

# Intro To SysAdmin



Jade Falcon LLC.

Domain Controllers  
Version:  
20200704

**Table of Contents:**

Table of Contents:..... 2

Copyright Information:..... 3

Prerequisites and Preface:..... 3

First Domain Controller in the Forest:..... 4

Active Directory Sites and Services:..... 10

Adding a DC to the Domain:..... 17

Creating a Child Domain:..... 20

DC NIC Settings:..... 22

DNS Forwarders:..... 22

DHCP:..... 25

Policy Store:..... 38

Basic Group Policy:..... 39

Flexible Single Master Operation (FSMO) Roles:..... 42

User Principle Name (UPN) Suffix:..... 49

DNS Aging and Scavenging:..... 51

Public Key Infrastructure (PKI) Script:..... 52

Active Directory Tombstone:..... 55

Distributed File System Replication (DFSR) and the SYSVOL:.... 56

Active Directory Recycle Bin:..... 57

Time:..... 58

Preventing Standard Users from Joining Computers to the Domain:  
..... 63

Replication:..... 64

KDS Root Key and Managed Service Accounts:..... 67

Granting Permissions:..... 69

Basic Troubleshooting and Maintenance:..... 74

SCONFIG:..... 83

Demoting A Domain Controller:..... 84

Backups (Never, ever, ever, use snapshots.):..... 88



## Copyright Information:

- This work is the intellectual property of Jade Falcon LLC (JFLLC).
- Reproducing this without permission from Jade Falcon LLC is not authorized.
- If you received an illegal copy, please purchase a legitimate copy. We tried not to break the bank on prices..
- Knowledge is meant to be shared. If you benefited from this, please consider purchasing a copy.

## Prerequisites and Preface:

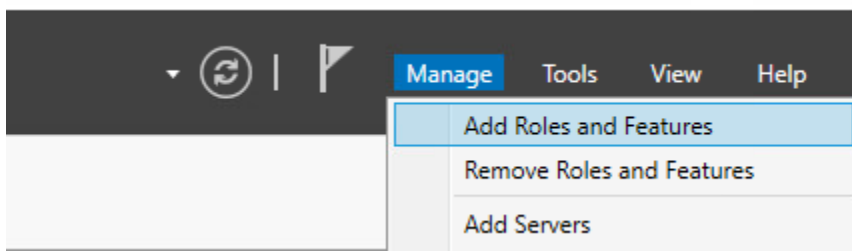
- Deploy Server 2016.
- Configure the server name.
- Configure the IP information, for the first server, DNS is 127.0.0.1. All other servers will point to the IP of the first server.
- Most of the tools such as Active Directory Users and Computers, DNS, etc can be found on the Start menu under Windows Administrative Tools, or on the Server Manager under the Tools menu.
- This is about Domain Controllers and assumes a limited knowledge about how to create a user account, group etc.
- Some of the commands are long. If the lines underneath are indented, it means it is part of the same command, and should all be on one line. IE:
  - Line one of the command.
  - Part of the same command.
  - Still part of the same command.
  - Part of the command line argument above it.
- The pictures follow the text, and may be on the next page.

**Important:** Never change the name or IP address of a Domain Controller once it is promoted.



## First Domain Controller in the Forest:

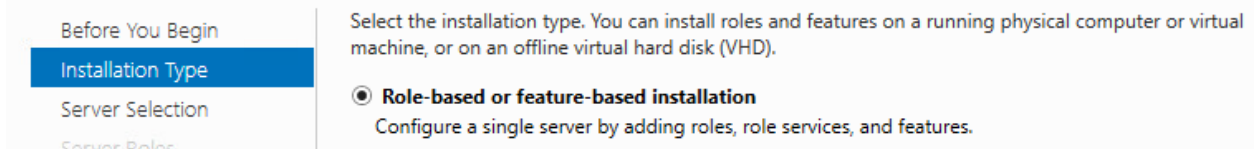
Open Server Manager, Manage, Add Roles and Features



Role-based or feature-based installation.

### Select installation type

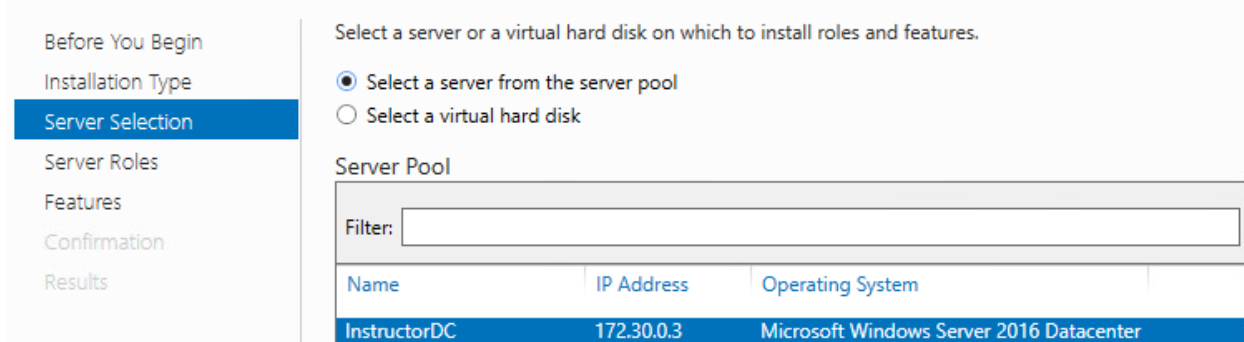
DESTINATION SERVER  
InstructorDC



Select the destination server. Server Manager can be connected to multiple servers and provide you a single location to manage your infrastructure.

### Select destination server

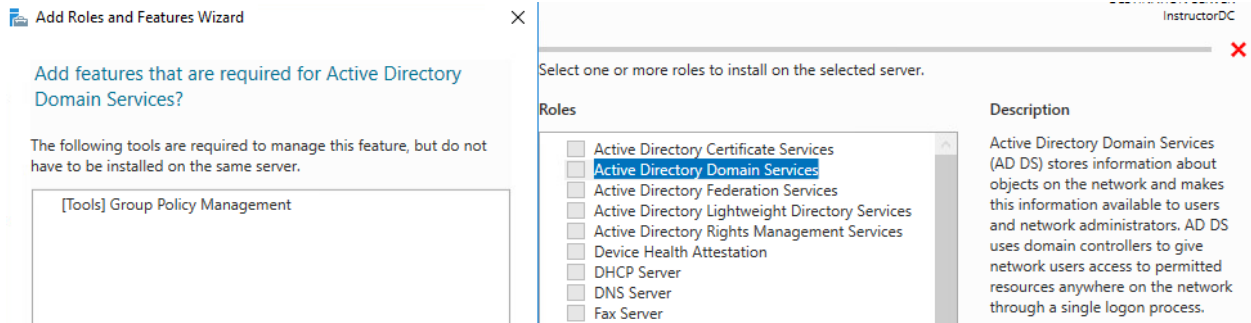
DESTINATION SERVER  
InstructorDC



Check the box next to Active Directory Domain Services (AD DS). Note: A window will pop up asking if you want to add the features required for the role. Unless you have a very specific reason not to, always add the features. Most of the time they are required for the Roles to install.



