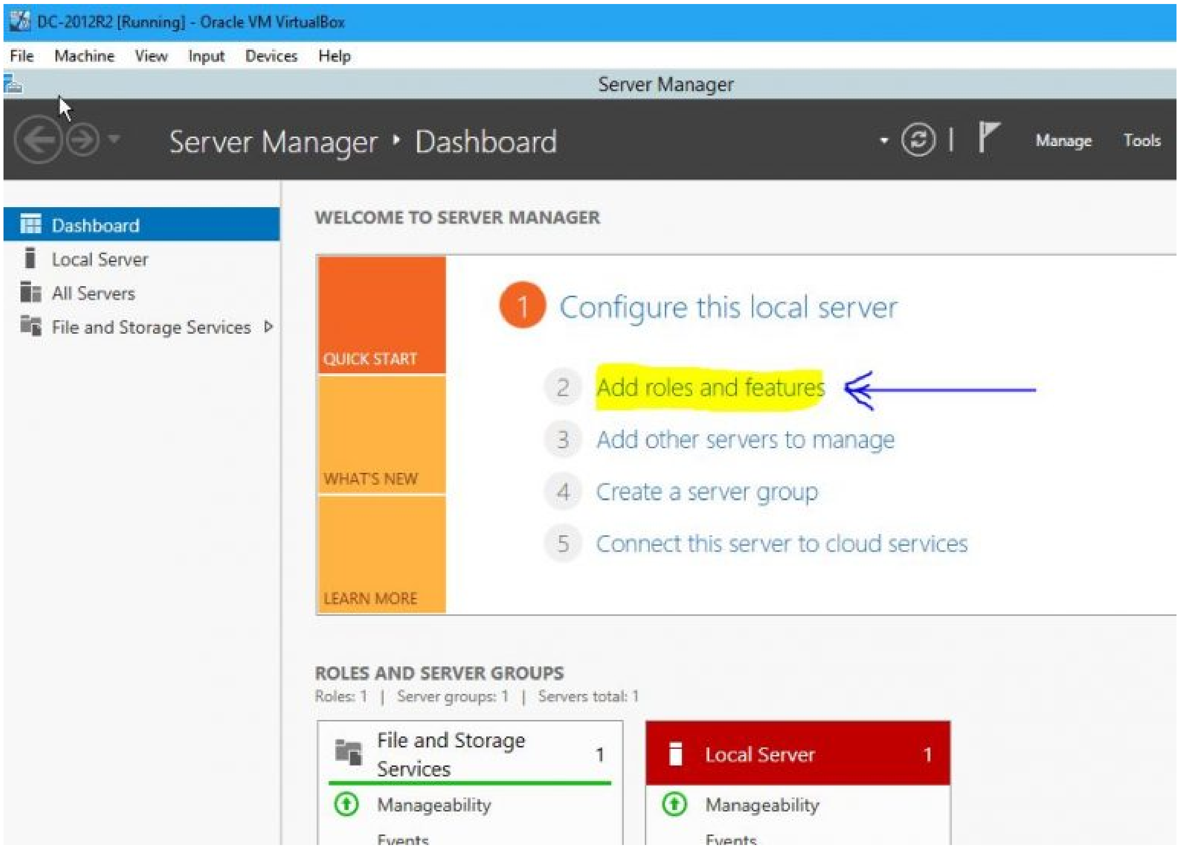
Change computer name and reboot

Installing the ADDS Role

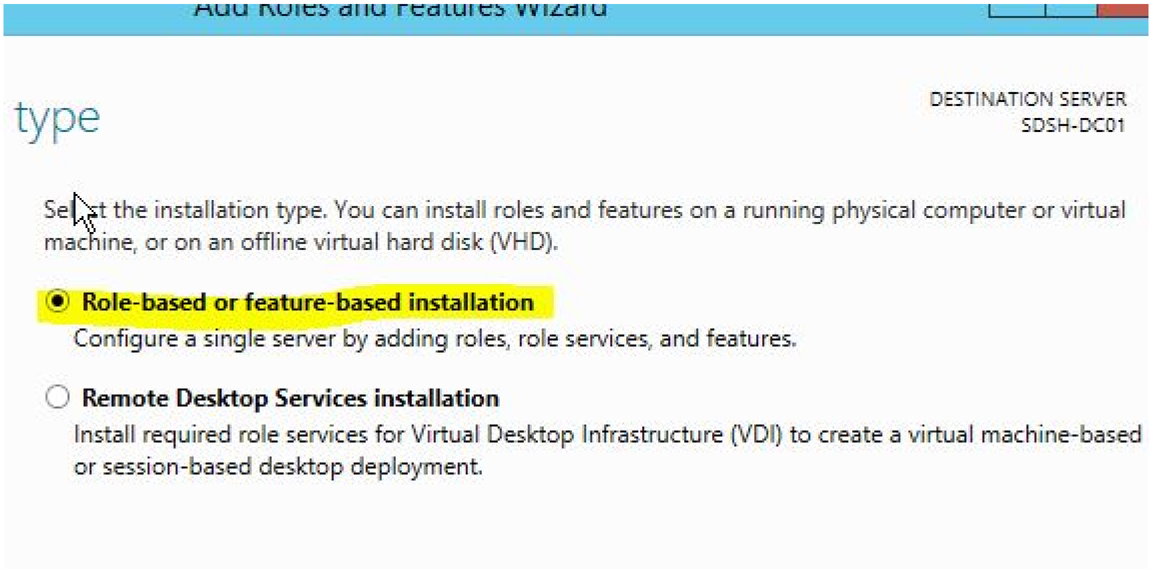
Promoting the Server to a Domain Controller

Create Forest and enter a domain name.

Go to Server Manager and click Add roles and features


DC-2012R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Local Server 1
Manageability
Events

