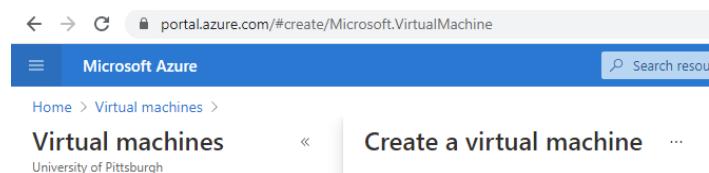


## Active Directory & DNS

The purpose of this assignment is to create your own Microsoft Active Directory Domain Services (AD DS) and work with DNS. A server running the AD DS role is called a domain controller. You will create your domain controller (DC) using a [Microsoft Azure](#). Using your Azure for Students subscription you will create three VMs; a bastion host, DC, and fileserver. (Note: If you are working on this assignment over an extended period of time be sure to power-off / shutdown the VMs so you can reduce the cloud charges.)

1. (5 points) Using the existing VNET and subnets from your previous assignment. Create a Windows VM with the following properties to be used for your bastion host.

- Resource group: LastnameDevVMs
- Name: LastnameBastionHost
- Image: windows server 2019
- Size: Standard\_B1s
- Create a username and password.
- Use default disks
- For Networking select the VNET you created earlier and select the DMZ subnet
- The rest of the settings can be left to defaults
- Create the VM



Provide screenshot(s) showing your VM was created, as well as the following:

- Virtual Machine Name



- Public IP assigned
  - 20.84.61.223
- Private IP assigned
  - 10.0.0.5

# Active Directory & DNS

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20220330220014 >

**CrichtonBastionHost** Virtual machine

Search (Cmd+)

Connect Start Stop Capture Delete Refresh Open in mobile CLI / PS Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Essentials

Resource group (move) : CrichtonDevVMs

Status : Running

Location : East US (Zone 1)

Subscription (move) : Azure for Students

Subscription ID : 94830b48-a466-499c-a767-0e143455e26b

Availability zone : 1

Tags (edit) : Click here to add tags

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard B1s (1 vcpu, 1 GiB memory)

Public IP address : 20.84.61.223

Virtual network/subnet : CrichtonDevVNET/DMZ

DNS name : Not configured

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	CrichtonBastion
Health state	-
Operating system	Windows (Windows Server 2019 Datacenter)
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-datacenter-gensecond
VM generation	V2
Agent status	Ready
Agent version	2.7.41491.1032
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

Networking

Public IP address	20.84.61.223
Public IP address (IPv6)	-
Private IP address	10.0.0.5
Private IP address (IPv6)	-
Virtual network/subnet	CrichtonDevVNET/DMZ
DNS name	Configure

Size

Size	Standard B1s
vCPUs	1
RAM	1 GiB

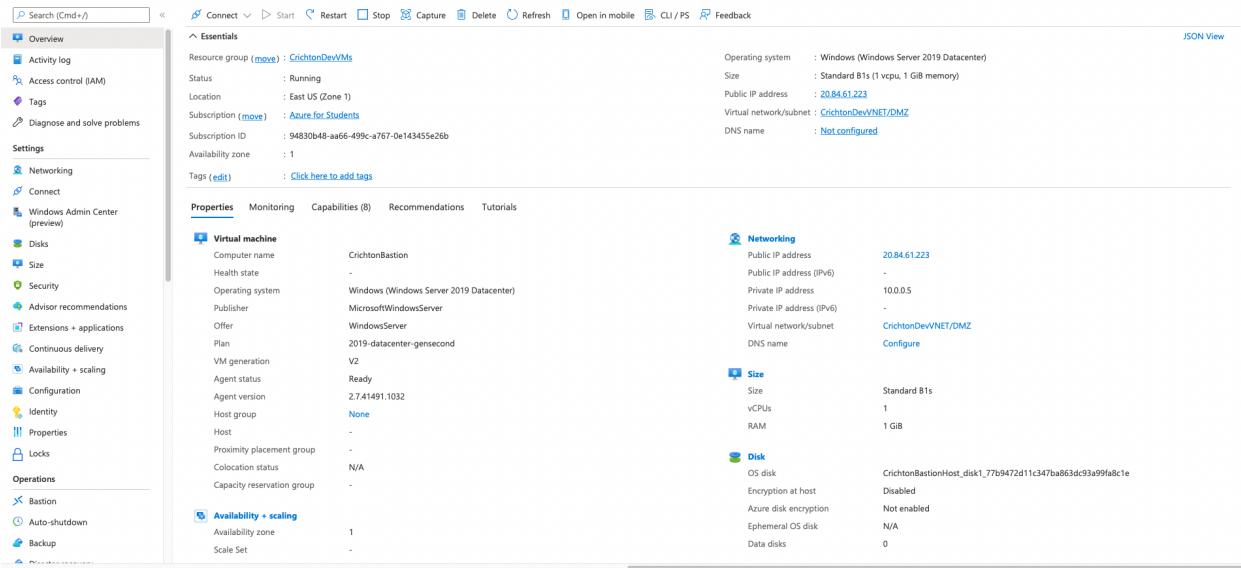
Disk

OS disk	CrichtonBastionHost_disk1_77b9472d11c347ba863dd53a99fa8c1e
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

Availability + scaling

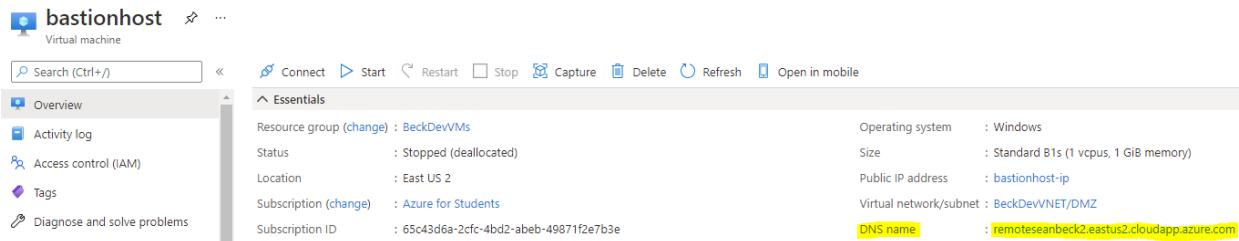
Availability zone	1
Scale Set	-

JSON View



## Active Directory & DNS

2. (5 points) Create a unique Azure DNS name for your LastnameBastionHost and explain what the purpose is of this DNS name? Provide a screenshot showing your DNS name.



The screenshot shows the Azure portal interface for a virtual machine named 'bastionhost'. In the 'Overview' section, under the 'Essentials' tab, the 'DNS name' field is highlighted in yellow and contains the value 'remoteSeanbeck2.eastus2.cloudapp.azure.com'.

Networking	
Public IP address	<a href="#">20.84.61.223</a>
Public IP address (IPv6)	-
Private IP address	10.0.0.5
Private IP address (IPv6)	-
Virtual network/subnet	<a href="#">CrichtonDevVNET/DMZ</a>
DNS name	<a href="#">remotebcrichton.eastus.cloudapp.azure.com</a>

The purpose of the DNS name is so you can add a mask to the IP address that you are connecting to. For example, instead of remembering the 192.168.0.0 number, you can just type in remote.domainname.com into the remote desktop and it will connect to that assigned machine. The DNS name acts sort of as a static ip, to where when you remote desktop into the VM, you can just type in the DNS name above, and it will always connect to that VM, no matter what the public IP is.

## Active Directory & DNS

3. (5 points) Using Google Domains create the following two DNS records for your domain that you registered earlier in the semester:

- remote, CNAME, DNS name from previous question
- remote2, A-record, public IP for BastionHost

Provide screenshot(s) of your records.

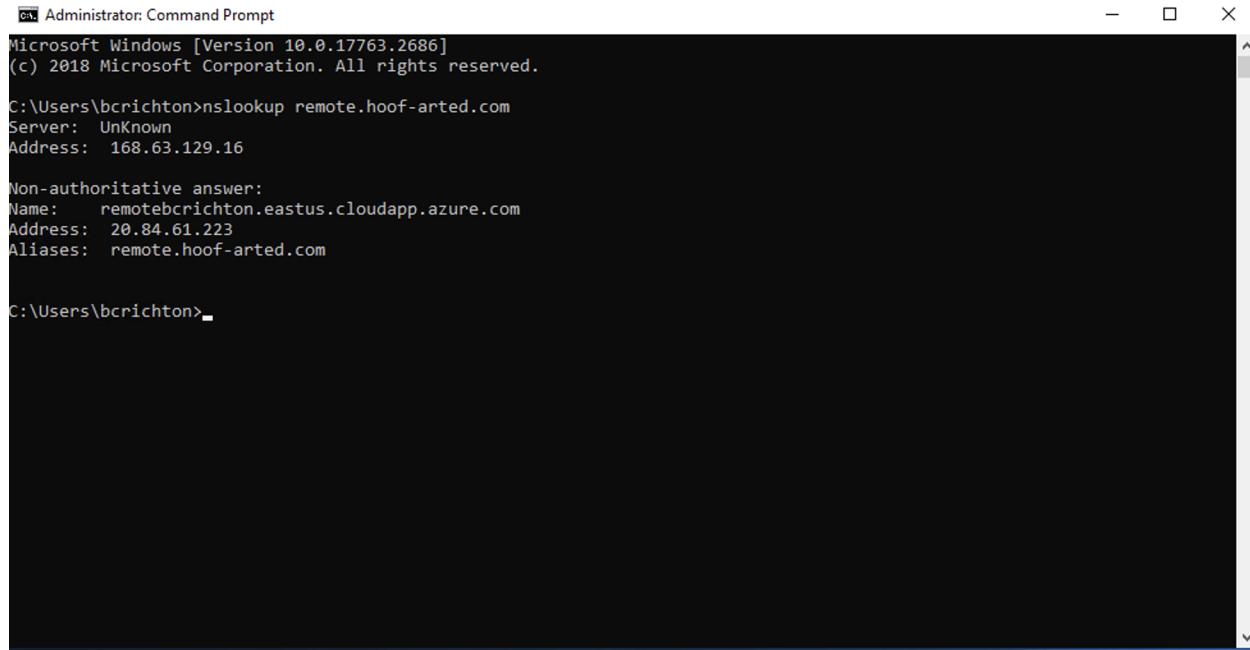
The screenshot shows the Google Domains DNS management interface. It displays two DNS records:

Host name	Type	TTL	Data
remote	CNAME	1h	remoteseanbeck2.eastus2.cloudapp.azure.com.
remote2	A	1h	52.184.229.158

Below the records, there are sections for "Resource records" and "Custom records". The "Custom records" section lists the same two entries with their details. There is also a "Required" section for informational records.

## Active Directory & DNS

4. (5 points) Using the nslookup command verify that the DNS records created in the last step have propagated to public DNS servers. (Hint: You may need to wait a few minutes)



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2686]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\bcrichton>nslookup remote.hoof-arted.com
Server: Unknown
Address: 168.63.129.16

Non-authoritative answer:
Name:    remotebcrichton.eastus.cloudapp.azure.com
Address: 20.84.61.223
Aliases: remote.hoof-arted.com