# Domain Controllers



Click next, and next.

## Active Directory Domain Services

DESTINATION SERVER  
InstructorDC

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

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.

We will let the server automatically add and configure the DNS Server Role when we promote the server to a Domain Controller.

Click install.



Jade Falcon LLC

# Confirm installation selections

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

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

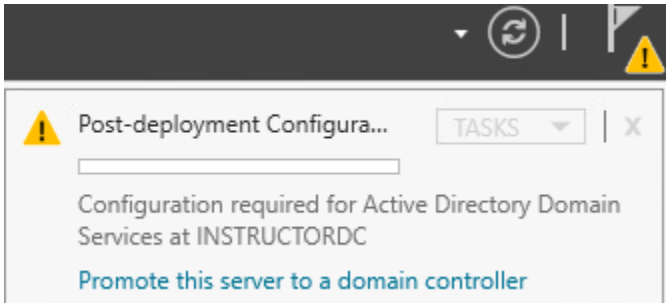
Optional features (such as administration tools) might be displayed on this page because been selected automatically. If you do not want to install these optional features, click Pr their check boxes.

Active Directory Domain Services  
Group Policy Management

[Export configuration settings](#)  
[Specify an alternate source path](#)

< Previous    Next >    Install

It is ok to close the window. When the task finishes, there are two ways to promote the server. If you left the window open, you can click the blue text saying Promote this server to a domain controller. If you closed the window, click on the yellow exclamation mark, and click the Promote this server to a domain controller link.

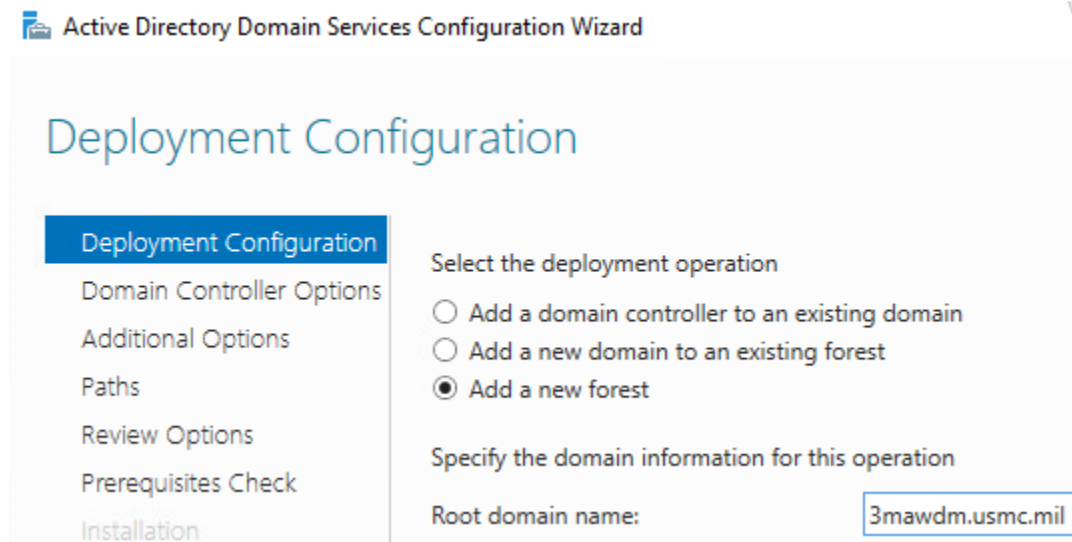


Because this is the first domain controller in our forest, we will be creating a new forest.



## Domain Controllers

Select Add a new forest, specify the domain name, and click next.



Active Directory Domain Services Configuration Wizard

### Deployment Configuration

- Deployment Configuration
- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation

Select the deployment operation

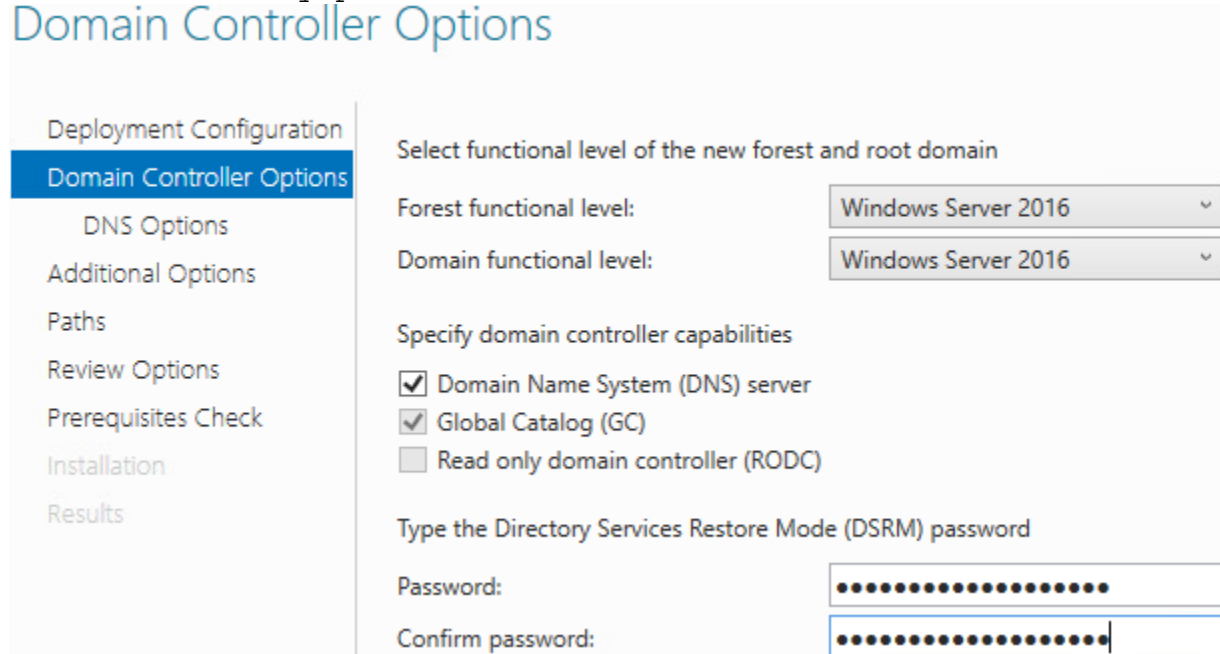
- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

Specify the functional levels for your domain. This is also where we will tell it to automatically install and configure DNS server.

Enter a recovery password and click next.



### Domain Controller Options

- Deployment Configuration
- Domain Controller Options
- DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select functional level of the new forest and root domain

Forest functional level:

Domain functional level:

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:

Do not worry about the DNS delegation.