Select the first option: – Role-based or feature-based installation

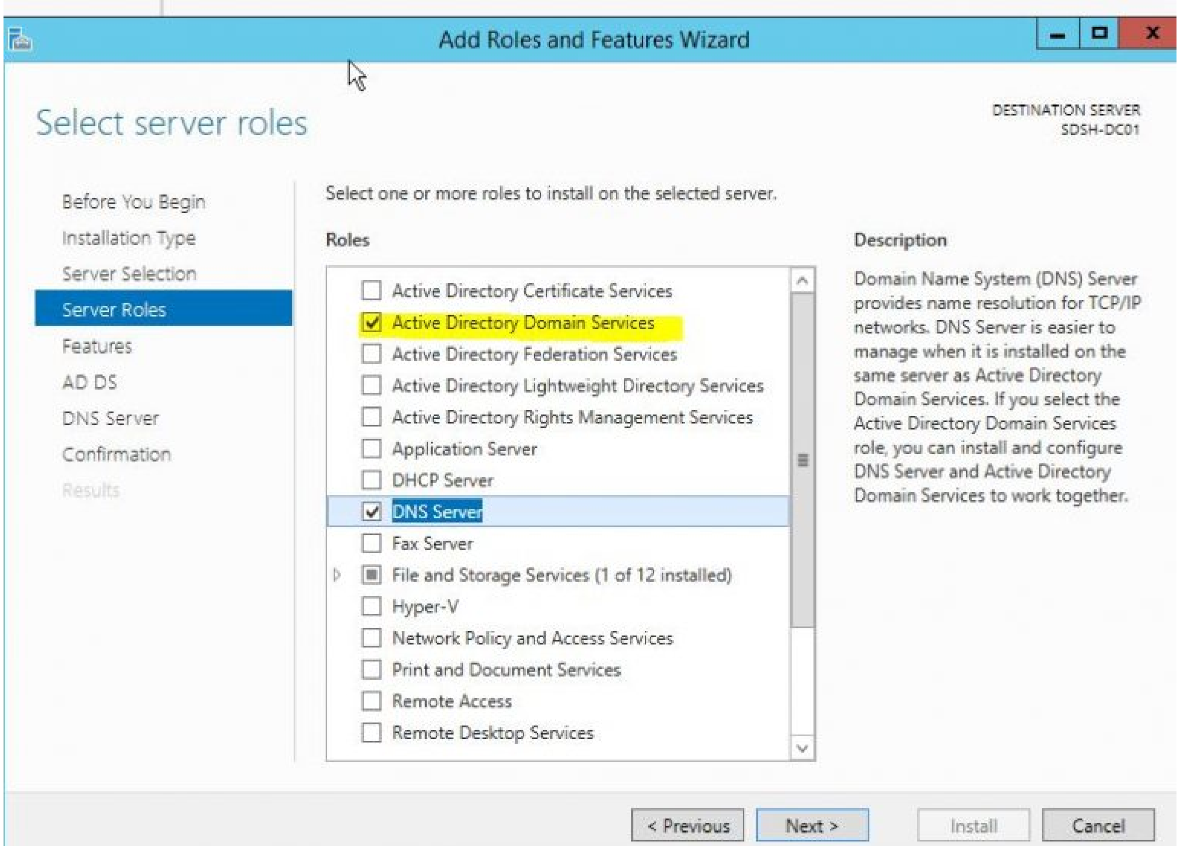


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

○ Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Click next until you reach the step to select roles. Select “Active Directory Domain Services” and click “Add Features” to the window that pops up. Click next.