C:\Users\bcrichton>
```

5. (5 points) Use the Remote Desktop Protocol (RDP) to connect to your newly created BastionHost VM.

## Active Directory & DNS

- Instead of connecting via IP use the remote and remote2 DNS records previously created. Provide a screenshot(s) showing you successfully connecting using both records.



## Active Directory & DNS

7. (5 points) Create two Windows VMs with the following properties to be used for your DC and fileserver:

- DC
  - Resource group: LastnameDevVMs
  - Name: LastnameDC1
  - Image: windows server 2019
  - Size: Standard\_B2s
  - Create a username and password.
  - Use default disks
  - For Networking select the VNET you created earlier and select the Intranet subnet
  - Public IP should be set to none
  - The rest of the settings can be left to defaults
  - Create the VM
- Fileserver
  - Resource group: LastnameDevVMs
  - Name: LastnameFile1
  - Image: windows server 2019
  - Size: Standard\_B1ms
  - Create a username and password.
  - Use default disks
  - For Networking select the VNET you created earlier and select the Intranet subnet
  - Public IP should be set to none
  - The rest of the settings can be left to defaults
  - Create the VM

Configure both VMs to have static private IPs.

Provide screenshot(s) showing your VMs were created, as well as the following:

- Virtual Machine Name
- Static Private IP
- No Public IP assigned

# Active Directory & DNS

CrichtonDC1:

The screenshot shows the Azure portal interface for a virtual machine named "CrichtonDC1". The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Networking, Connect, Windows Admin Center (preview), Disks, Size, Security, Advisor recommendations, Extensions + applications, Continuous delivery, Availability + scaling, Configuration, Identity, Properties, Locks), Operations (Bastion, Auto-shutdown, Backup, Disaster recovery), and Help & feedback.

The main content area displays the "Essentials" tab under the "Properties" section. It includes the following details:

Setting	Value
Resource group (move)	CRICHTONDEVVMS
Status	Running
Location	East US (Zone 1)
Subscription (move)	Azure for Students
Subscription ID	94830b48-aa66-499c-a767-0e143455e26b
Availability zone	1
Tags (edit)	Click here to add tags

Below the Essentials tab, there are several other tabs: Properties, Monitoring, Capabilities (8), Recommendations, and Tutorials. The "Properties" tab is currently selected.

Under the "Properties" tab, there are three main sections: Virtual machine, Networking, and Size.

**Virtual machine:**

Setting	Value
Computer name	CrichtonDC1
Health state	-
Operating system	Windows (Windows Server 2019 Datacenter)
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-datacenter-gensecond
VM generation	V2
Agent status	Ready
Agent version	2.7.41491.1044
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