## Domain Controllers

**⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more X**

Deployment Configuration | Specify DNS delegation options  
Domain Controller Options |  Create DNS delegation  
DNS Options

In our example, the domain name we chose was 3mawdm.usmc.mil. The error means either it could not contact usmc.mil or that the DNS servers for usmc.mil did not authorize the new forest namespace of 3mawdm to exist on the IP address you specified.

The NetBIOS name is typically the name of the domain, and automatically populates.

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

If you wanted to change where AD DS stores its information, you are able to do so here.

Deployment Configuration | Specify the location of the AD DS database, log files, and SYSVOL  
Domain Controller Options | Database folder:   
DNS Options | Log files folder:   
Additional Options | SYSVOL folder:   
Paths

Review your chosen options, then click next.





## Review Options

TARGET SERVER  
InstructorDC

- Deployment Configuration
- Domain Controller Options
  - DNS Options
  - Additional Options
  - Paths
  - Review Options**
  - Prerequisites Check
- Installation
- Results

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "3mawdm.usmc.mil". This is also the name of the new forest.

The NetBIOS name of the domain: 3MAWDM

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

View script

[More about installation options](#)

< Previous

Next >

Install

Cancel

The prerequisites check may have some warnings depending on your server baseline. Click install.

## Prerequisites Check

✔ All prerequisite checks passed successfully. Click 'Install' to begin installation.

The installation will take a few minutes. It will display the step it is on throughout the process. When it finishes, the server will restart and is successfully promoted to a domain controller.

Adding additional domain controllers to a domain is almost the exact same as above, except you join the server to the domain before you promote it. Normally, each site should have at least two domain controllers.

**Extra:** For this lesson, we will be putting a single domain controller in three separate sites. This will be covered after we establish the additional sites.

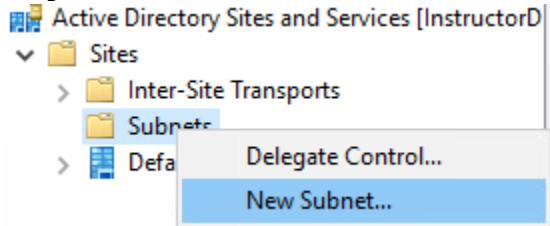


## Active Directory Sites and Services:

Active Directory Sites and Services assist the machines with locating the services your domain provides based on their subnet. It is very important to correctly assign the subnets to their respective sites.

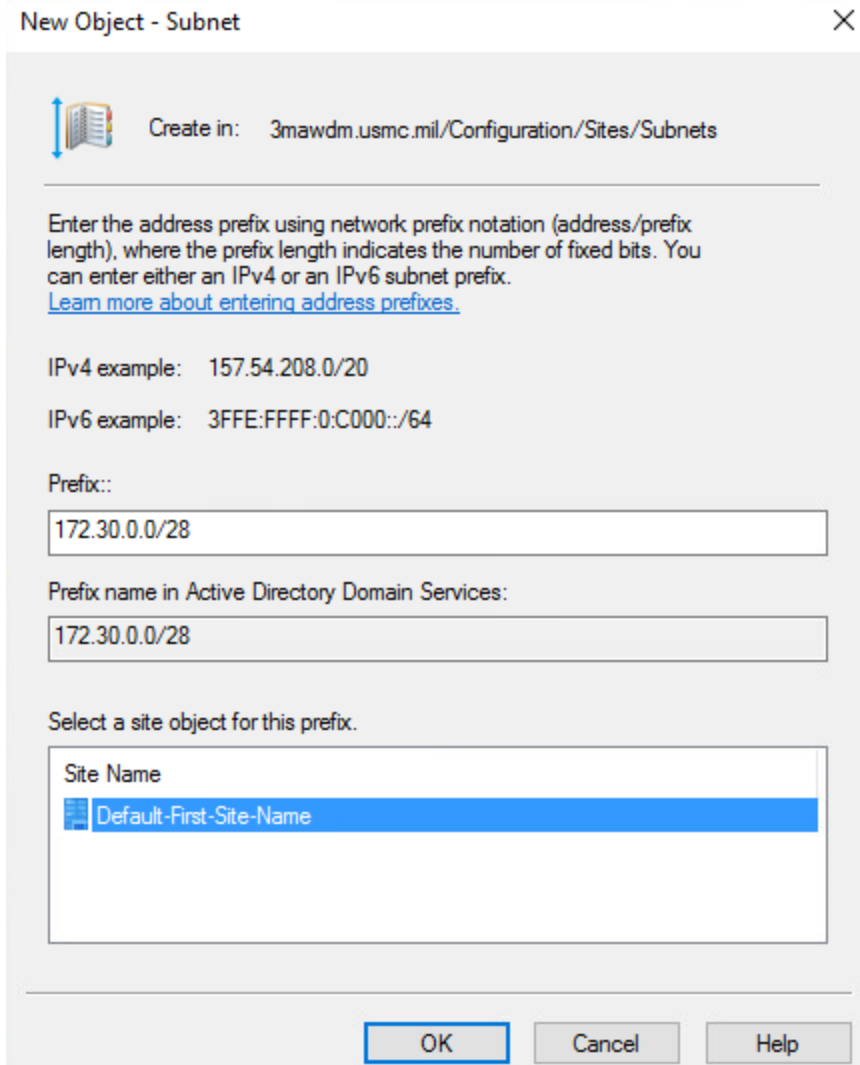
To assign a subnet to a site, open Active Directory Sites and Services.

Right click on Subnets and Select New Subnet.

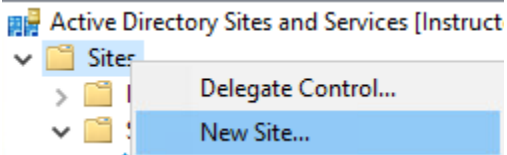


Type the subnet into the box, select the site it belongs to, and click ok.





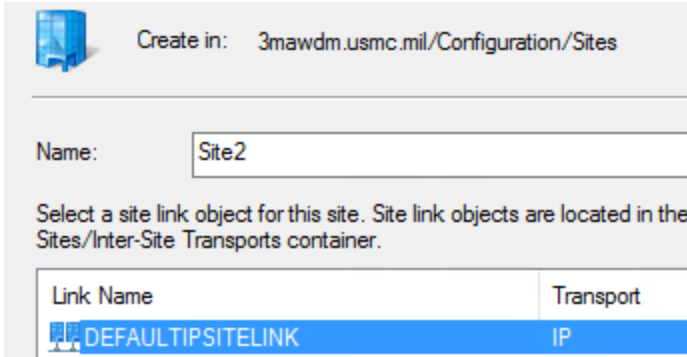
A site is either a geographically or logically separated area. To add a new site, right click on Sites and select New Site.