Select server roles

DESTINATION SERVER
SDSH-DC01

Select one or more roles to install on the selected server.

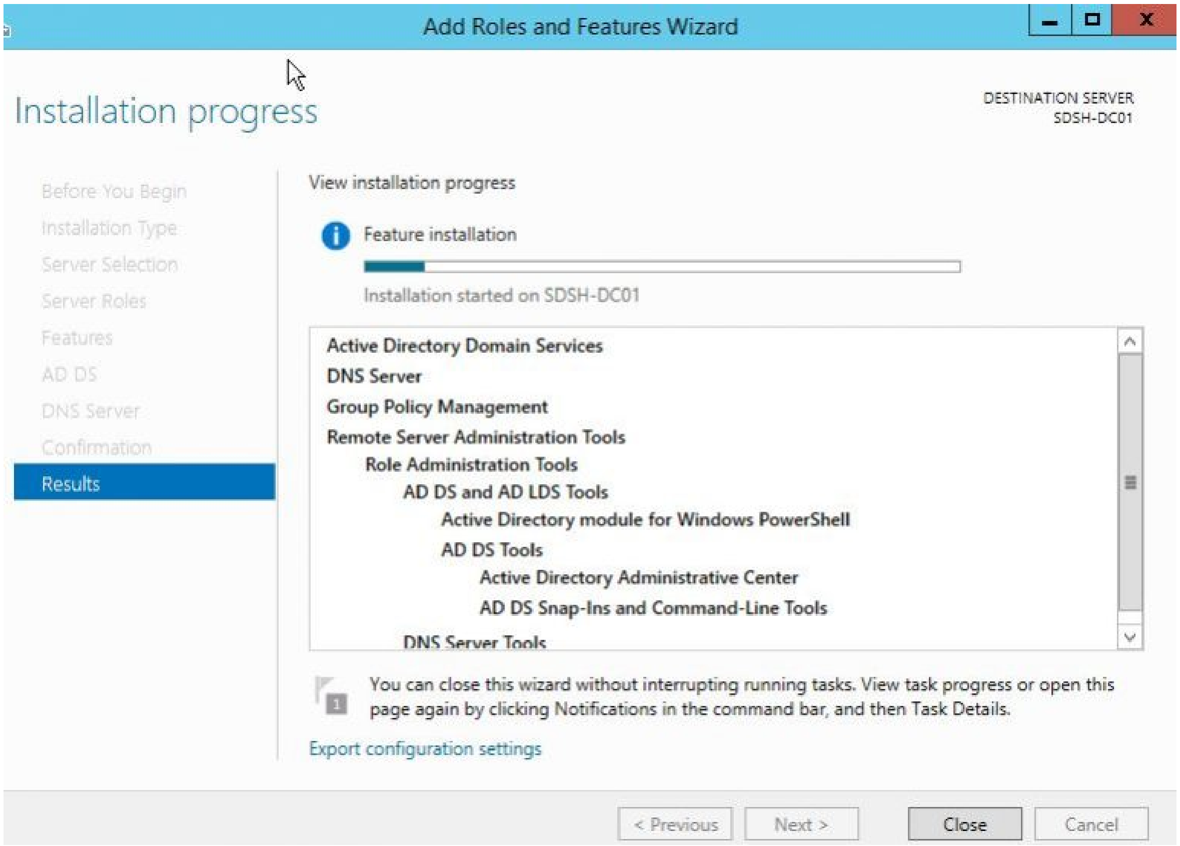
Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

Keep clicking "Next" until it installs roles and features. It takes some time to install the roles.