**Networking:**

Setting	Value
Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.132
Private IP address (IPv6)	-
Virtual network/subnet	CrichtonDevVNET/intranet
DNS name	-

**Size:**

Setting	Value
Size	Standard B2s
vCPUs	2
RAM	4 GiB

**Disk:**

Setting	Value
OS disk	CrichtonDC1_OsDisk_1_d39c6d2f36a247e093443d0fe712072f
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

## Active Directory & DNS

[Home](#) > [Virtual machines](#) > [CrichtonDC1](#) > [crichtondc1787\\_z1](#) >

### ipconfig1

...

crichtondc1787\_z1



Save



Discard

---

Public IP address settings

Public IP address

[Disassociate](#)

[Associate](#)

Private IP address settings

Virtual network/subnet

[CrichtonDevVNET/Intranet](#)

Assignment

[Dynamic](#)

[Static](#)

IP address \*

10.0.0.132

# Active Directory & DNS

## CrichtonFile1:

The screenshot shows the Azure portal interface for a virtual machine named "CrichtonFile1". The main pane displays the "Essentials" section with details like Resource group (CrichtonDevVMs), Status (Running), Location (East US (Zone 1)), and Subscription (Azure for Students). The "Properties" tab is selected, showing sections for Virtual machine, Networking, Size, and Disk. The "Virtual machine" section includes fields for Computer name, Health state, Operating system, Publisher, Offer, Plan, VM generation, Agent status, Agent version, Host group, Host, Proximity placement group, Colocation status, Capacity reservation group, Availability zone, and Scale Set. The "Networking" section shows Public IP address (-), Private IP address (10.0.0.133), Private IP address (IPv6) (-), Virtual network/subnet (CrichtonDevVNET/intranet), and DNS name (-). The "Size" section shows Standard B1ms, 1 vCPU, and 2 GiB RAM. The "Disk" section shows the OS disk (CrichtonFile1\_OsDisk\_1\_36fc...), Encryption at host (Disabled), Azure disk encryption (Not enabled), Ephemeral OS disk (N/A), and Data disks (0).

Home > Virtual machines > CrichtonFile1 > crichtonfile1663\_z1 >

## ipconfig1

crichtonfile1663\_z1

Save Discard

### Public IP address settings

#### Public IP address

Disassociate Associate

### Private IP address settings

#### Virtual network/subnet

CrichtonDevVNET/intranet

#### Assignment

Dynamic Static

#### IP address \*

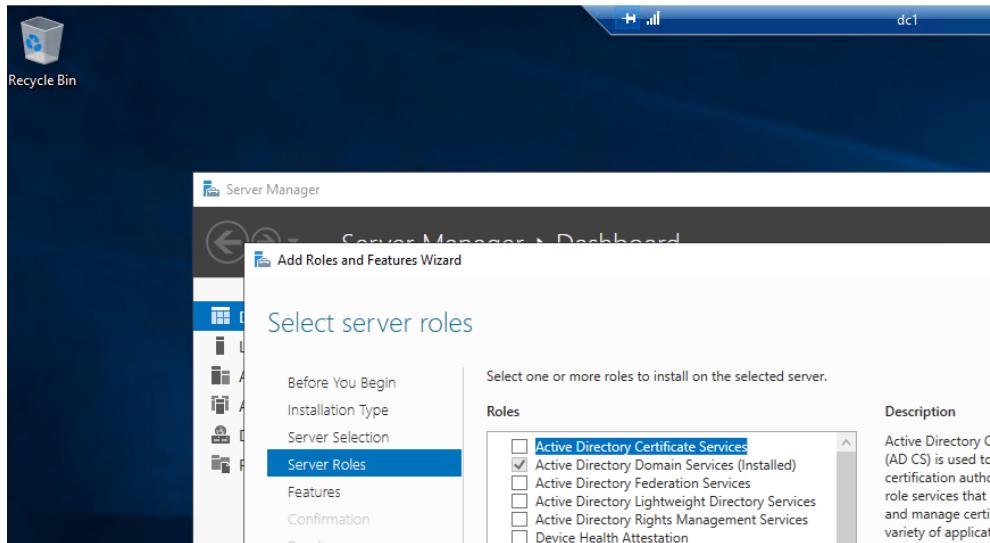
10.0.0.133

## Active Directory & DNS

7. (15 points) Use the Remote Desktop Protocol (RDP) to connect to your newly created BastionHost VM, then RDP to your domain controller (DC). Install / add the Active Directory Domain Services role to the Windows 2019 server. Use the following URL as a guide to aid you during the install:

<https://www.windowscrush.com/promote-windows-server-2019-to-domain-controller.html>

\*Remember since you made the VMs private IPs static in Azure, you do not need to configure the Windows server with a static IP.