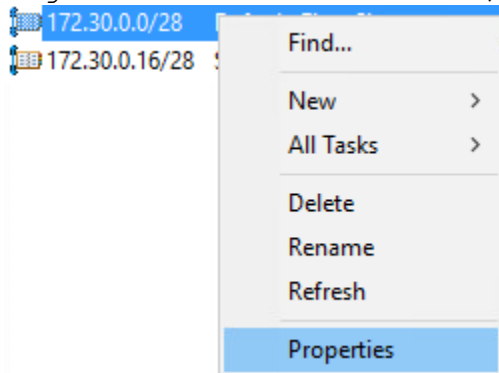
Type in the name for the site, select the link, and click ok.



## Domain Controllers

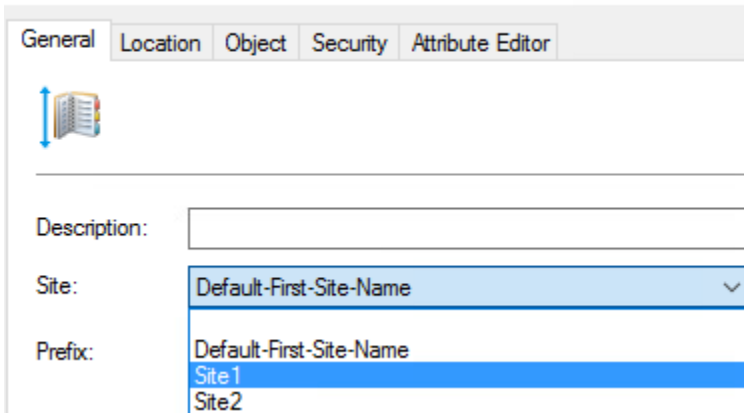


It is possible to reassign subnets to another site. Right click on the subnet, select properties.



Change the drop down to the site you want to reassign the subnet to.

### 172.30.0.0/28 Properties

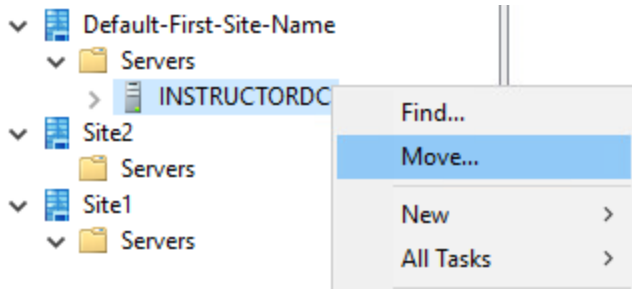


It is possible to manually move/assign a domain controller to another site. It is always best to create the sites, assign the subnets to the sites, and then promote a domain controller for that site.

Right click on the server, select move.

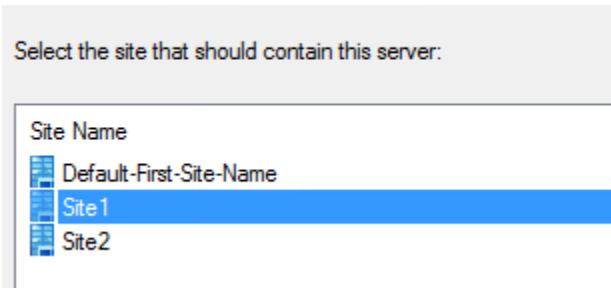


## Domain Controllers

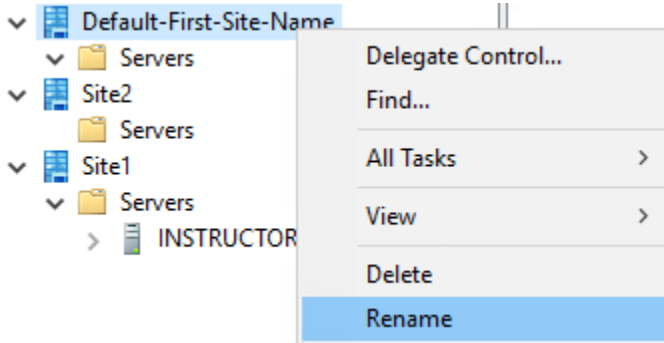


Select the site, click ok.

Move Server



To rename a site, right click on the site, select rename.

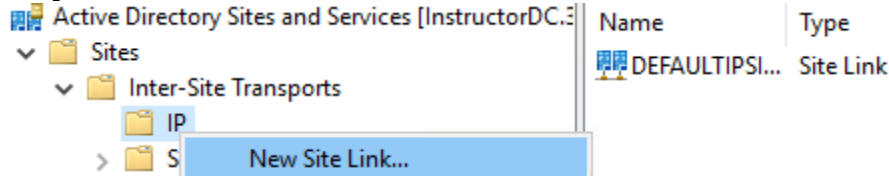


Be aware, renaming a site on a live network can have consequences. If you rename a site which is hosting Exchange services, you will have to go into each Exchange server, and point it to the new site name. This is just one example of a service which is site specific, and does not automatically update itself.

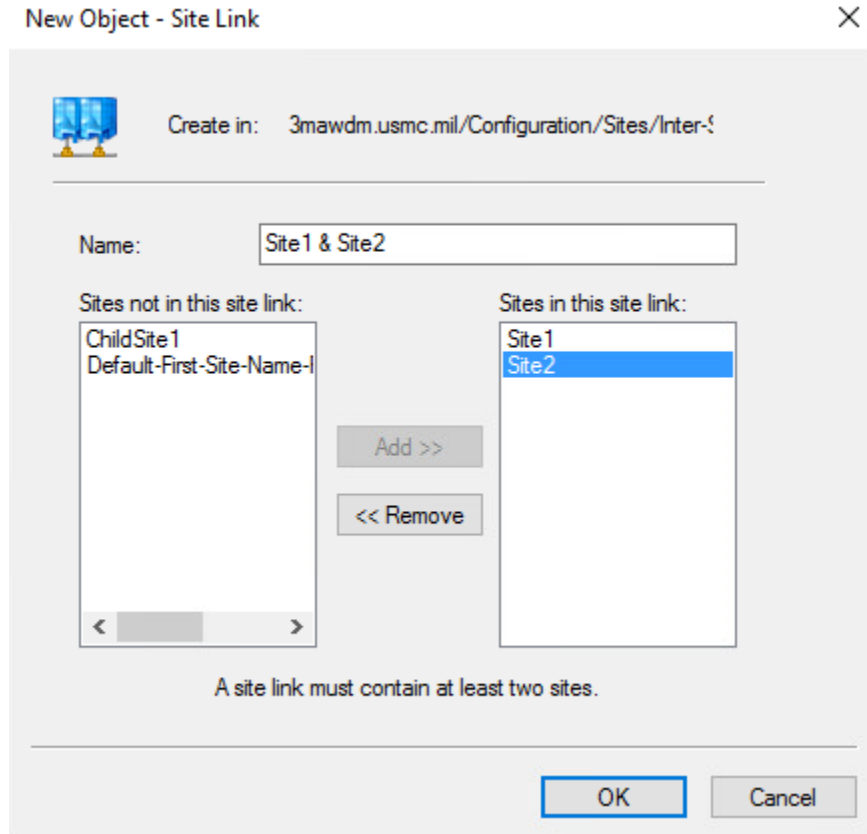
Inter-site transports are used by Active Directory and other services to exchange information between the different sites. For this setup, we will be creating inter-site links between each of the sites. For sites that are part of the same domain, the IP connector is required.