Installation progress

DESTINATION SERVER
SDSH-DC01

View installation progress

Feature installation

Installation started on SDSH-DC01

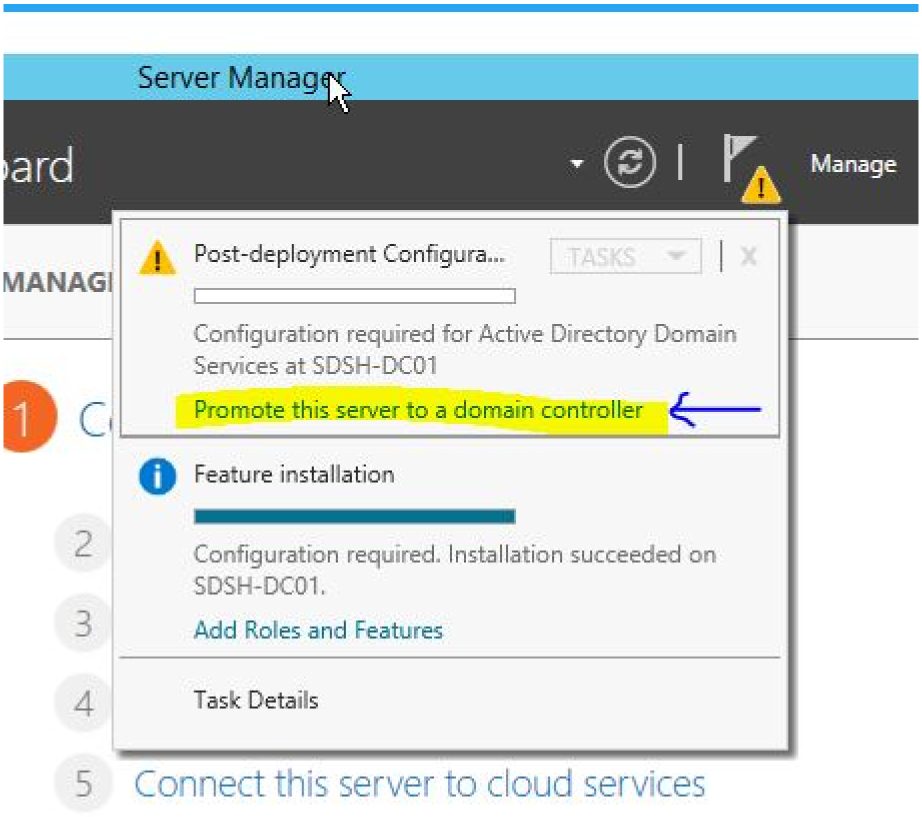
Active Directory Domain Services
DNS Server
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools
        DNS Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

- **Promoting the Server to a Domain Controller**

After the roles and features are installed, it will show an exclamation mark in the Server Manager. Click this to select the option to "*Promote this Server to Domain Controller*"



Post-deployment Configura...