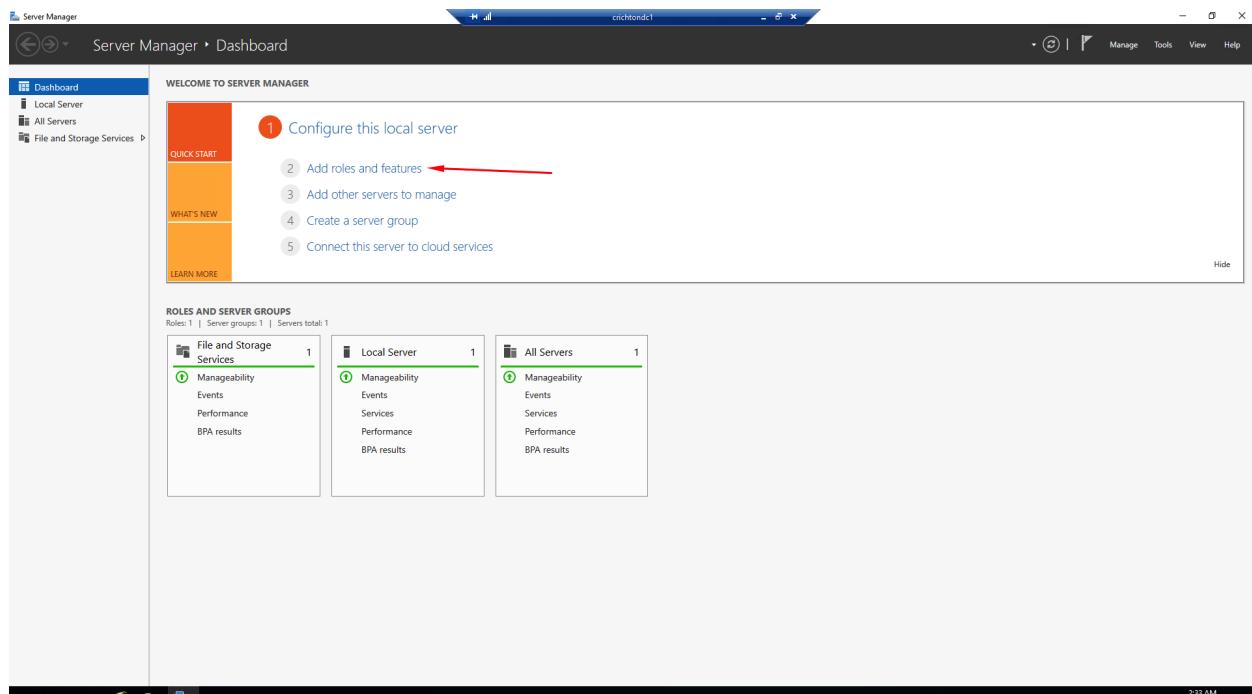


**NOTE: Your root domain name should be ad.yourdomain (ie. ad.seanbeck.com)**

Provide screenshot(s) showing your installation and configuration of AD DS.

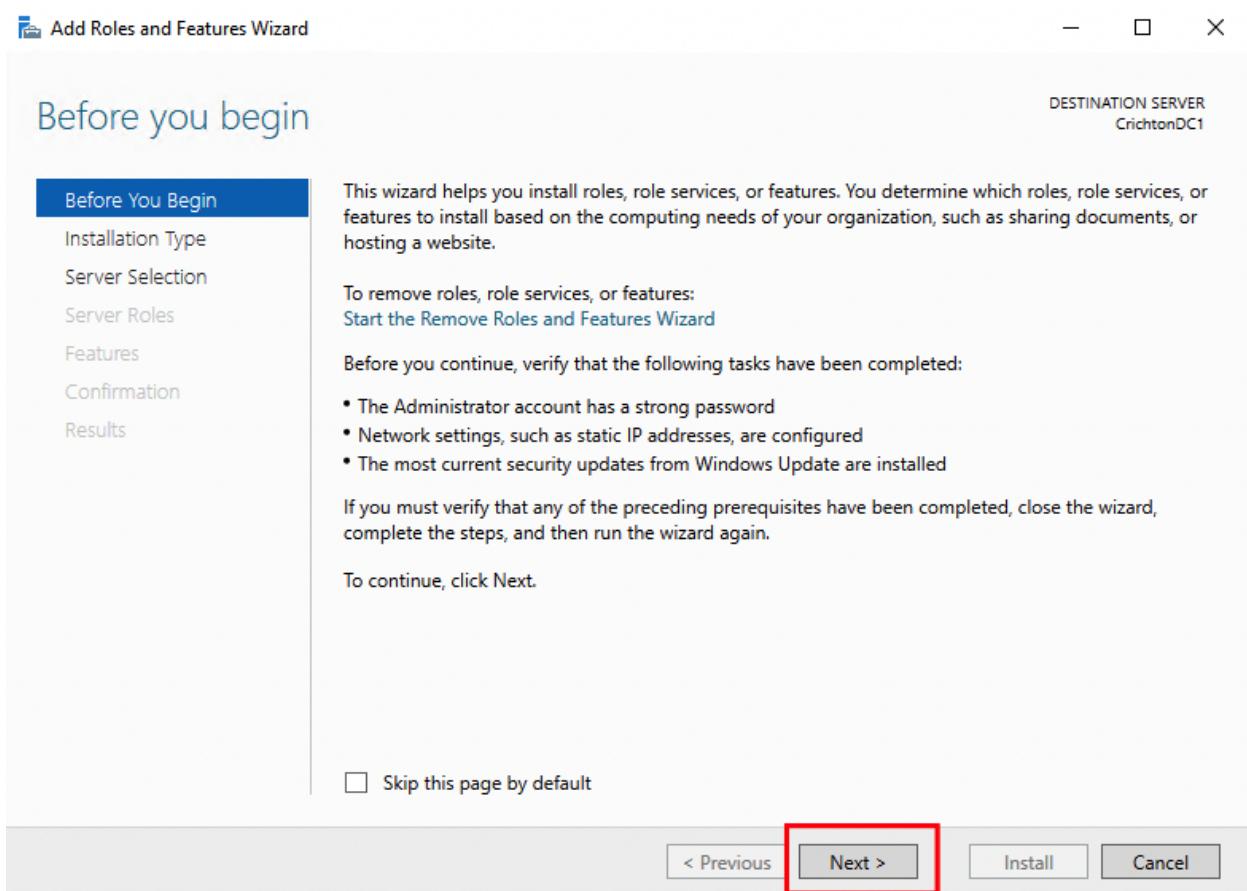
# Active Directory & DNS

Click the **Add Roles and Features** link.



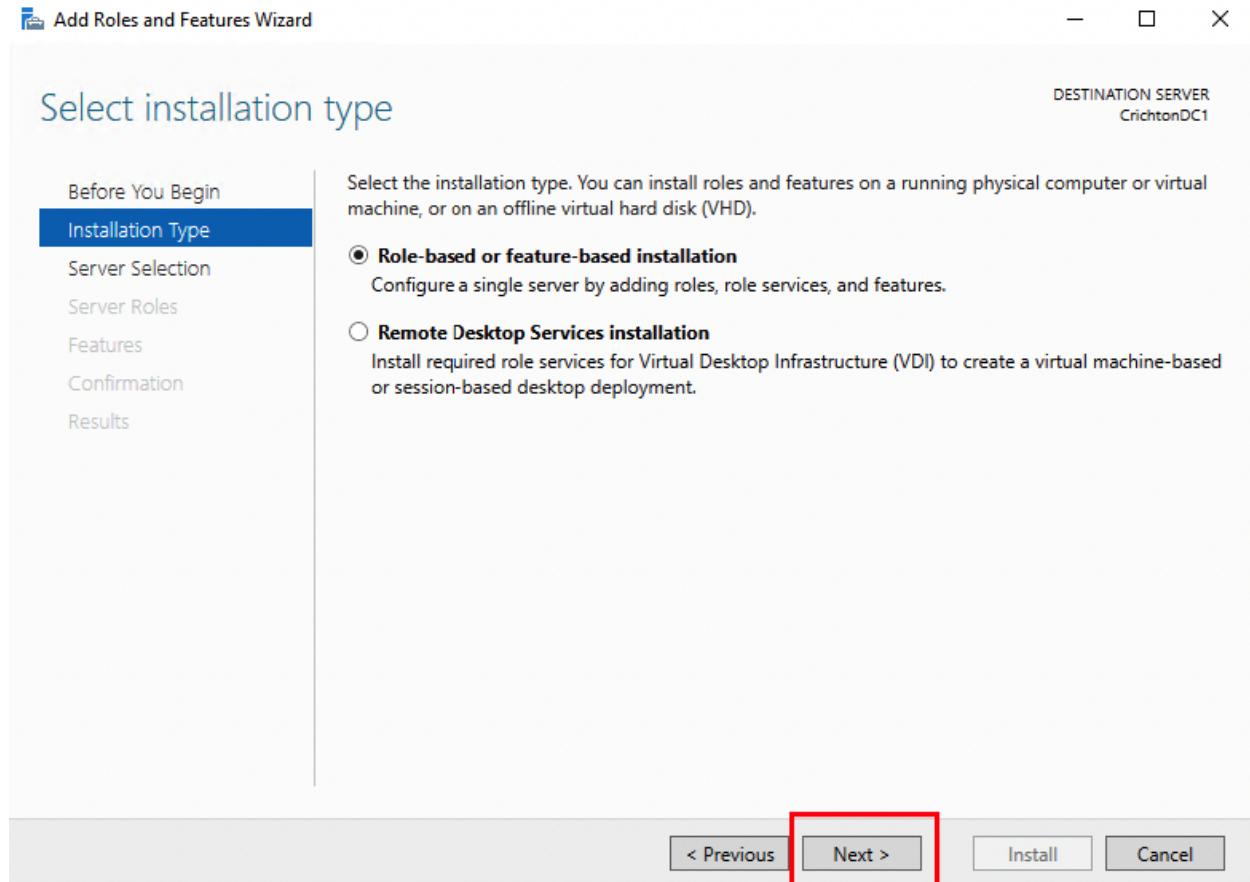
# Active Directory & DNS

Click **Next**



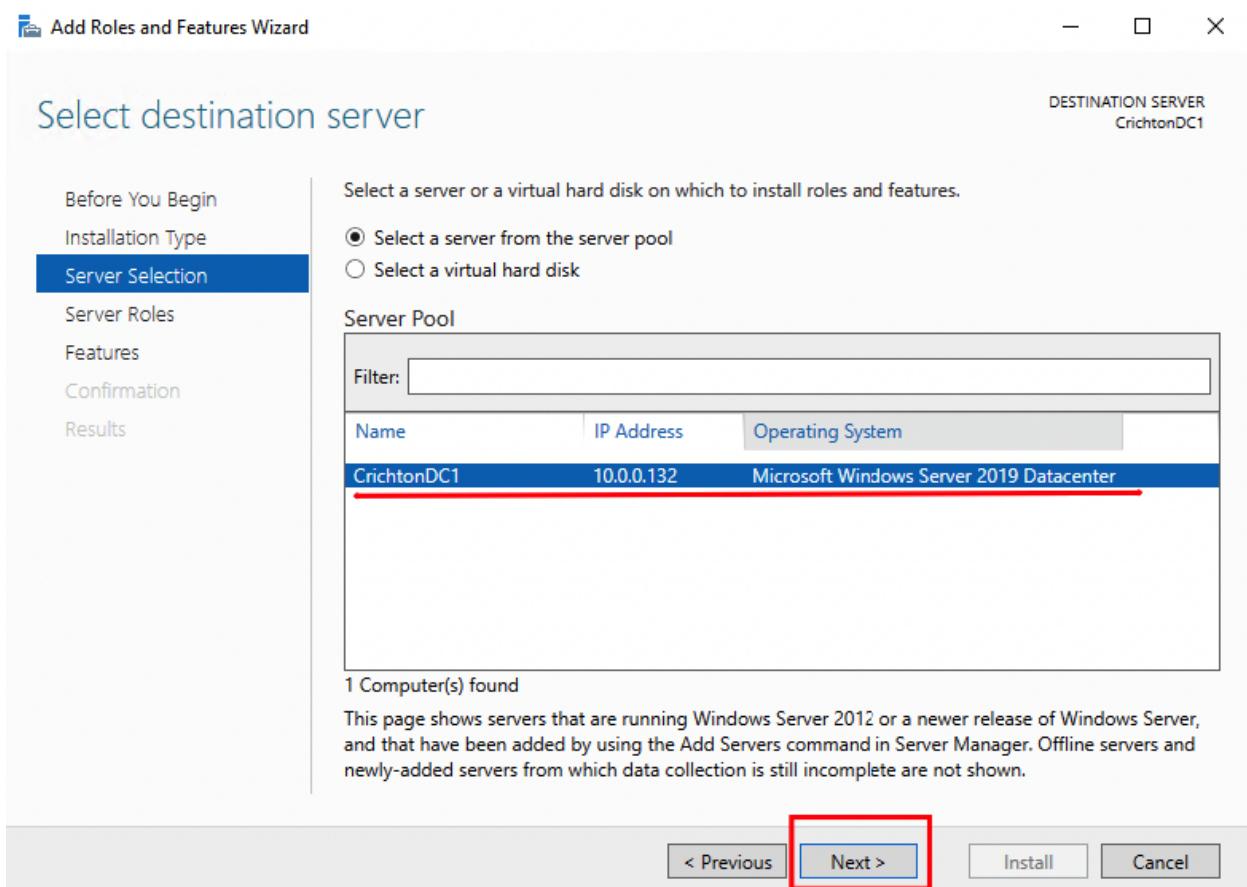
## Active Directory & DNS

Select the desired installation type, in this case we are going to choose **Role-based or feature-based installation**, then click **Next**.



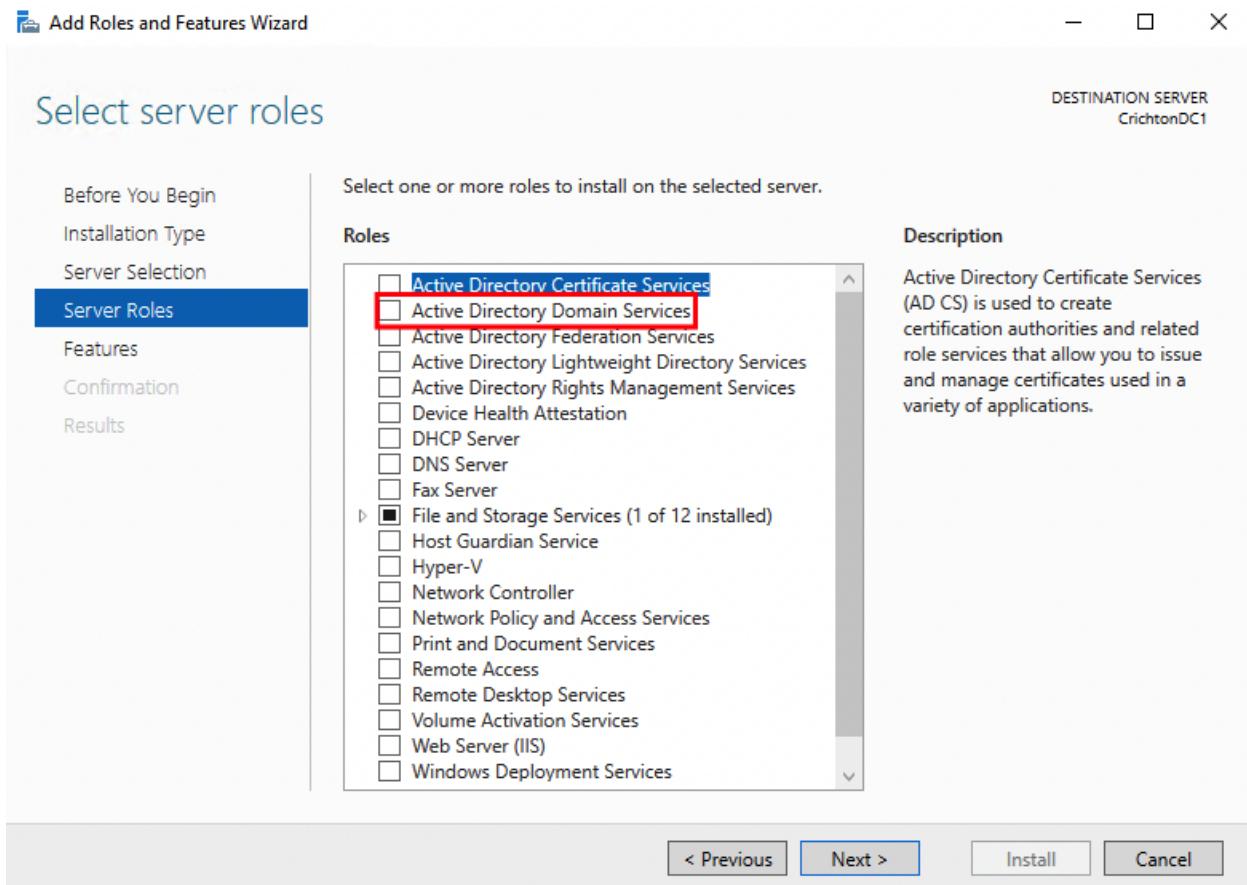
# Active Directory & DNS

Ensure that the correct DC1 server is on the list, then click **Next**.



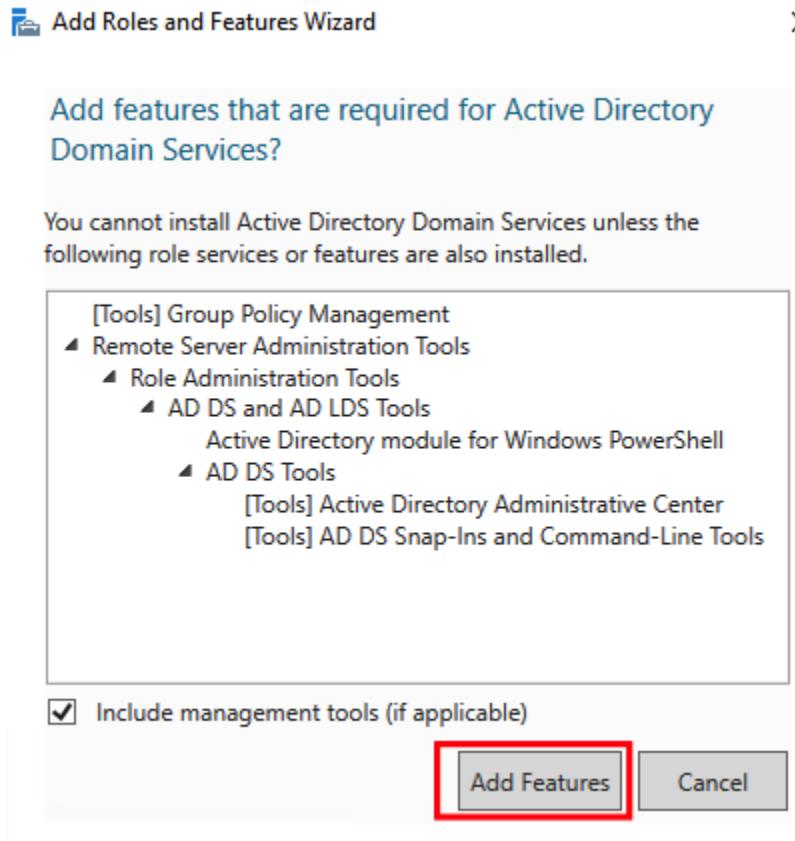
# Active Directory & DNS

Check the **Active Directory Domain Services** server role.



## Active Directory & DNS

The **Add Roles and Features Wizard** will appear. The roles and features that are going to be installed are listed in below. Confirm that these are correct, and then click **Add Features**.

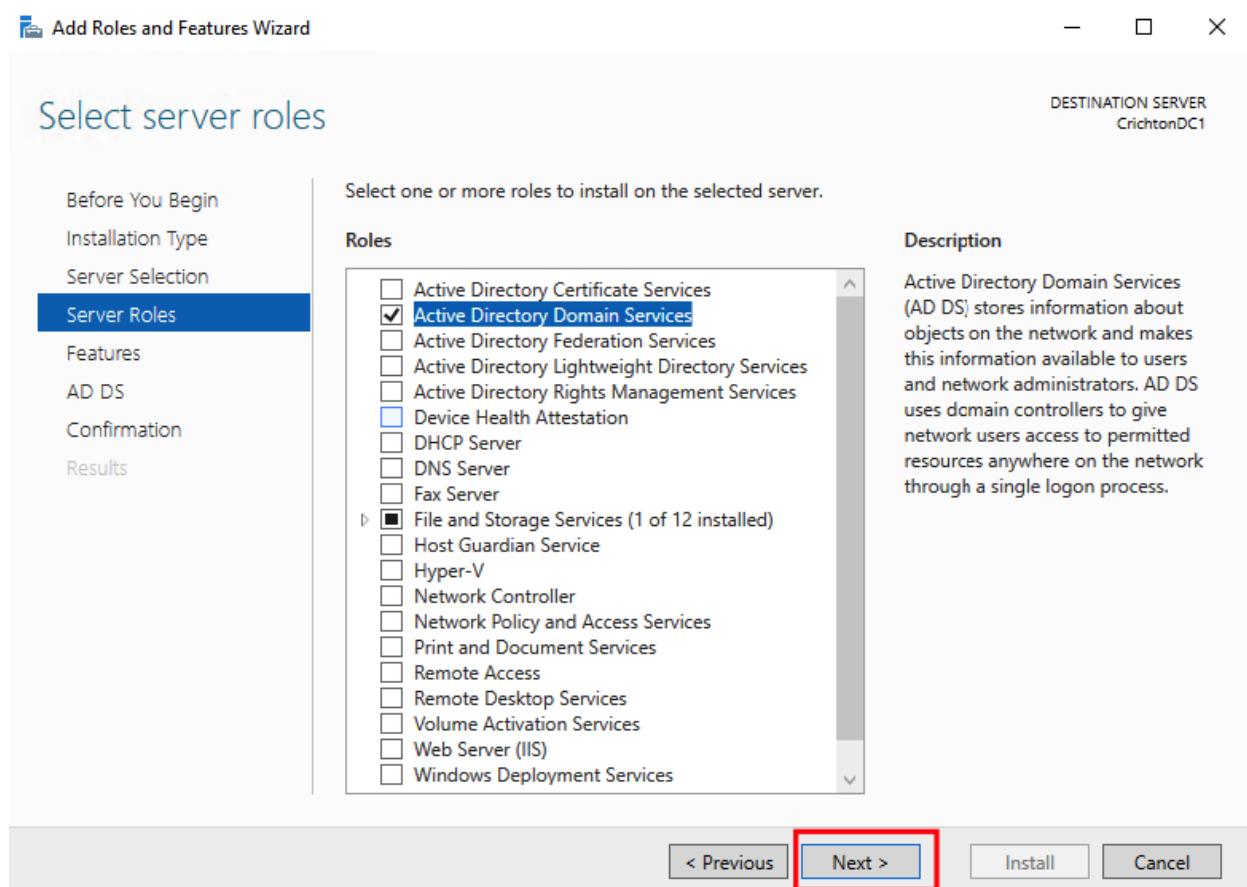


Include management tools (if applicable)

**Add Features** **Cancel**

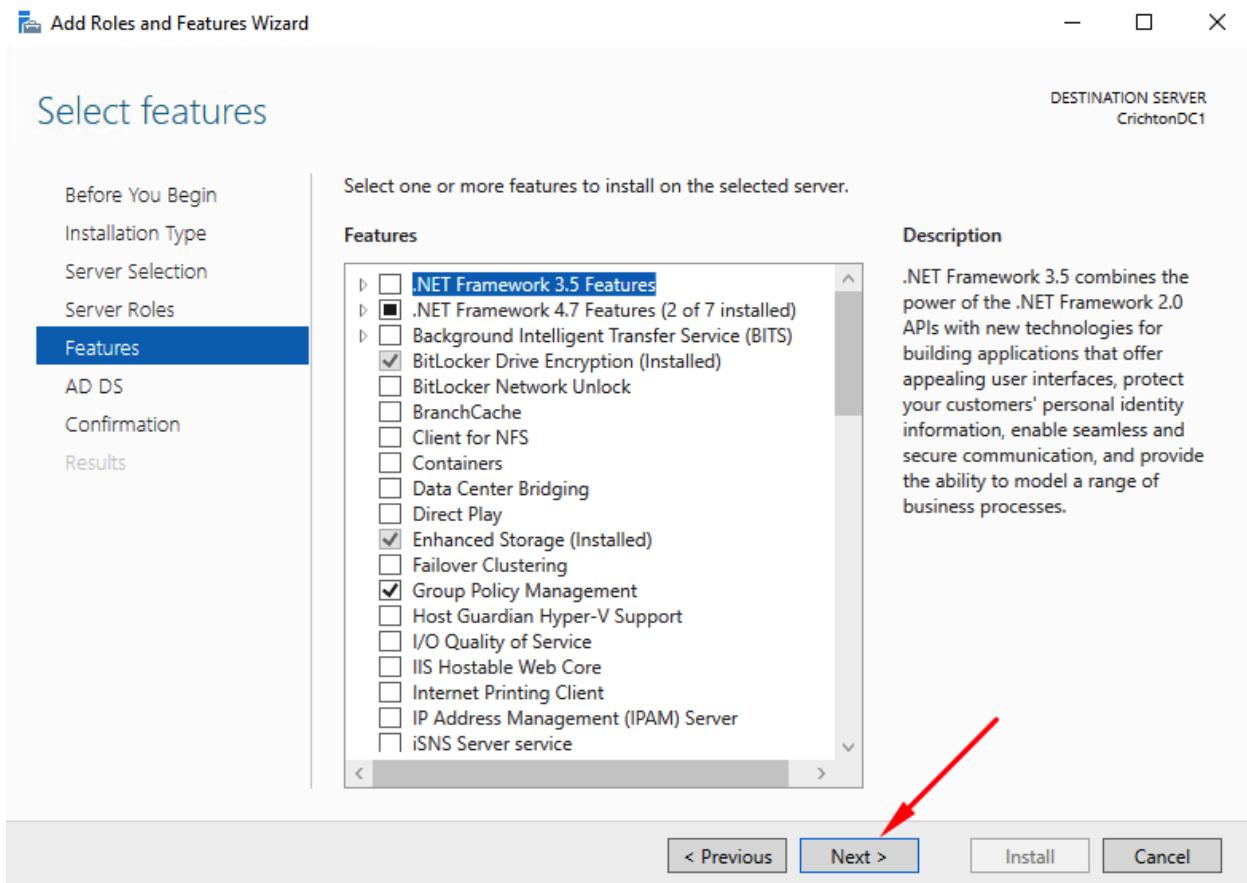
## Active Directory & DNS

Ensure that there is a check next to **Active Directory Domain Services** after the wizard has completed the installation, then click **Next**.



# Active Directory & DNS

Click **Next**



Click **Next**.

# Active Directory & DNS

Add Roles and Features Wizard

## Active Directory Domain Services

DESTINATION SERVER  
CrichtonDC1

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
**AD DS**  
Confirmation  
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

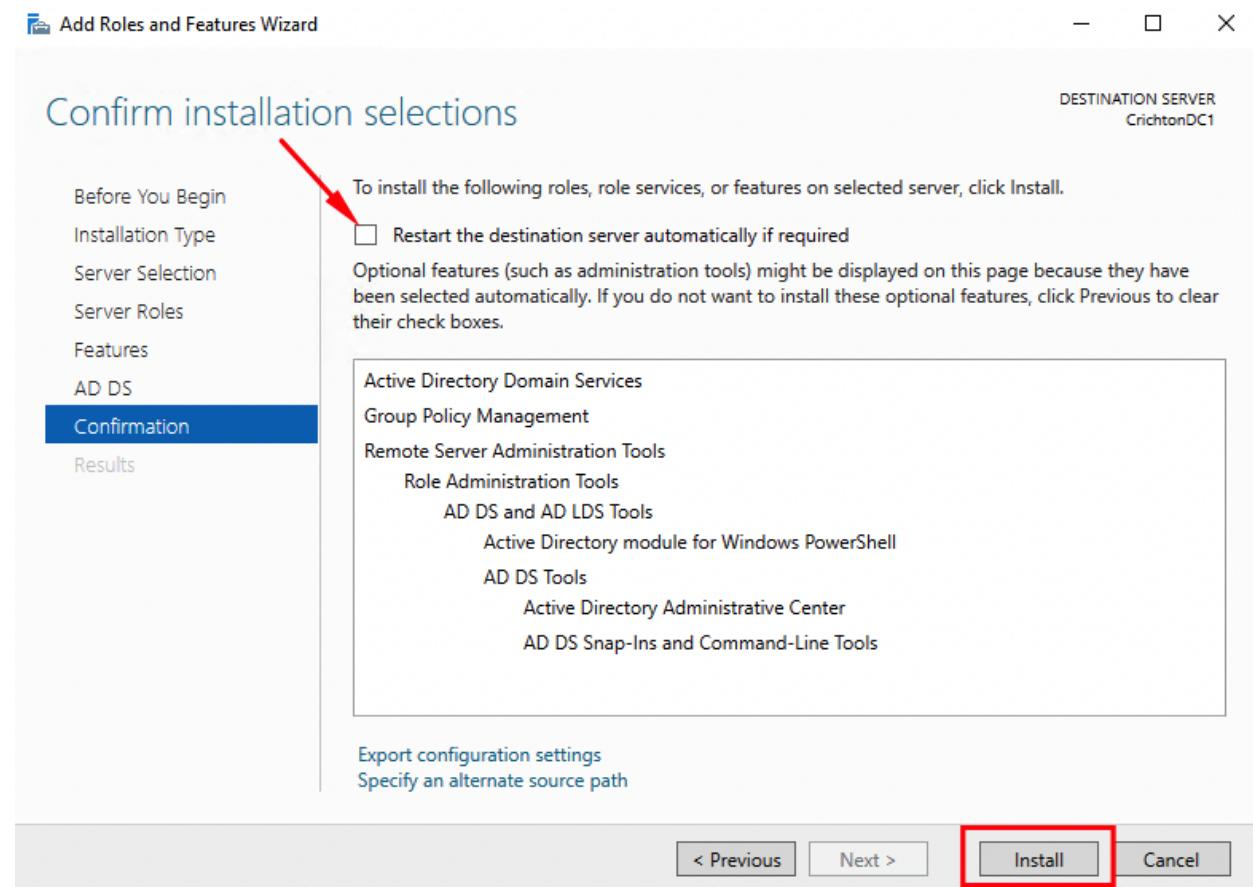
---

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.  
[Learn more about Azure Active Directory](#)  
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous **Next >** Install Cancel

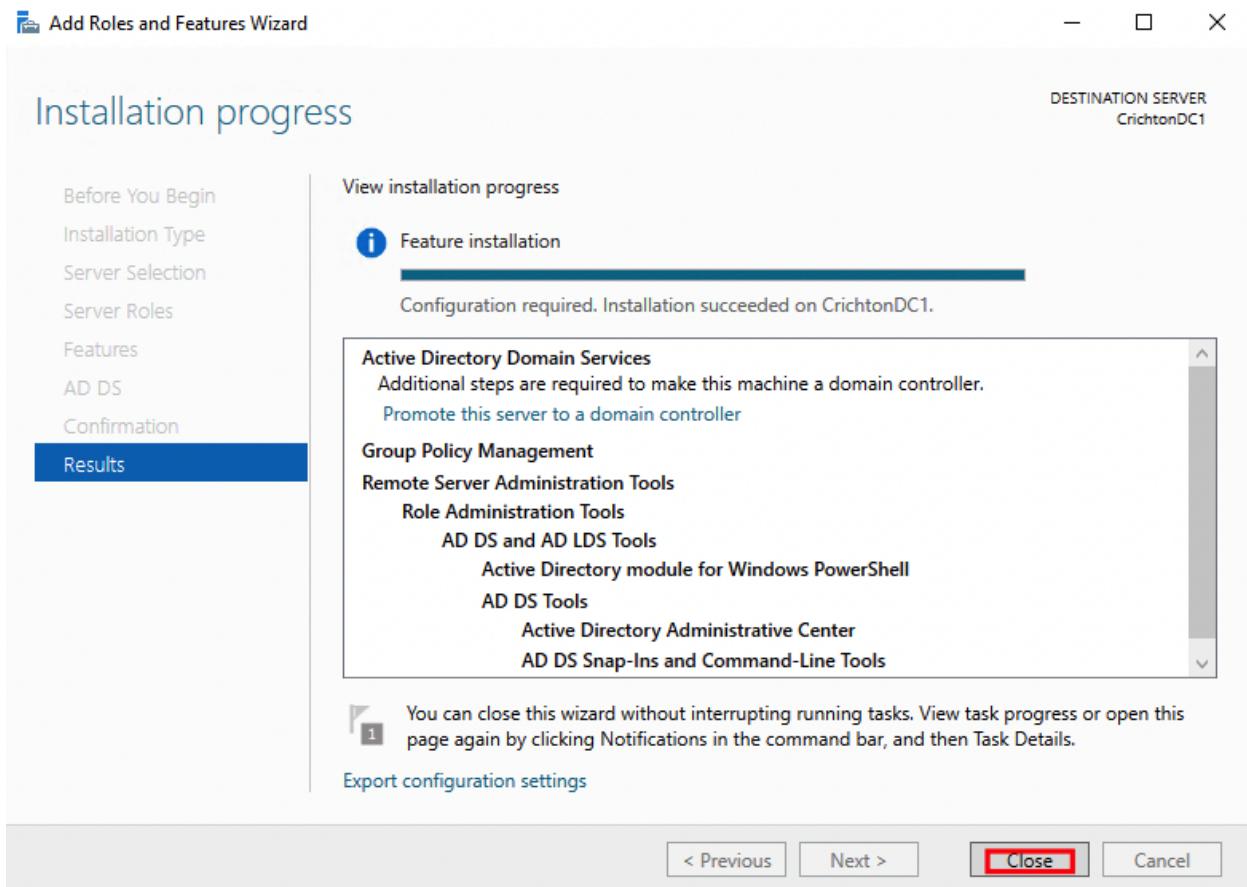
# Active Directory & DNS

Leave the box **unchecked** and click **Install**.



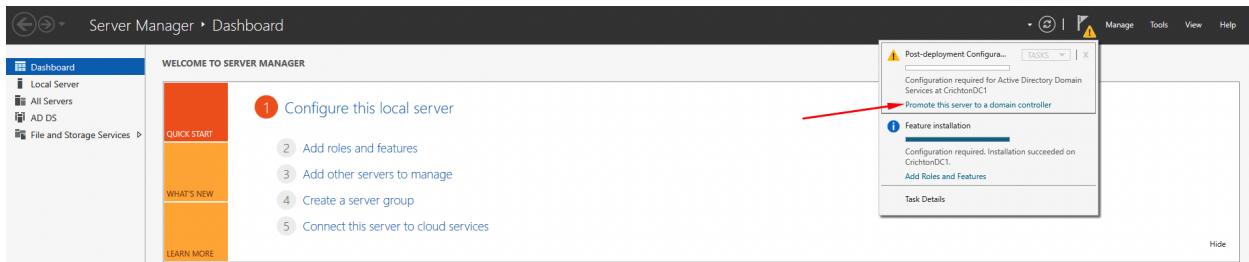
# Active Directory & DNS

After the installation has completed, click **Close**.



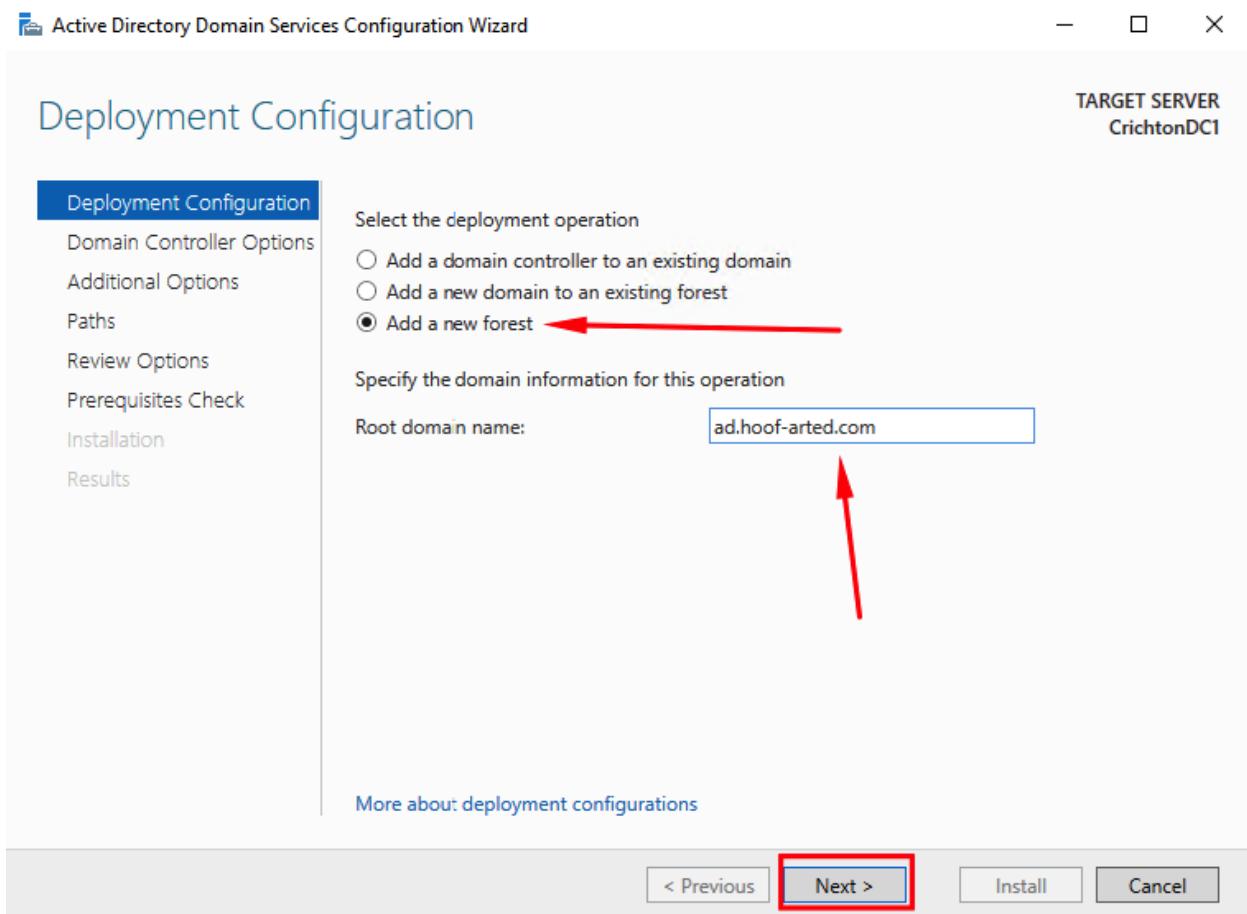
# Active Directory & DNS

Click the **Flag with the Caution Symbol** in the top right of server manager. Then click on the link that says **Promote this server to a domain controller**.



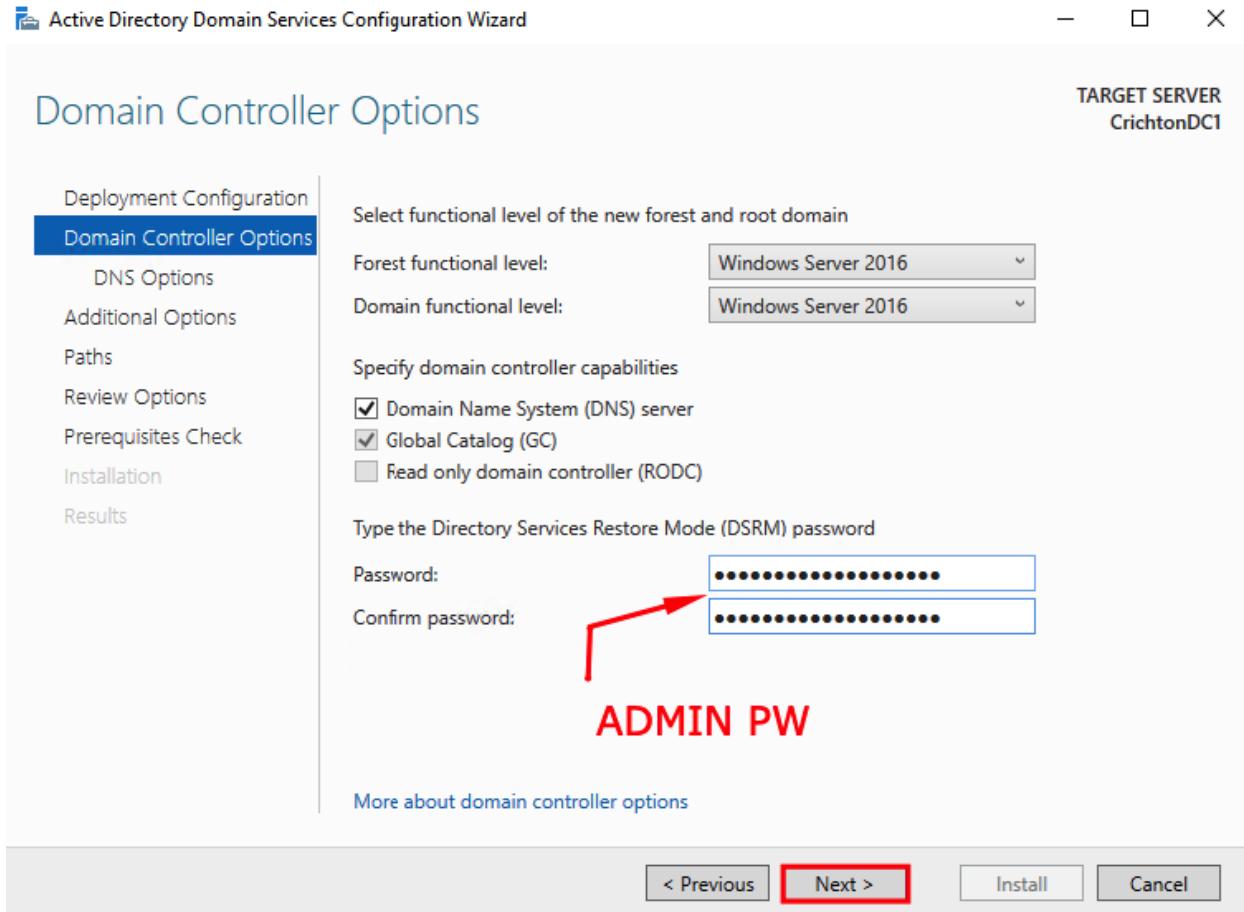
## Active Directory & DNS

Under **Deployment Configuration**, fill the bubble in next to **Add a new forest**. Then for the root domain name, enter your fully qualified domain name, preceded by **ad.** before the domain as shown below. Then click **Next**.



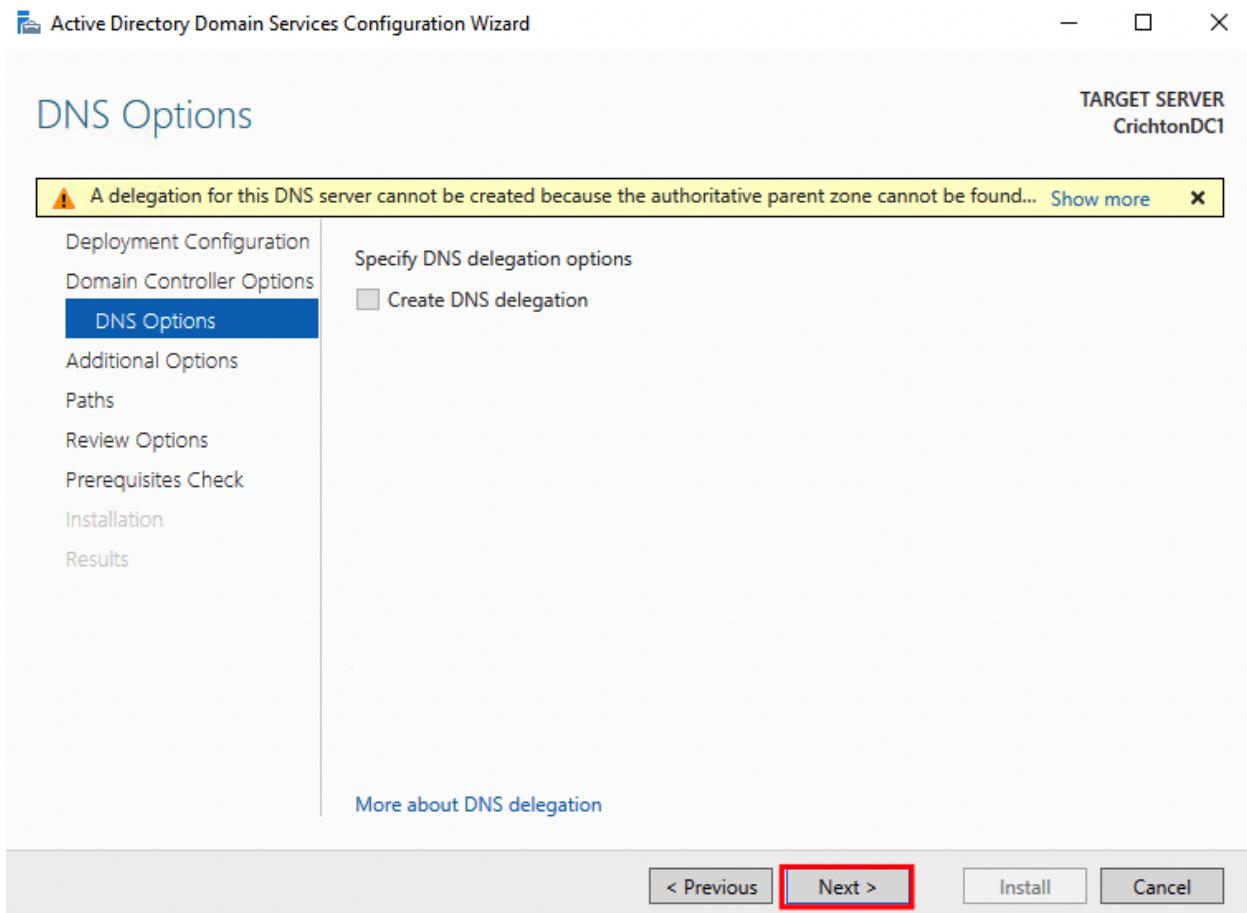