Right click IP, select New Site Link.



Type in a name for the site link. Select the site on the left side and click add. A site link must contain at least two sites.



The default settings for a new site link are a cost of 100, and a replication interval of 180 minutes (once every 3 hours).

Name	Type	Description	Cost	Replication Interval
DEFAULTIPSITELI...	Site Link		100	180
Site1 & Site2	Site Link		100	180

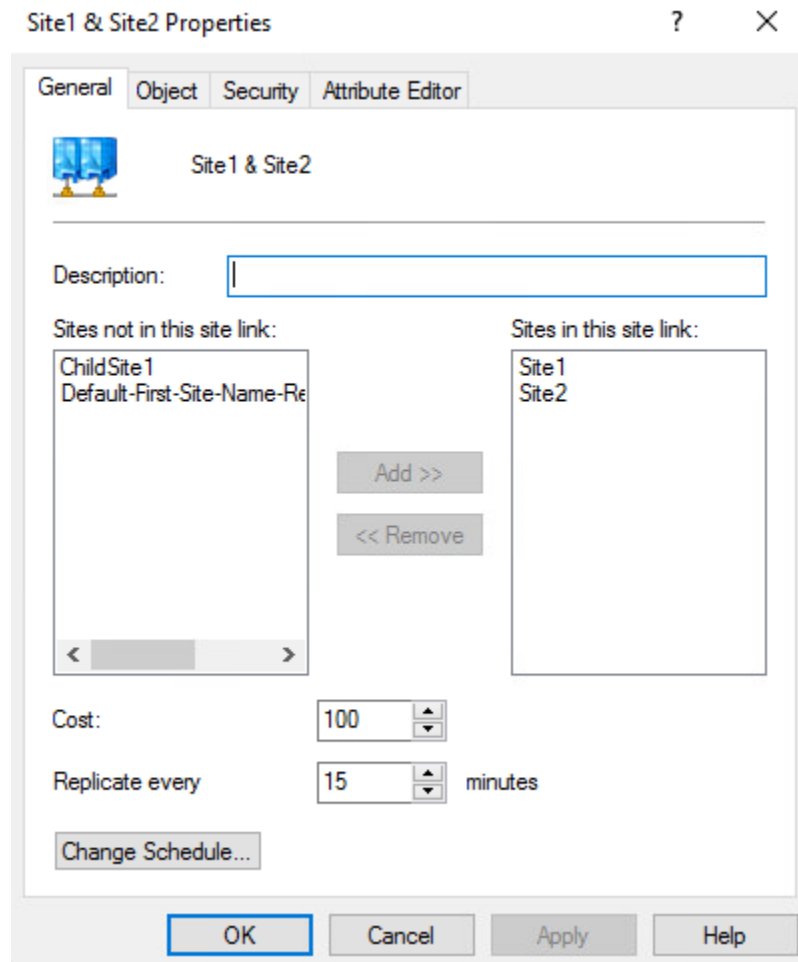
Your organization will determine what these settings should be based on the available bandwidth at, and location of each site.



**Extra:** In this lesson, we are going to assume that Site1 and Site2 are geographically separated with a WAN link, and that the child domain site is co-located with Site2. We will be setting the interval to every 15 minutes, and we will be enabling change notification on the link between Site2 and ChildSite1.

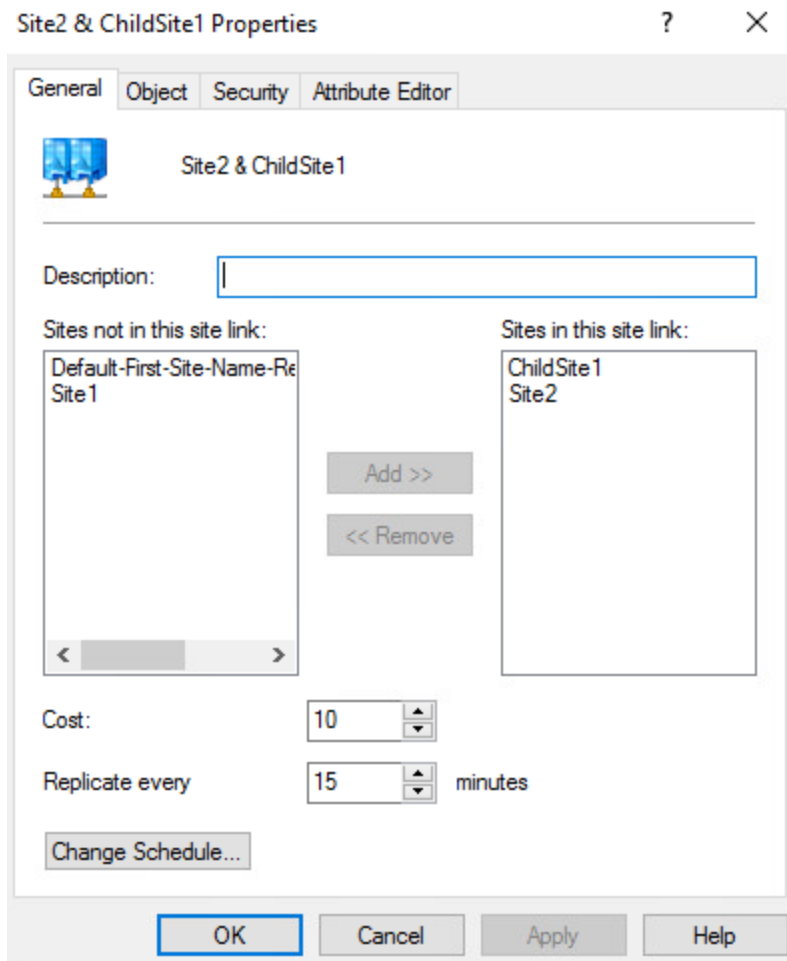
With change notification on, a domain controller who has a change, will notify its replication partner in another site that it has a change. It is primarily used for two sites that are geographically co-located but logically separated.

To change these values, double click on the site link.



Next we are going to create the site link between Site2 and ChildSite1. The cost will be 10, interval 15.