Configuration required for Active Directory Domain Services at SDSH-DC01

Promote this server to a domain controller

Feature installation

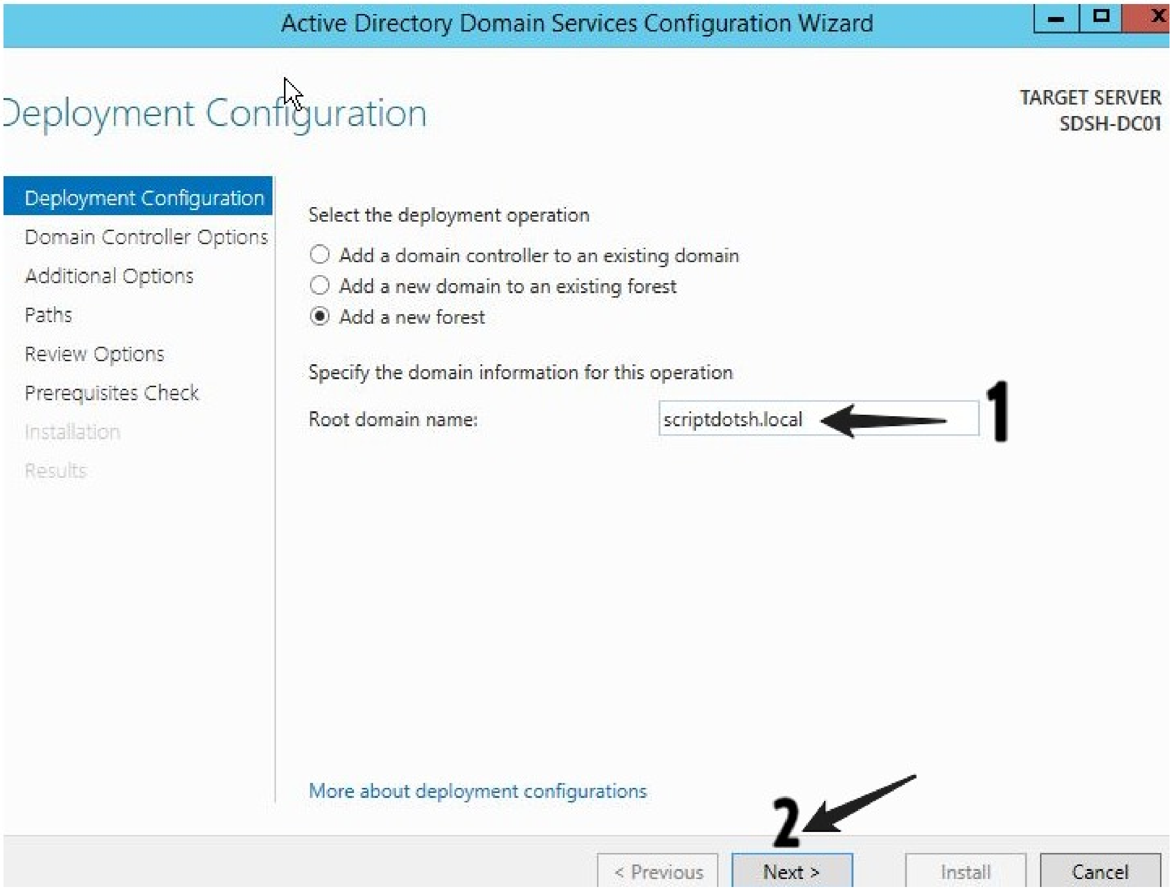
Configuration required. Installation succeeded on SDSH-DC01.

Add Roles and Features

Task Details

- **Add a new forest**

Here, it shows an option to create a forest. Select "Add a New Forest" and enter a domain name. I named the forest as "scriptdotsh.local"



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SDSH-DC01

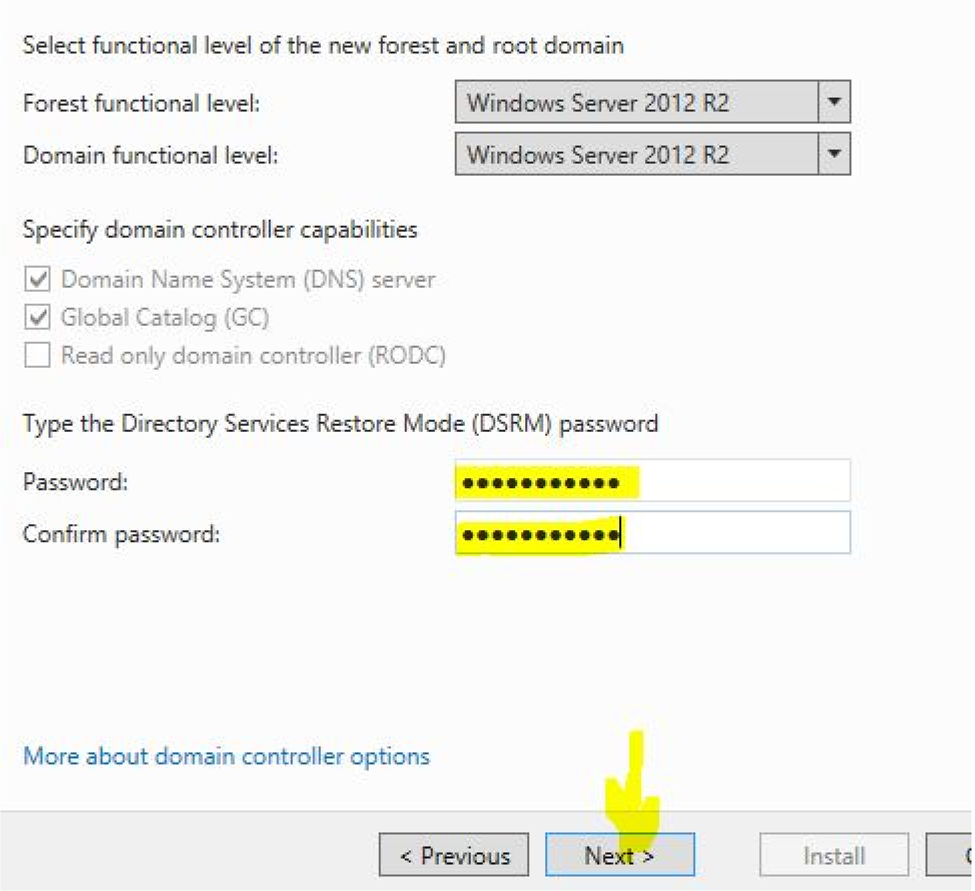
Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: scriptdotsh.local