## Active Directory & DNS

We are going to leave the **function level of the new forest and the root domain as Windows Server 2016**. Then enter your **ADMIN password** into the **Directory Services Restore Mode (DSRM) password**. Then click **Next**



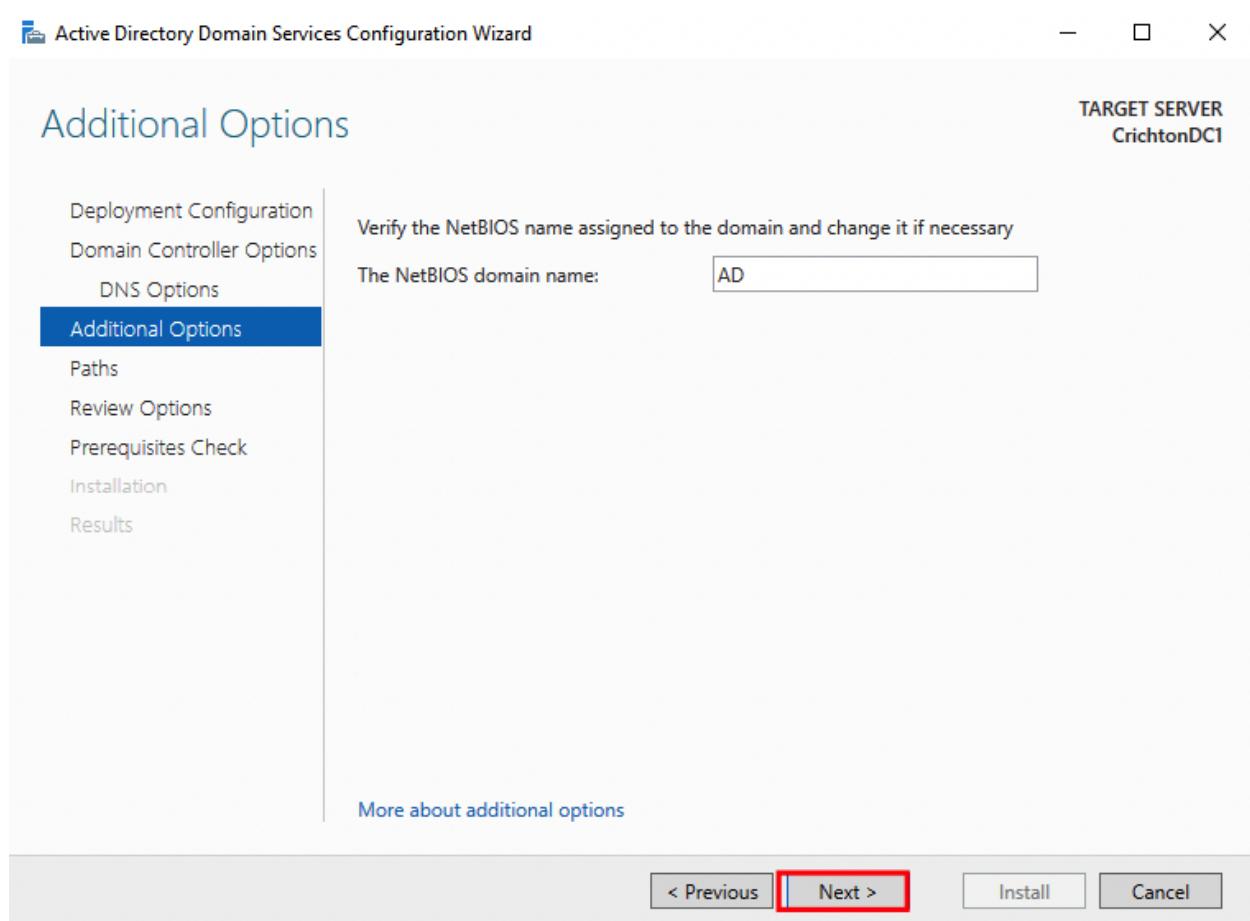
# Active Directory & DNS

Click **Next**.



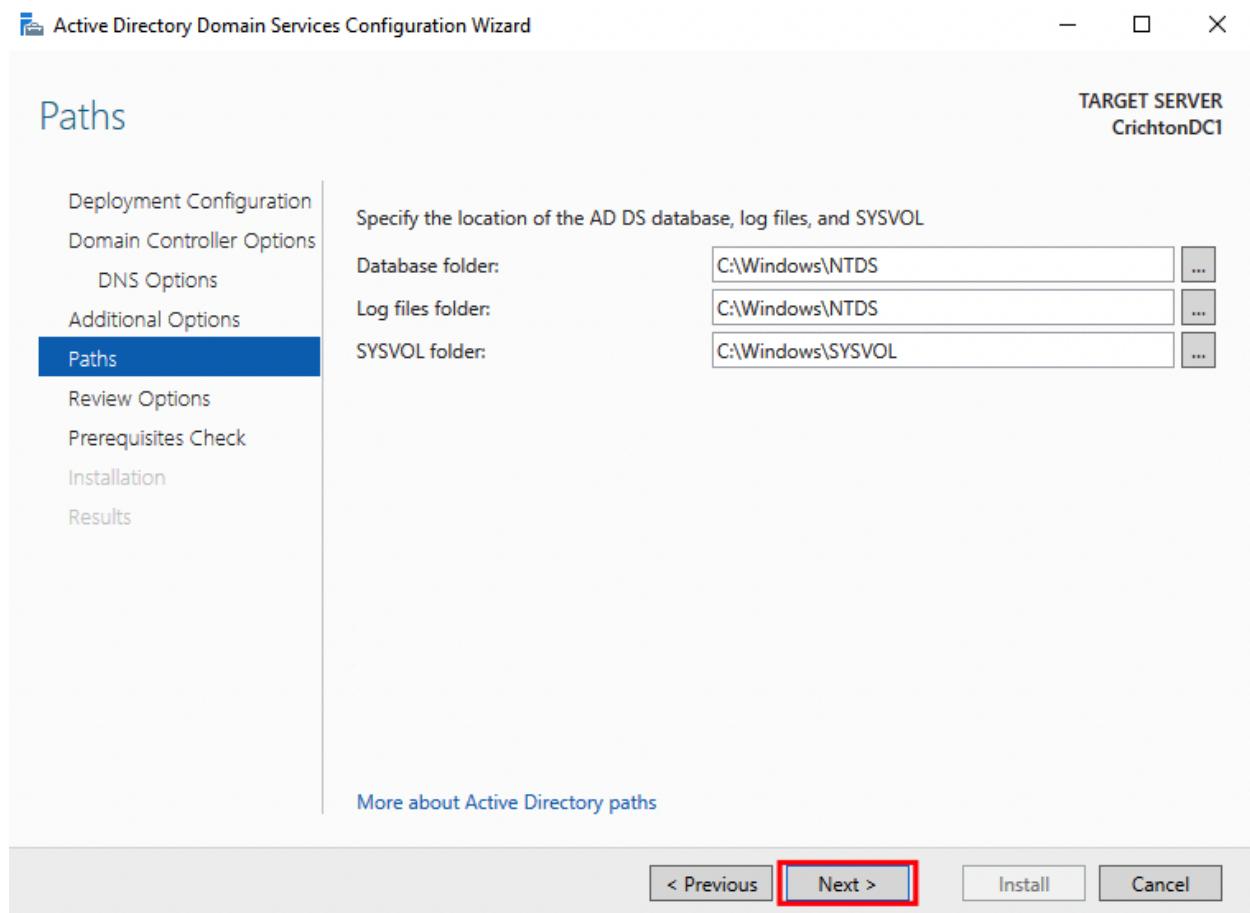
# Active Directory & DNS

Click **Next**



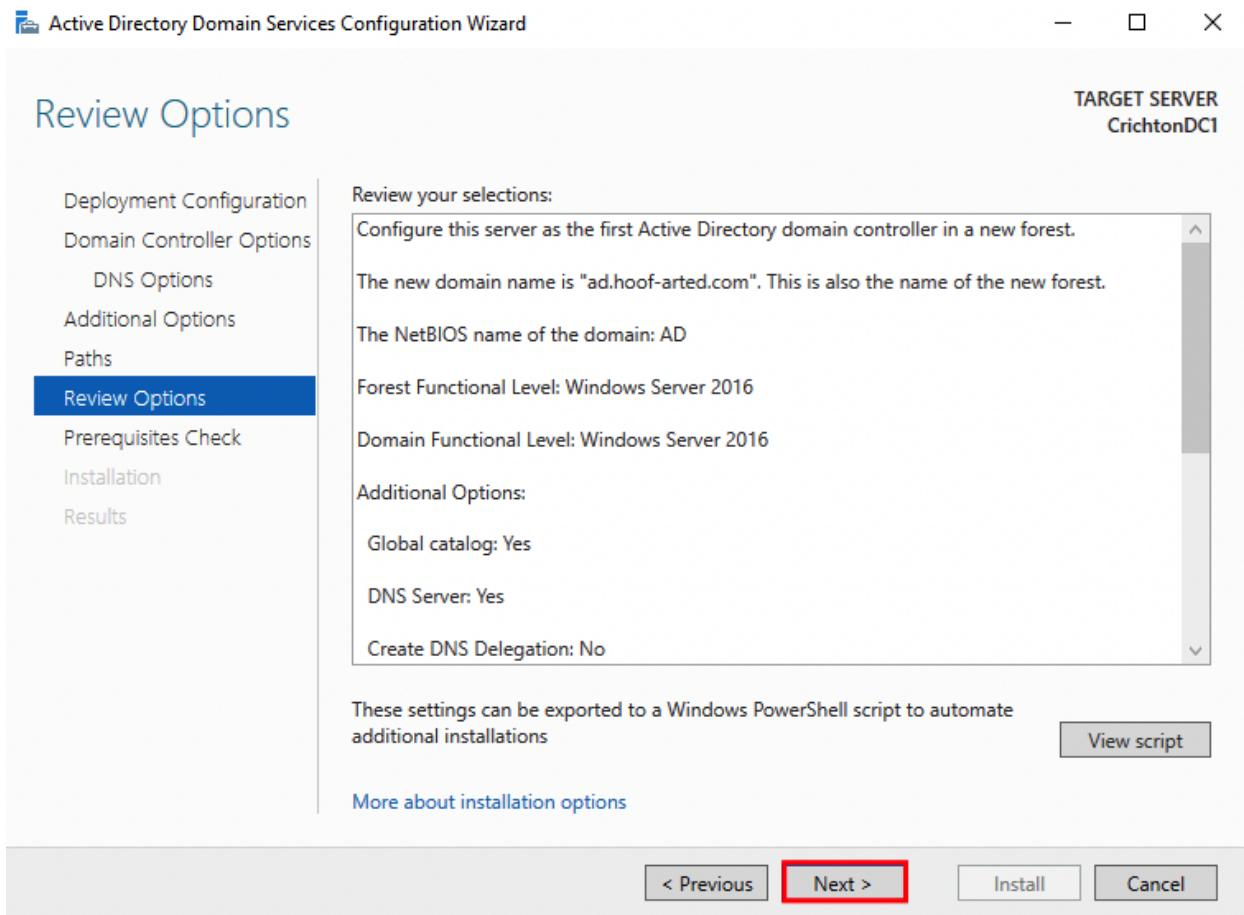
## Active Directory & DNS

Select the file path of the location of the **AD DS database, log files, and SYSVOL** if you desire, but you can leave them as default if you prefer. Then click **Next**.



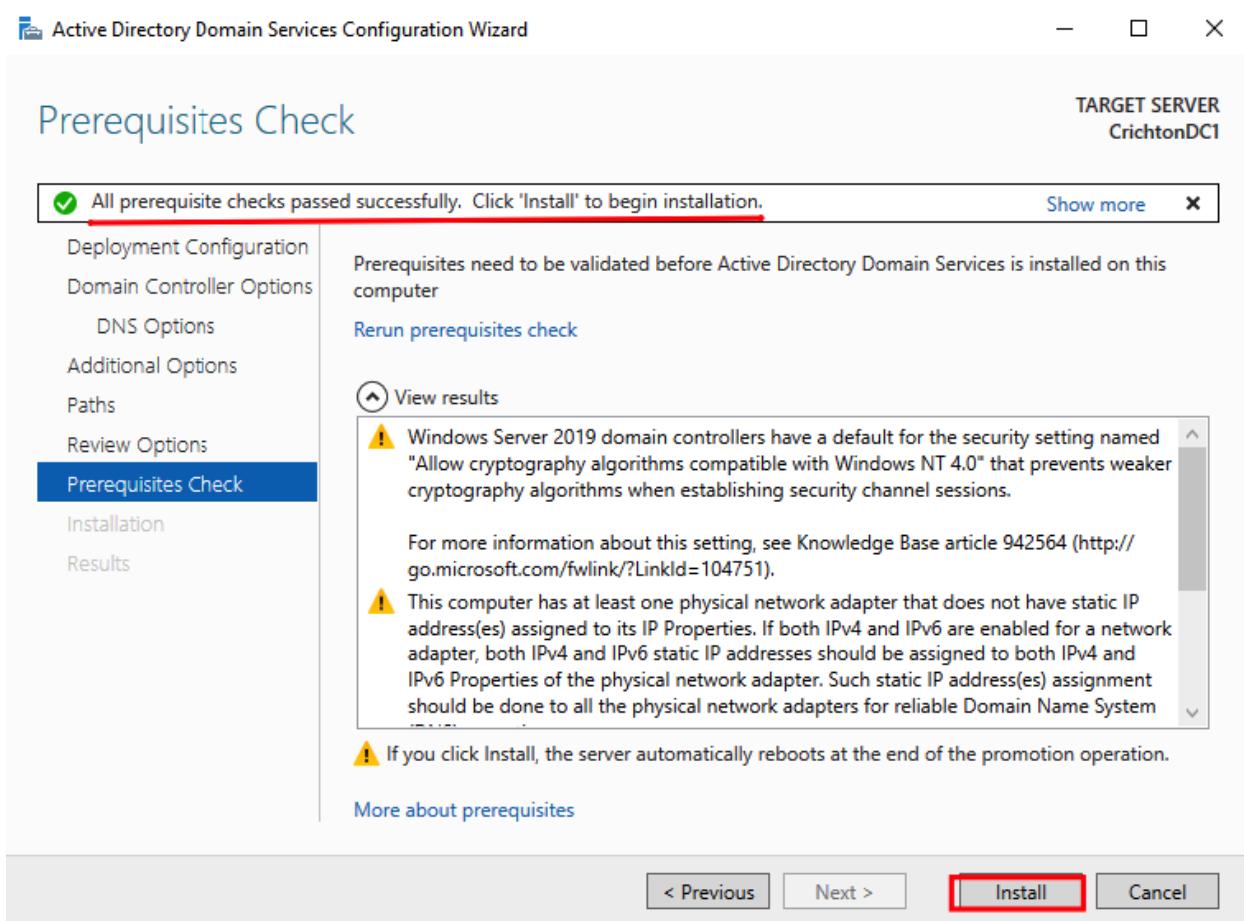
# Active Directory & DNS

Review your selections, ensure that your configurations are set properly, then click **Next**.



# Active Directory & DNS

Ensure that the prerequisites pass the check successfully. Then click **Install**.



**The VM will reboot after everything is installed. Give it some time to refresh and reconnect to it via RDP.**

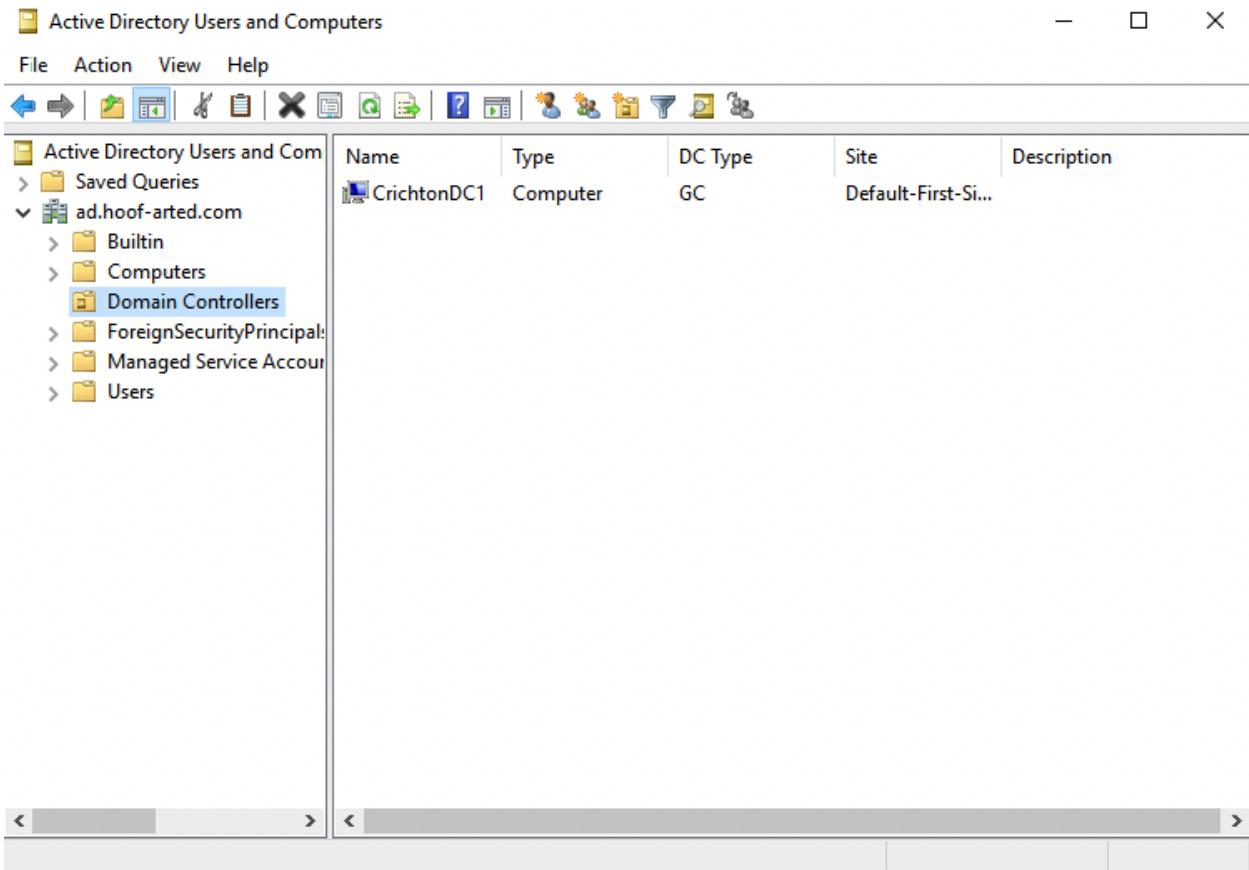
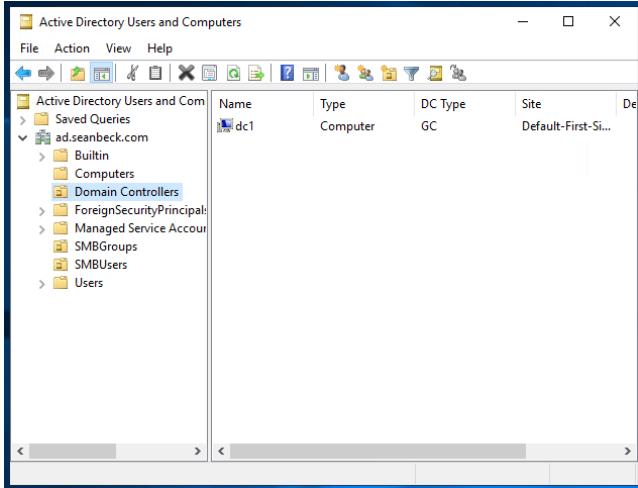
## **Active Directory & DNS**

8. (5 points) Was Microsoft DNS installed as a role during the process of adding the AD DS role? If so, what purpose does it serve?

Microsoft DNS was installed as a role during the process of adding the AD DS role. One of the main purposes is that it uses DNS to make it possible for clients to locate domain controllers and for the domain controllers that host the directory service to communicate with each other. It also allows you to use features such as Active Directory-Integrated DNS zones, which make it easier for you to deploy DNS by eliminating the need to set up secondary zones, and then configure zone transfers.

## Active Directory & DNS

9. (5 points) Once the AD DS role has been installed and configured open “Active Directory Users and Groups” click on the Domain Controllers OU and provide a screenshot similar to the one below.



## Active Directory & DNS

10. (15 points) From “Active Directory Users and Groups” you will create the following AD objects:

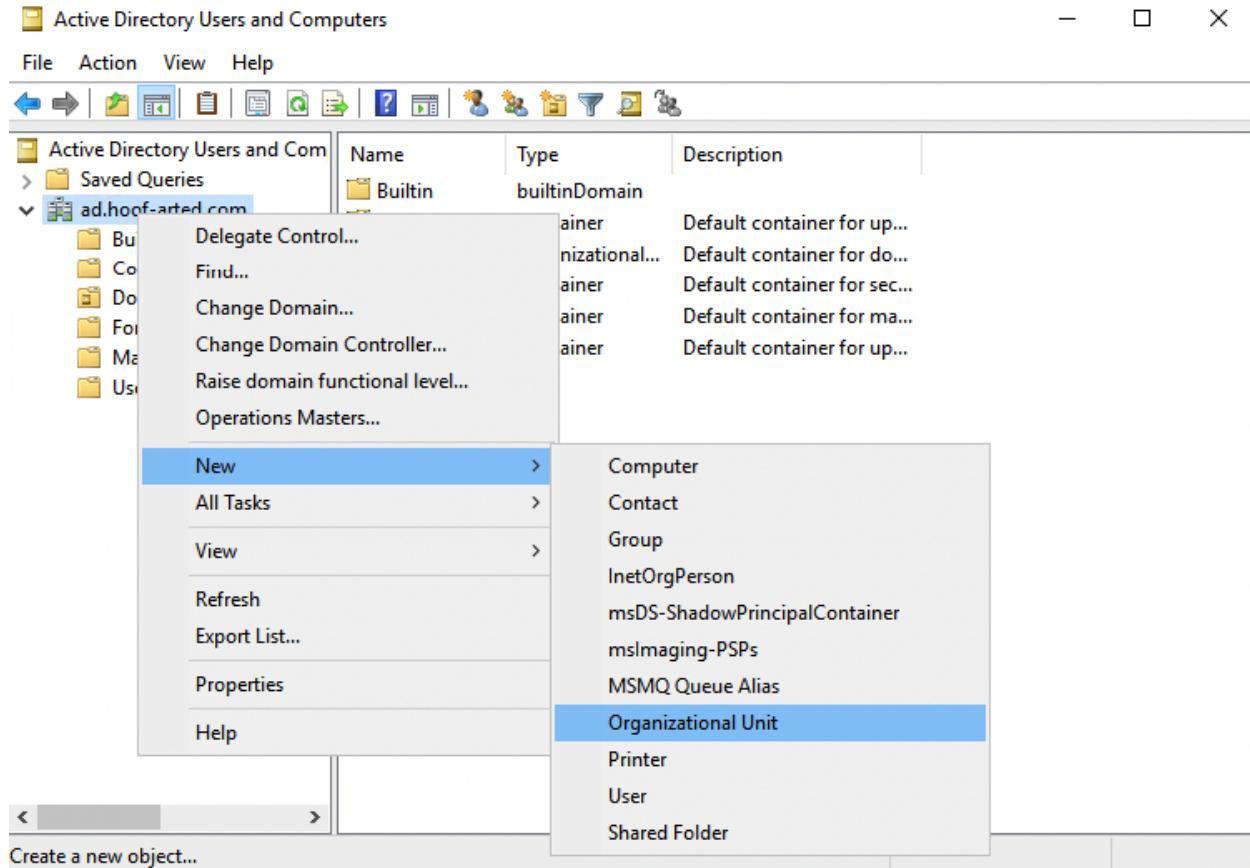
- Create the following OUs
  - xUsers
  - xGroups

\*x can be used or you can use your own prefix
- Create the following users within the xUsers OU (Hint: Remember the passwords you set)
  - Luke Skywalker
  - Leia Skywalker
  - Han Solo
  - Lando Calrissian
  - Your Name (ie. Sean Beck)
    - Assign your user to the Domain Admins group
- Create the following security groups within the xGroups OU and assign the users to the appropriate group
  - Senior Leadership
    - Assign the following users to this group:
      - Luke Skywalker
      - Leia Skywalker
      - Your User
  - Procurement
    - Assign the following users to this group:
      - Han Solo
  - Entertainment