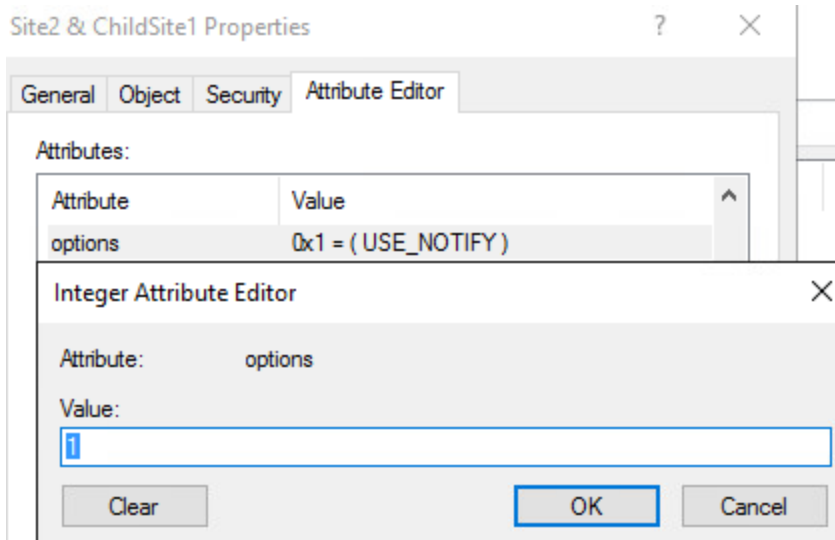




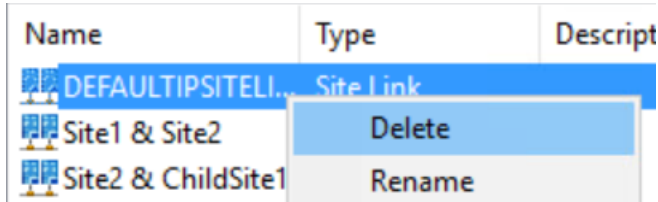
To enable change notification, go to the Attribute Editor tab, scroll down to the options attribute, double click or click edit, change the value from <not set> to a 1. Click ok.







After creating your inter-site transports, we will delete the default IP site link connector. Right click, select Delete.



**Extra Reading:**

The three articles below contain some good information concerning the KCC and how it works. Just because they reference Sever 2000 and Server 2003 doesn't mean they are not applicable.

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961781\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961781(v=technet.10))

<https://blogs.technet.microsoft.com/markmoro/2011/08/05/you-are-not-smarter-than-the-kcc/>

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755994\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755994(v=ws.10))

**Adding a DC to the Domain:**

When preparing to add a new domain controller to a domain, the first thing to do is to join the server to the domain. After it is joined to the domain, install the AD DS role. If you are adding a domain controller to a separate site, ensure the site is configured first.



## Domain Controllers

Log onto the server with a user who is a member of the Domain Admins group.  
After the role is installed, click the Promote this server to a domain controller link.

[View installation progress](#)

**i** Feature installation

---

Configuration required. Installation succeeded on Site2DC.3mawdm.usmc.mil.

---

**Active Directory Domain Services**  
Additional steps are required to make this machine a domain controller.  
[Promote this server to a domain controller](#)

**Group Policy Management**

Select Add a domain controller to an existing domain. The rest of the information should auto-populate.

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

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

Domain:

Supply the credentials to perform this operation

3MAWDM\DomainAdmin (Current user)

Based off the subnet association to the AD Site, the Site should populate with the correct site.

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify domain controller capabilities and site information

Domain Name System (DNS) server

Global Catalog (GC)

Read only domain controller (RODC)

Site name:

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:



## Domain Controllers

Once again, ignore the DNS delegation warning.

**⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more X**

Deployment Configuration | Specify DNS delegation options

Domain Controller Options |  Update DNS delegation

There are a few different ways for the new domain controller can receive the AD DS information. One is the Install From Media option. We will not use this. Normally we would leave the default of Replicate from: Any domain controller. This should use AD Sites and Services to figure out which domain controller is the closest and replicate from it. But, if for some reason you wanted to replicate from a specific domain controller, change it in the drop down.

Deployment Configuration | Specify Install From Media (IFM) Options

Domain Controller Options |  Install from media

DNS Options

**Additional Options** | Specify additional replication options

Paths | Replicate from: Any domain controller

Review Options | Any domain controller

Prerequisites Check | InstructorDC.3mawdm.usmc.mil

Once again, you can configure the paths.

### Paths

TARGET SERVER  
Site2DC.3mawdm.usmc.mil

Deployment Configuration | Specify the location of the AD DS database, log files, and SYSVOL

Domain Controller Options

DNS Options

Additional Options

**Paths**

Database folder:  ...

Log files folder:  ...

SYSVOL folder:  ...

Review your options and click next.



## Review Options

TARGET SERVER  
Site2DC.3mawdm.usmc.mil

Review your selections:

Configure this server as an additional Active Directory domain controller for the domain "3mawdm.usmc.mil".

Site Name: Site2

Additional Options:

Read-only domain controller: No

Global catalog: Yes

DNS Server: Yes

Update DNS Delegation: No

Source domain controller: any writable domain controller

Do not worry about the warnings, as long as the prerequisites check passes.

## Prerequisites Check

TARGET SERVER  
Site2DC.3mawdm.usmc.mil

✔ All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) ✕

Click install.

The server will install the DNS Server service, configure it, replicate the current AD information, and restart.

## Creating a Child Domain:

When creating a child domain, you do not join the domain controller to the existing forest first. This will require an account which is a member of the Enterprise Admins group.



## Domain Controllers

The screenshot shows the 'Deployment Configuration' window. On the left is a navigation pane with 'Deployment Configuration' selected. The main area is titled 'Select the deployment operation' and has three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest' (which is selected), and 'Add a new forest'. Below this is the section 'Specify the domain information for this operation'. It includes a 'Select domain type:' dropdown menu set to 'Child Domain', a 'Parent domain name:' text box containing '3mawdm.usmc.mil' with a 'Select...' button to its right, and a 'New domain name:' text box containing 'child'. The final section is 'Supply the credentials to perform this operation', showing the text '3mawdm\enterpriseadmin' and a 'Change...' button to its right.

To enter the Enterprise Administrator credentials, click the Change button on the right hand side. The credentials need to be entered as either <Parent Domain>\enterpriseadmin or <Parent Domain FQDN>\enterpriseadmin.

This screenshot shows a 'Windows Security' dialog box titled 'Credentials for deployment operation'. It prompts the user to 'Supply credentials for the deployment operation'. The username field contains '3mawdm.usmc.mil\enterpriseadmin' and the password field is masked with dots. There are 'Select...' and 'Change...' buttons on the right side of the dialog.

For the most part, the windows are identical to deploying any other domain controller. One slight difference is with DNS. Do want to create a DNS delegation for the child domain. Some additional permissions may end up being needed on the account to properly perform the actions.