Click next. On the next screen, leave the defaults as it is and create a recovery password. This is called **DSRM** password. This password provides the administrator with a kind-of backdoor to the AD database in case there is some issue with the domain or when you need to restore/recover the AD database.



Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

Just accept the defaults in the next series of prompts. It will check some pre-requisites and show some warnings, that's Okay. Click "Install". Now in the backend, installation and configuration of Active Directory and DNS will take place and then the server will reboot. After the reboot, your domain controller is ready! A logon screen will appear. You can log in using the same Administrator account. Please note that now the account is promoted to a Domain Administrator as the computer is a Domain Controller now. Below is the format for login:

Username– scriptdotsh\Administrator

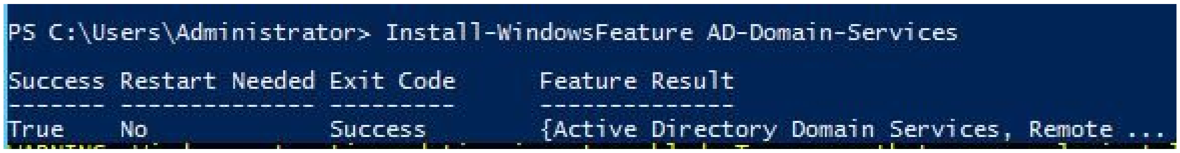
Password– XXXXXXXXX

CommandLine-Fu

In only 4 commands, you can set up the domain controller. In short, these 4 commands will do the same things that was explained above in GUI way. Run PowerShell as administrator and enter below commands:

- **Installing AD DS Role**

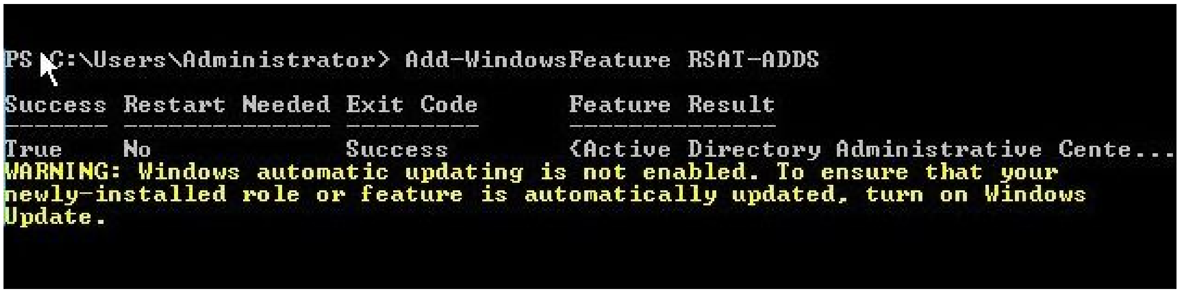
```
Install-windowsFeature AD-Domain-Services
```



```
PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Remote ...
```

- **Installing ADDS RSAT features:**

```
Add-windowsfeature RSAT-ADDS
```



```
PS C:\Users\Administrator> Add-WindowsFeature RSAT-ADDS

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Administrative Cente...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is automatically updated, turn on Windows
Update.
```