    - Assign the following users to this group:
      - Lando Calrissian

Provide screenshot(s) showing the members of the groups created above. Also, provide a screenshot showing the Domain Admins.

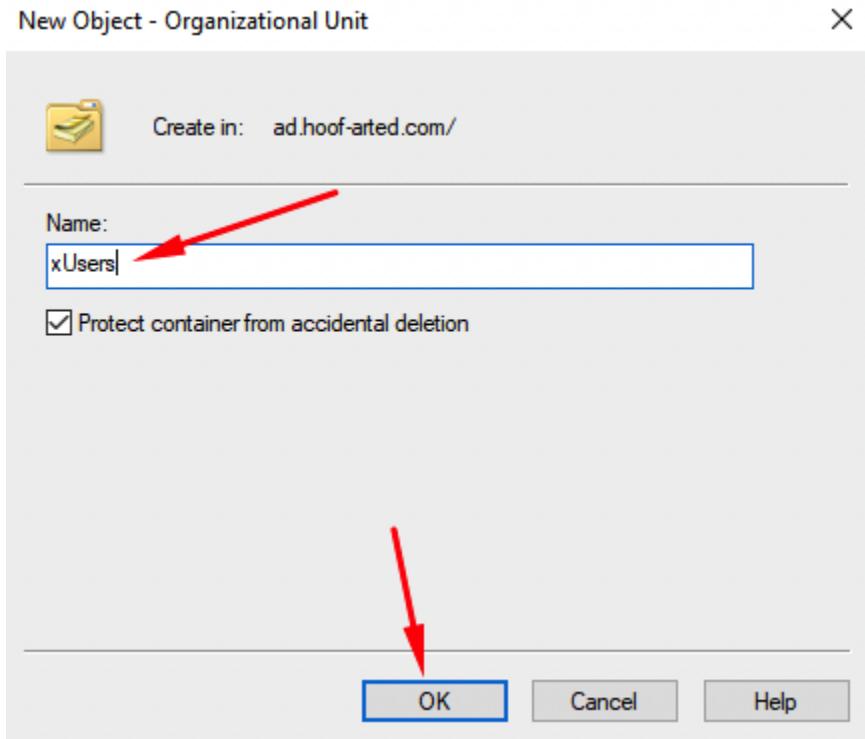
# Active Directory & DNS

Navigate to **Active Directory Users and Computers**, right click on your domain, click **New**, then click **Organizational Unit**.



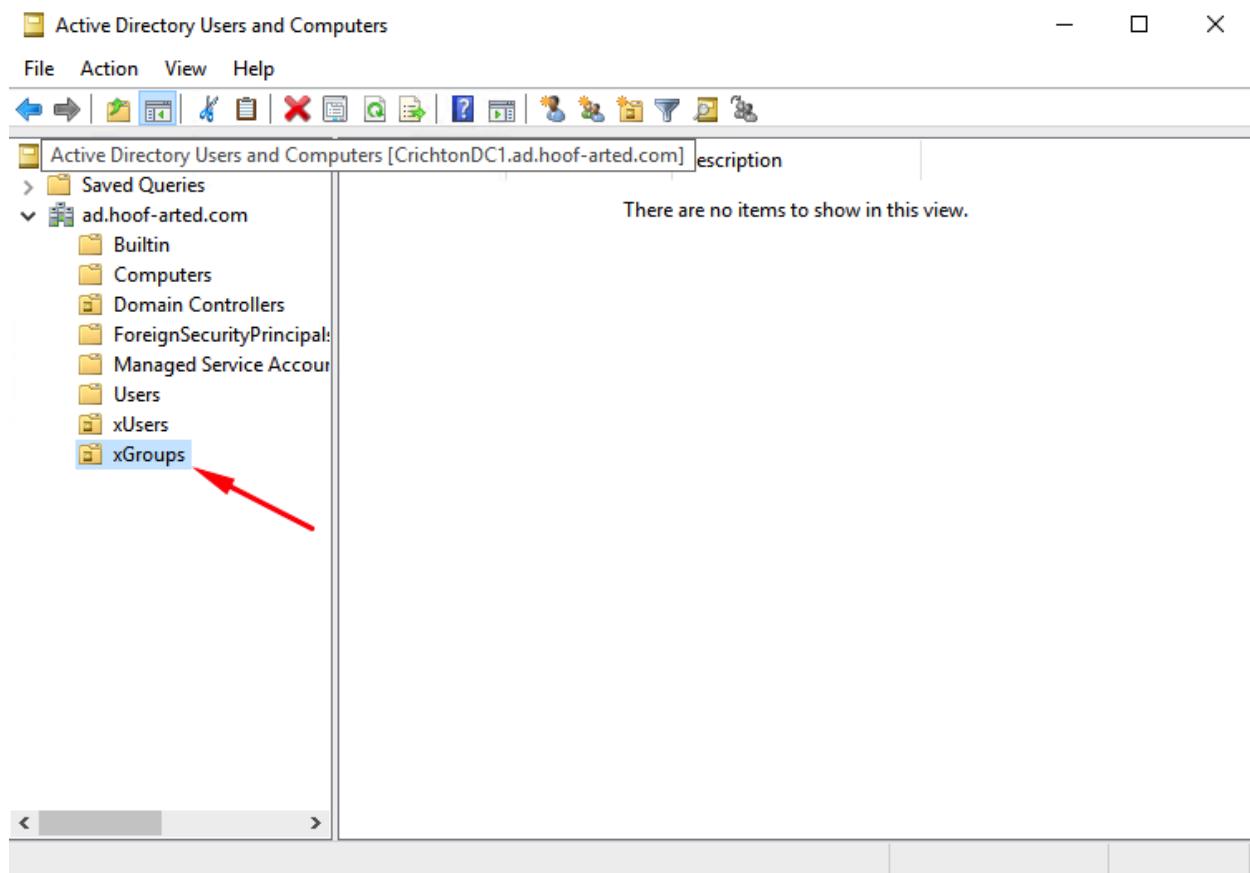
## Active Directory & DNS

Enter the name of the group that you want to create, then click **OK**.



## Active Directory & DNS

This screenshot shows that the xGroups was created as well.



## Active Directory & DNS

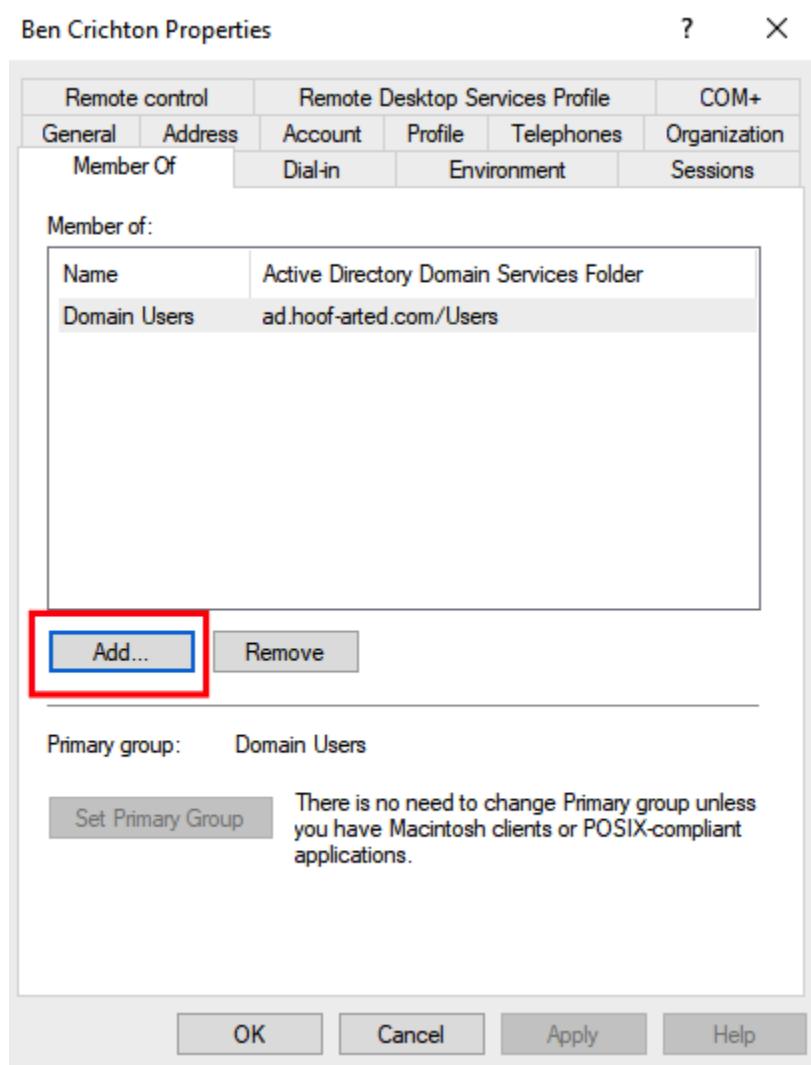
This screenshot shows that all of the Users were created and added to the xUsers group.

The screenshot displays the Windows Active Directory Users and Computers management console. The left pane shows a tree view of the directory structure under 'ad.hoof-arted.com'. The 'xUsers' folder is selected and highlighted in grey. The right pane is a table listing users:

Name	Type	Description
Luke Skywalker	User	
Leia Skywalker	User	
Han Solo	User	
Lando Calrissian	User	
Ben Crichton	User	

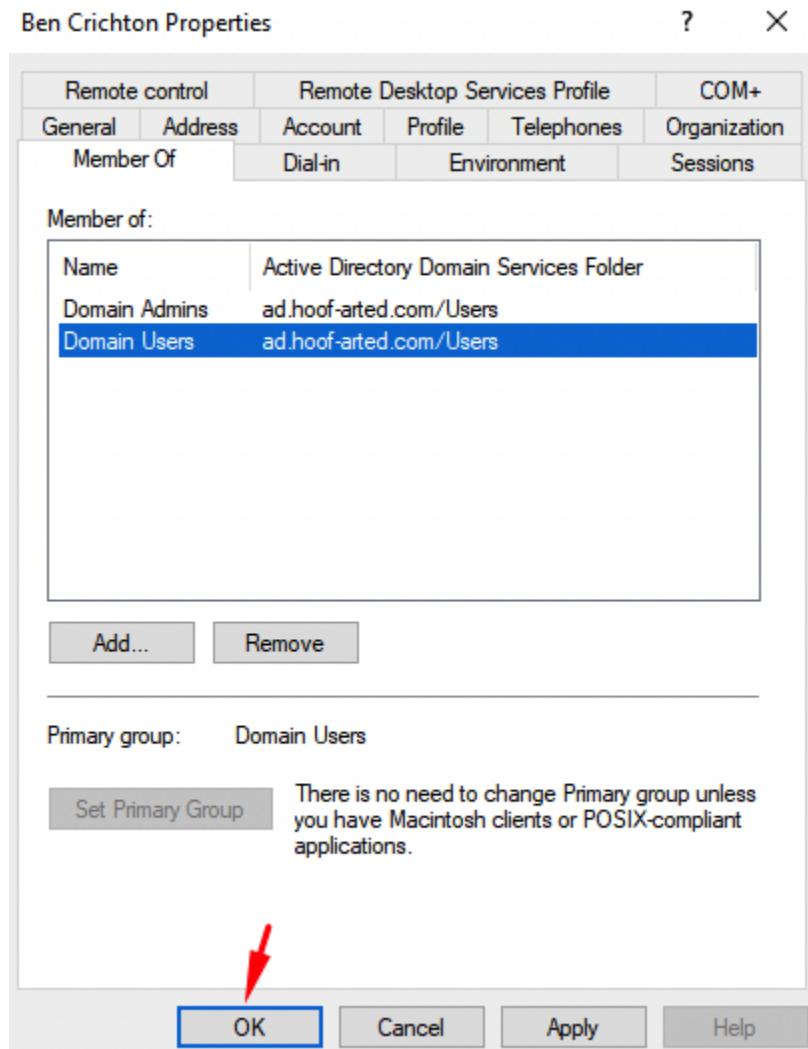
## Active Directory & DNS

To add a user to domain admins, double click on their user profile in Active Directory, then click **Member Of**, and then click **Add**.



## Active Directory & DNS

Type in **Domain Admins**, click **Check Names**, and then click **OK**, you will notice that **Domain Admins** has been added to what this user is a member of.



## Active Directory & DNS

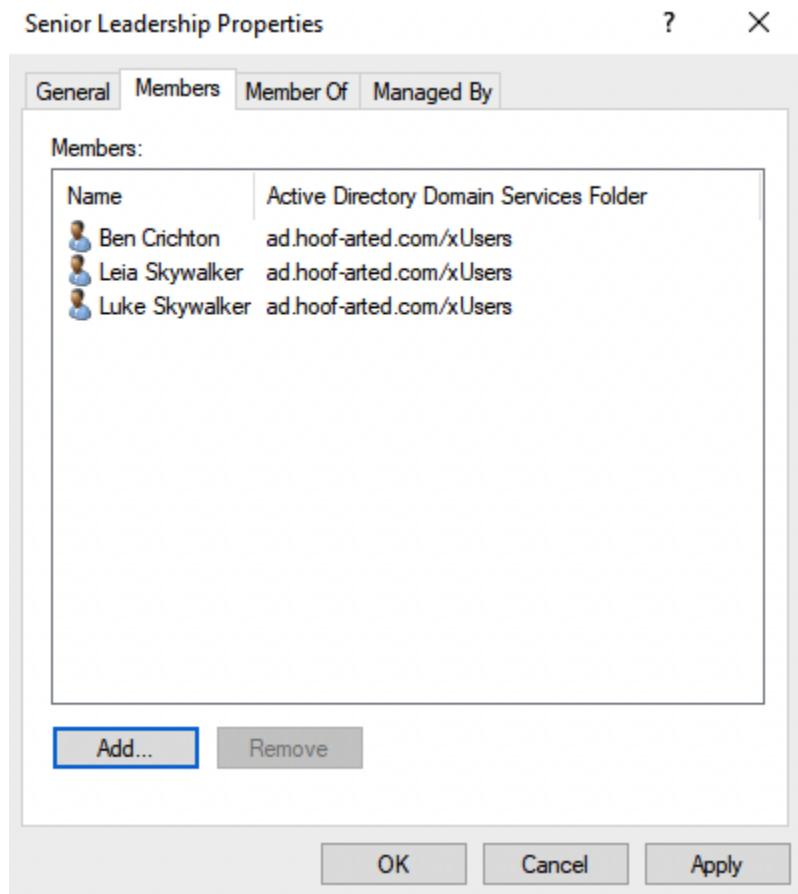
This screenshot shows the xGroups that were created.

The screenshot displays the Windows Active Directory Users and Computers management console. The left pane shows a tree view of the directory structure under 'ad.hoof-arted.com'. The 'xGroups' folder is selected. The right pane is a table listing three security groups:

Name	Type	Description
Entertainment	Security Group...	
Procurement	Security Group...	
Senior Leadership	Security Group...	

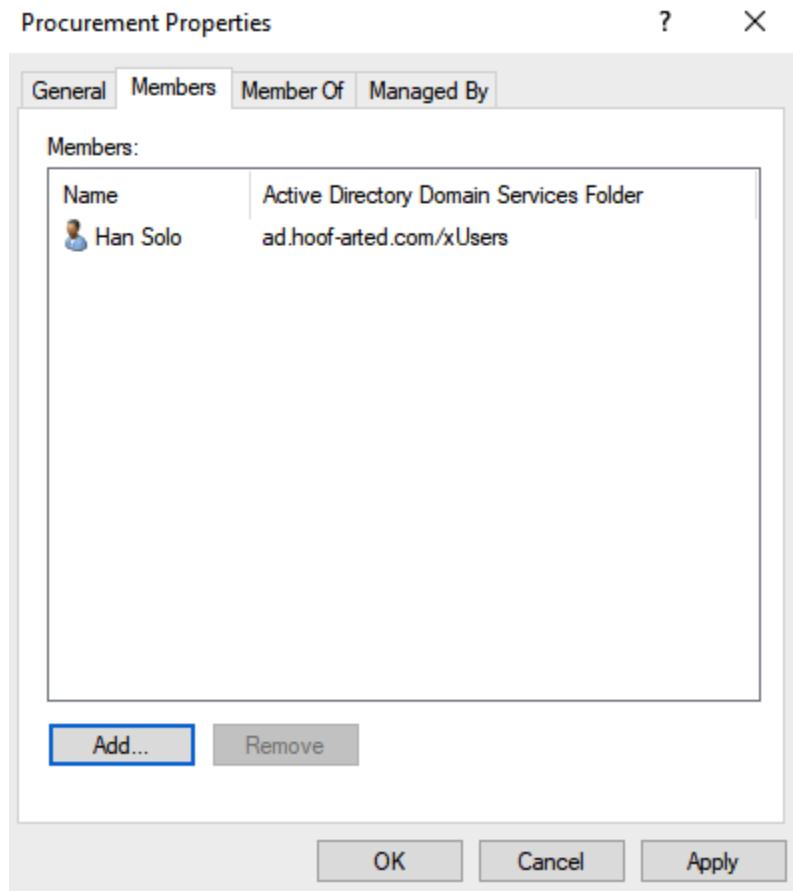
## Active Directory & DNS

This screenshot shows the users that have been added to the Senior Leadership Group.



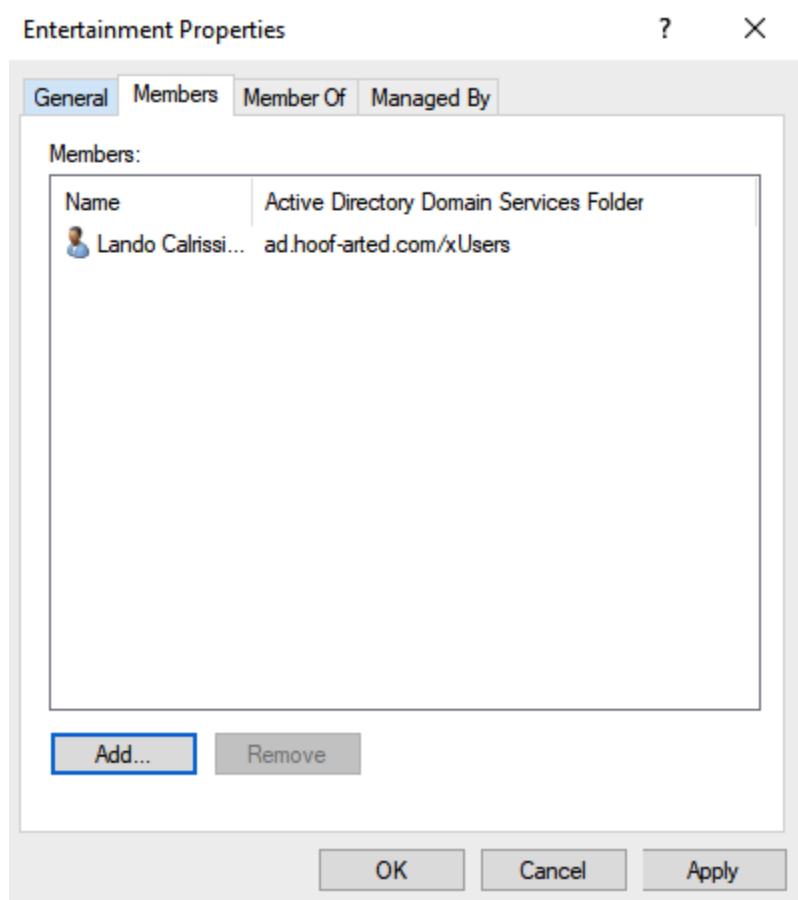
# Active Directory & DNS

Screenshot of the Procurement Group



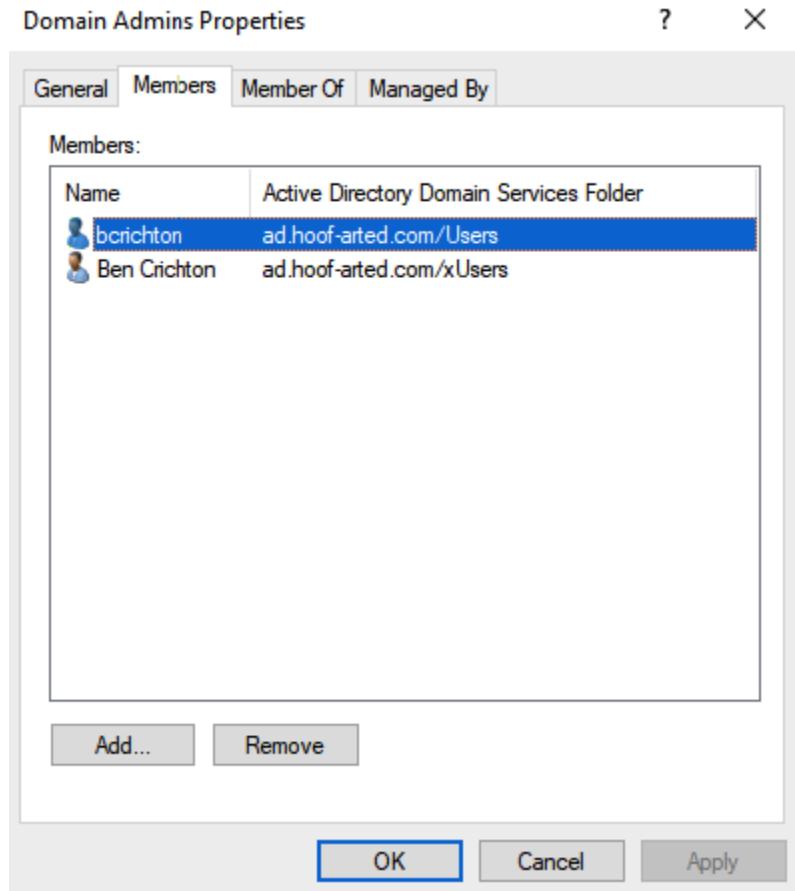
# Active Directory & DNS

Screenshot of the Entertainment Group



# Active Directory & DNS

Screenshot showing I have made myself a Domain Admin



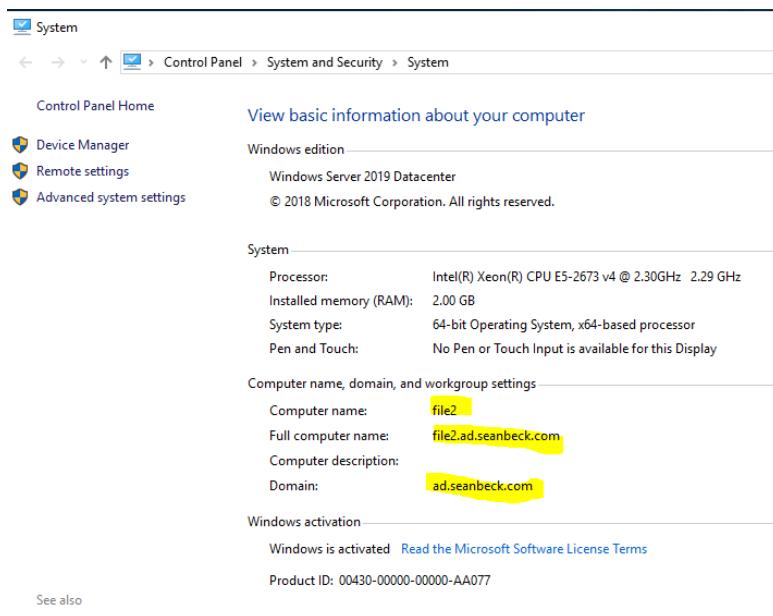
## Active Directory & DNS

11. (10 points) Use the Remote Desktop Protocol (RDP) to connect to your Fileserver VM, as you will join this Windows 2019 server to the domain you created. (Hint: Before you can join the fileserver to the domain you must set the Primary DNS server to the IP of your DC).