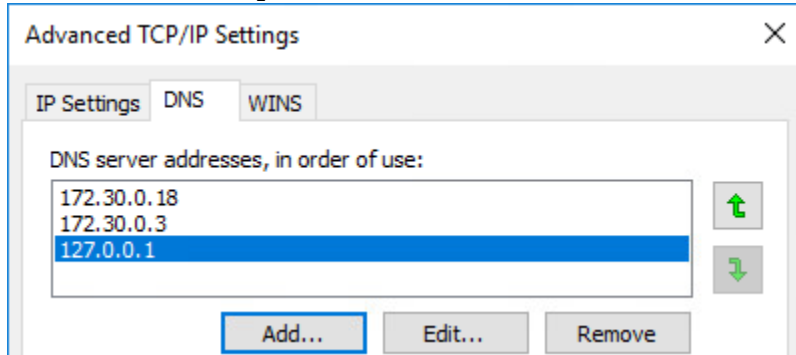
The screenshot shows the 'DNS Options' section of the deployment configuration. It is titled 'Specify DNS delegation options' and has a checked checkbox for 'Create DNS delegation'. Below this is the section 'Credentials for delegation creation' with the text '3mawdm\enterpriseadmin'.



## DC NIC Settings:

With a domain controller, the DNS configuration on the NIC is important. The correct DNS settings on the domain controller are

- First: A partner domain controller in the same site.
- Second: A domain controller in a remote site.
- Last: The loopback.



Active directory relies on DNS, and DNS is active directory integrated. When the domain controller is powering on, it creates a race condition. DNS will not go live until AD is synced, AD will not go live without DNS. When powering everything on, I have found the easiest method is to power on the first domain controller, power on the second, which will then sync off of the first, the restart the first domain controller, which will then successfully sync off of the second.

If a domain controller cannot sync its DNS settings, it will go live after 10 minutes. There is also a registry edit to bypass the initial sync.

HKLM\System\CurrentControlSet\Services\NTDS\Parameters\Repl Perform Intial Synchronizations

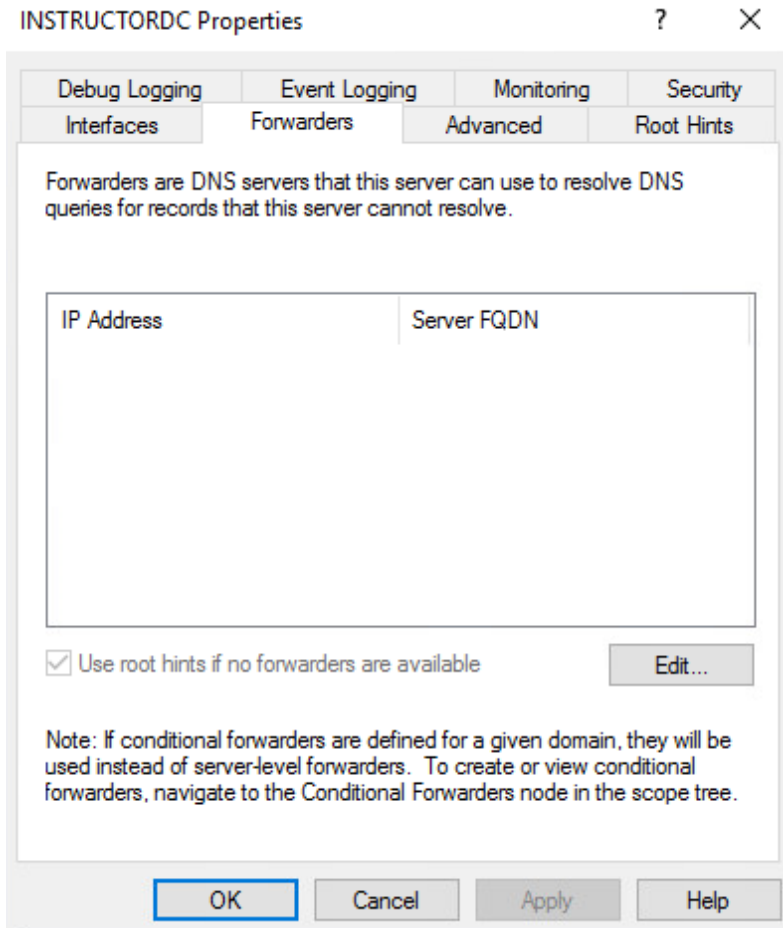
Create the key as a REG\_DWORD and set the value to 0.

This will allow the domain controller to start and function without performing the initial synchronizations.

## DNS Forwarders:

DNS forwarders are used to resolve information not hosted on the DNS server. Typically, these are only used to point to external DNS servers.





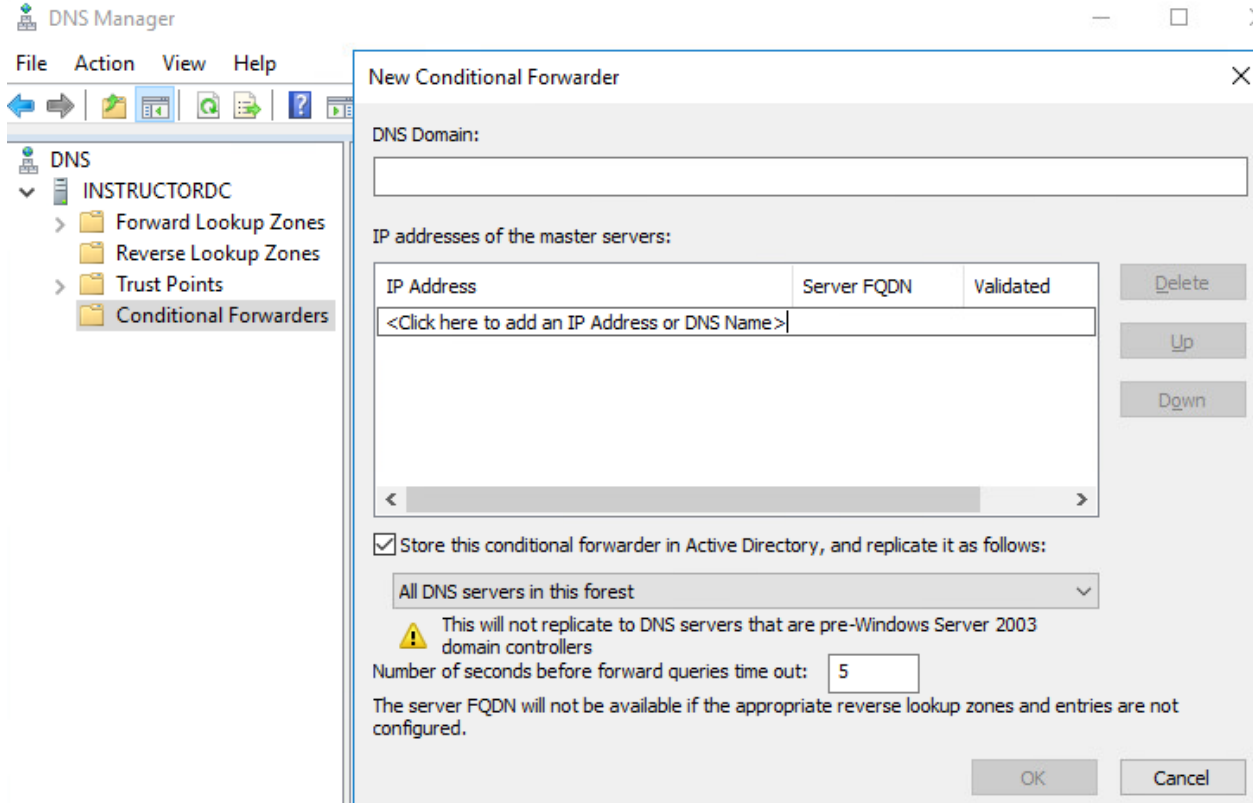
If a conditional forwarder is configured, it will be used instead of the forwarder.