- **Promoting the Server to a Domain Controller**

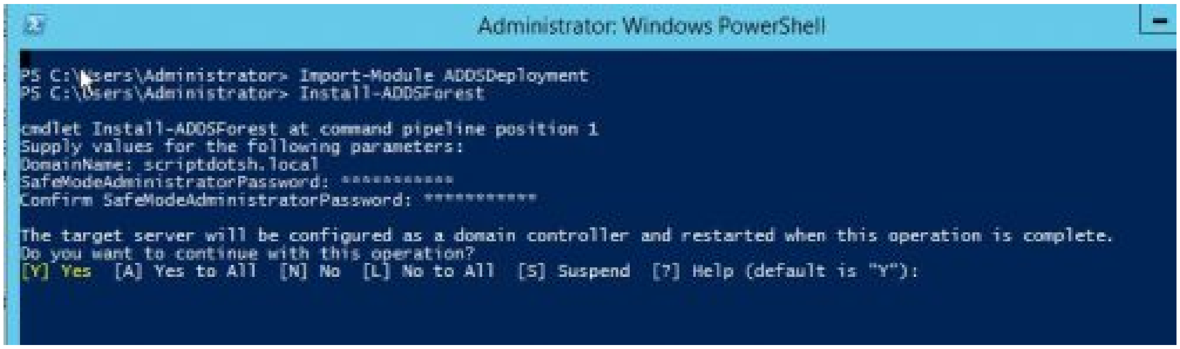
```
Import-Module ADDSDeployment
```

Note: There will be no output for this command.

- **Add a new forest**

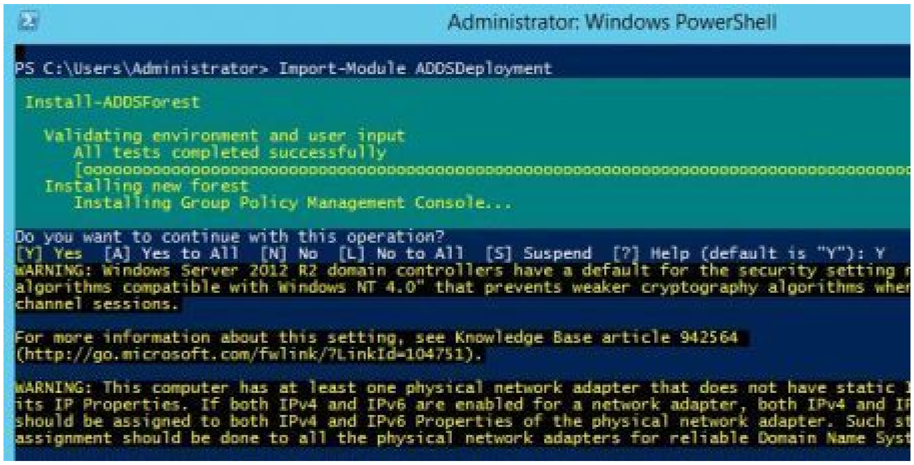
```
Install-ADDSForest
```

Enter the domain name and password and select “Yes” to continue.



```
PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator> Install-ADDSForest

cmdlet Install-ADDSForest at command pipeline position 1
Supply values for the following parameters:
DomainName: scriptdotsh.local
SafeModeAdministratorPassword: ***********
Confirm SafeModeAdministratorPassword: ************

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

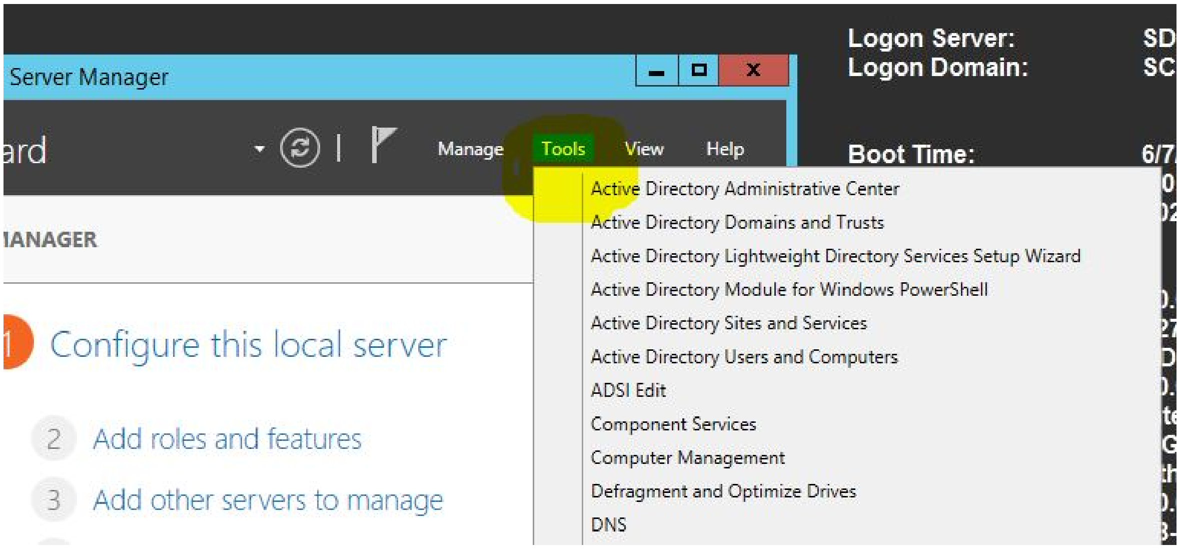
AD Domain forest “scriptdotsh.local” is being installed