Using the following article to assist you in joining the server to the domain:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain>

Provide a screenshot showing your file server is now part of the domain, similar to the one shown below:



Provide a screenshot from Active Directory Users and Computers showing the file server object similar to the one shown below:

# Active Directory & DNS

The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the directory structure under 'ad.seanbeck.com'. The right pane is a table with three columns: 'Name', 'Type', and 'Description'. A single entry, 'file2', is listed under the 'Computers' type. The table has a header row with these column names.

Name	Type	Description
file2	Computer	

The screenshot shows the Windows Control Panel System settings page. At the top, it displays the Windows edition as 'Windows Server 2019 Datacenter'. Below this, there are sections for 'System' (processor: Intel(R) Xeon(R) Platinum 8370C CPU @ 2.80GHz 2.79 GHz, RAM: 2.00 GB, system type: 64-bit Operating System, x64-based processor), 'Computer name, domain, and workgroup settings' (computer name: CrichtonFile1, full computer name: CrichtonFile1.ad.hoof-arted.com, domain: ad.hoof-arted.com), and 'Windows activation' (Windows is activated, Read the Microsoft Software License Terms). At the bottom, there are links for 'See also' and 'Security and Maintenance'.

## Active Directory & DNS

Active Directory Users and Computers

File Action View Help

Back Forward Home Copy Paste Find Filter Refresh

Active Directory Users and Computers  
Saved Queries  
ad.hoof-arted.com  
Builtin  
Computers  
Domain Controllers  
ForeignSecurityPrincipal:  
Managed Service Account  
Users  
xGroups  
xUsers

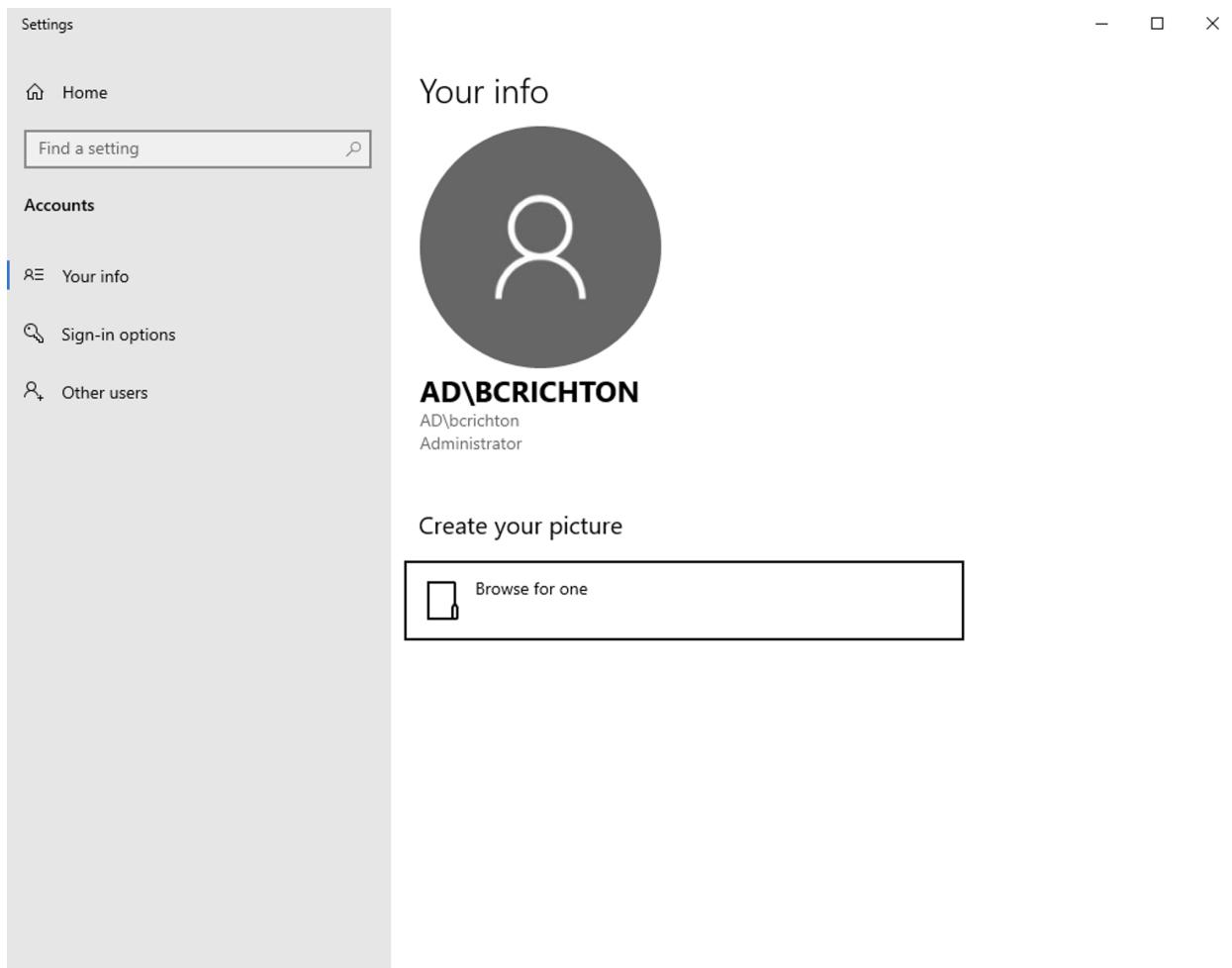
Name	Type	Description
CrichtonFile1	Computer	

## Active Directory & DNS

12. (10 points) Now that your Fileserver is joined to the domain you can use AD users to connect to the server via RDP. Using your AD user (ie. Sean Beck) RDP to LastnameFile1. Were you able to successfully RDP? If so signout / logoff as your user and try to RDP to LastnameFile1 using the Han Solo user. Why can you not successfully RDP with the user Han Solo? How do you grant Han Solo to the ability to RDP to any server joined to the domain? Apply the fix / update to the Han Solo user so he has the ability to RDP to servers joined to the domain.

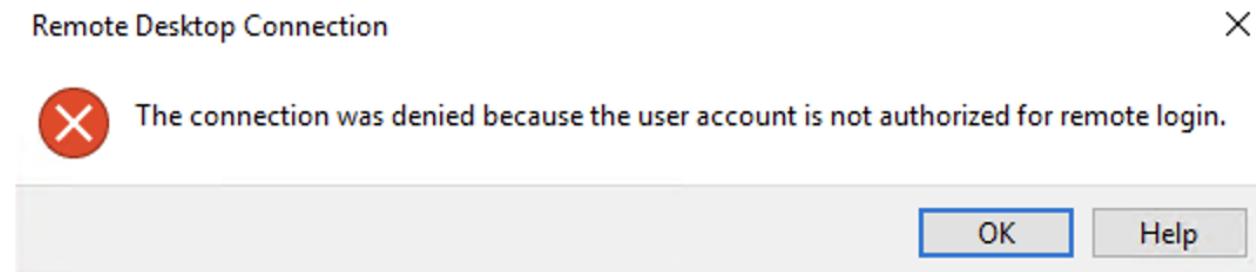
Provide screenshot(s) supporting your answers.

I was able to sign into the server and RDP to CrichtonFile1 with my AD user account.



## Active Directory & DNS

For the Han Solo account, it would not let me RDP due to the following error:



In order to give Han Solo access to Remote Desktop, go to **Active Directory Users and Computers >> Domain >> Builtin >> Remote Desktop Users** and add the user or group that you want to be able to remote desktop. **Be sure to set this in both the Domain Controller, as well as the file server.**

Active Directory Users and Computers

Name      Type      Description

Name	Type	Description
Guests	Security Group...	Guests have the same ac...
Hyper-V Administrators	Security Group...	Members of this group ...
IIS_IUSRS	Security Group...	Built-in group used by I...
Incoming Forest Trust Buil...	Security Group...	Members of this group ...
Network Configuration Op...	Security Group...	Members in this group c...
Performance Log Users	Security Group...	Members of this group ...
Performance Monitor Users	Security Group...	Members of this group ...
Pre-Windows 2000 Compa...	Security Group...	A backward compatibilit...
Print Operators	Security Group...	Members can administe...
RDS Endpoint Servers	Security Group...	Servers in this group run...
RDS Management Servers	Security Group...	Servers in this group can...
RDS Remote Access Servers	Security Group...	Servers in this group ena...
Remote Desktop Users	Security Group...	Members in this group a...
Remote Management Users	Security Group...	Members of this group ...
Replicator	Security Group...	Supports file replication ...
Server Operators	Security Group...	Members can administe...
Storage Replica Administr...	Security Group...	Members of this group ...
Terminal Server License Se...	Security Group...	Members of this group ...
Users	Security Group...	Users are prevented fro...
Windows Authorization Ac...	Security Group...	Members of this group ...

## Active Directory & DNS

Add to the Remote Desktop Users Properties

### Remote Desktop Users Properties



General

Members

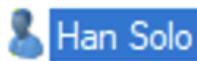
Member Of

Managed By

Members:

Name

Active Directory Domain Services Folder



ad.hoof-arted.com/xUsers

Add...

Remove

OK

Cancel

Apply

## Active Directory & DNS

13. (5 points) When completed with this assignment power-off all the VMs. Provide a screenshot showing this is completed.

**We will use these VMs for future assignments, so you do not need to delete / destroy them.  
However, if you do not power-off the VMs you will use all your cloud credits.**

<input type="checkbox"/> Name ↑↓	Type ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	Status ↑↓	Operating system ↑↓	Size ↑↓	Public IP address ↑↓	Disk
<input type="checkbox"/> CrichtonBastionHost	Virtual machine	Azure for Students	CrichtonDevVMs	East US	Stopped (deallocated)	Windows	Standard_B1s	20.84.61.223	1
<input type="checkbox"/> CrichtonDC1	Virtual machine	Azure for Students	CRICHTONDEVVMSS	East US	Stopped (deallocated)	Windows	Standard_B2s	-	1
<input type="checkbox"/> CrichtonFile1	Virtual machine	Azure for Students	CrichtonDevVMs	East US	Stopped (deallocated)	Windows	Standard_B1ms	-	1