```
PS C:\Users\Administrator> Import-Module ADDSDeployment

 Install-ADDSForest

   Validating environment and user input
      All tests completed successfully
      [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
   Installing new forest
      Installing Group Policy Management Console...

Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
WARNING: Windows Server 2012 R2 domain controllers have a default for the security setting n
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms wher
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: This computer has at least one physical network adapter that does not have static I
its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IP
should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such st
assignment should be done to all the physical network adapters for reliable Domain Name Syst
```

It takes a few minutes to complete the operation and then the server will reboot. After reboot, your domain controller is ready! Login in same way as shown in above GUI section.

Once you're in, you can explore different AD tools:


Server Manager
ard
Manage
Tools
View
Help
IANAGER
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Logon Server:
Logon Domain:
Boot Time:
SD
SC
6/7

Epilogue

I believe this would be it for the first blog post. In the next post, I will populate AD with DHCP, member servers, Proxy Server, client machines, users etc. And after that, I will start with recon, exploiting misconfigurations and DC based attacks and hunts. Do comment below if you have any doubt :). You're welcome to provide any suggestions to add into this series. Stay tuned for coming blogs 🙂

Winsaaf Man

Security Engineer | Security Analytics using #ELK | #Pentesting AD | #ActiveDirectory Attacks | Blogger | Twitter ID is @WinsaafMan

Tags: Active Directory, Pentesting Active Directory, Windows AD

Written by

Winsaaf Man

Security Engineer | Security Analytics using #ELK | #Pentesting AD | #ActiveDirectory Attacks | Blogger | Twitter ID is @WinsaafMan

View all posts by Winsaaf Man

5 COMMENTS

finch

May 22, 2019 at 12:03 pm

Thanks a lot mate really great job thanks for sharing

Umar

April 28, 2019 at 3:46 pm

Just what I was looking for, thank you very much <3

Tushar

December 4, 2018 at 10:56 pm

Awesome very knowledgeable great !

Thanks !

sanjeev jha

October 30, 2018 at 12:26 pm

Very comprehensive…I was waiting for such writeup.

Winsaaf Man □

October 30, 2018 at 1:50 pm

Thanks 🙂

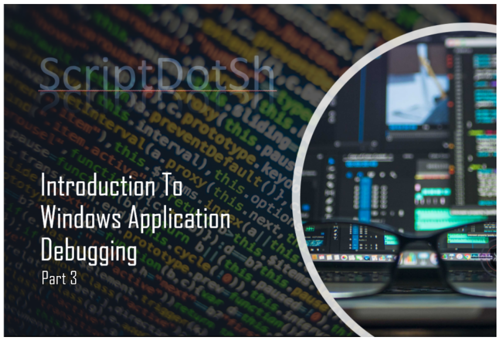
We don't get paid for writing these blogs. If you enjoy reading our blogposts and would like to support our work, you can buy us a coffee by donating here:
14mN2S5JYmy98KDFWkxC33Urhmu8NvHP3X
Or scan the **QR Code** here

RECENT POSTS

← →

May 13, 2019

Understanding Windows OS Architecture – Theory



May 4, 2019

WinDBG Configuration