A conditional forwarder is created when you know the IP addresses of the DNS servers which are authoritative for the zone.

The most common use is for building a trust between two entities after establishing a lateral networking connection. Why would you go all the way out to the internet, when you can go over the LAN to find the information?



## Domain Controllers



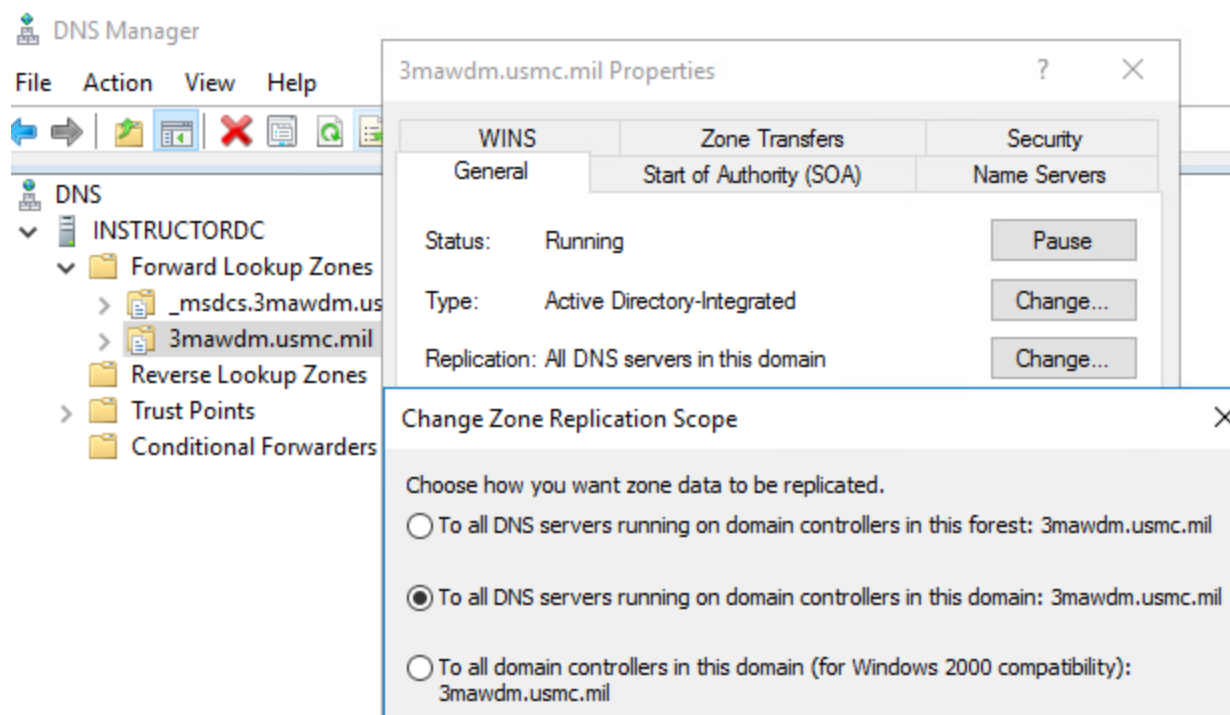
You can store the conditional forwarder in AD, and replicate it to all DNS servers in the domain / forest.

By default, the zone for your domain is replicated to all domain controllers in the domain. Depending on how many child domains and their interaction with each other, it may be best to have the DNS information replicated to every domain controller in the forest.





## Domain Controllers



### DHCP :

With Server 2016, it is possible to configure load balancing and failover on the DHCP role. It is advised to create a DHCP service account, which will be used to register and deregister the DNS records. This account will be shared between the two DHCP servers. On the Cisco side, it is possible to have multiple IP helper entries. The gateway will send a unicast packet to each entry.

When running in a load balancing mode, the two servers will each issue addresses from the same DHCP pool. They will split the pool in half, the first server starting to issue from the start of the pool and the second from the midpoint of the pool. For example, on a Class C subnet, the first would issue starting at .1 and the second would start issuing from .128.

While it takes an administrator to install the DHCP role on a server, it will take an Enterprise Admin to come behind and actually authorize the server in Active Directory. Until the server is authorized in AD, it will not issue addresses.

The first step is to add the DHCP Server role.



## Select server roles

DESTINATION SERVER  
InstructorDC.3mawdm.usmc.mil

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

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

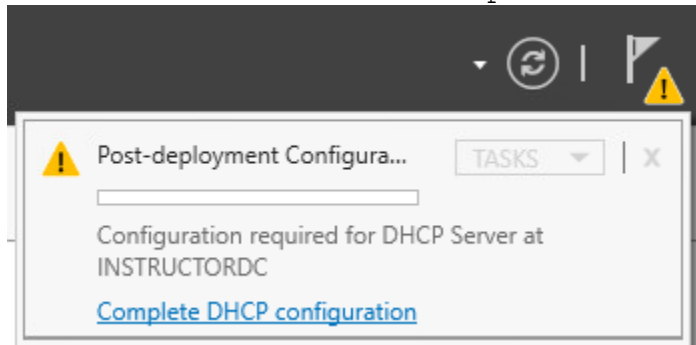
Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	
<input checked="" type="checkbox"/> Active Directory Domain Services (Installed)	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input checked="" type="checkbox"/> <b>DHCP Server</b>	Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
<input checked="" type="checkbox"/> DNS Server (Installed)	

The Dynamic Host Configuration Protocol allows servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients. Deploying a DHCP server on the network provides computers and other TCP/IP-based network devices with valid IP addresses and the additional configuration parameters these devices need, called DHCP options. This allows computers and devices to connect to other network resources, such as DNS servers, WINS servers, and routers.

### Things to note:

- You should configure at least one static IP address on this computer.
- Before you install DHCP Server, you should plan your subnets, scopes and exclusions. Store the plan in a safe place for later reference.

Once the role is installed there are two locations where an Enterprise Admin can authorize the server. The first is in the Server Manager, as part of the post installation tasks. The second is in the DHCP snapin.



The screenshot shows the 'Description' step of the DHCP Post-Install configuration wizard. It contains a list of steps: 'Description' (selected), 'Authorization', and 'Summary'. The main text states: 'The following steps will be performed to complete the configuration of the DHCP Server on the target computer: Create the following security groups for delegation of DHCP Server Administration. - DHCP Administrators - DHCP Users Authorize DHCP server on target computer (if domain joined).'

We are going to skip the authorization here, as the Domain Admin user account does not have permissions to authorize the server. Specify the credentials to be used to authorize this DHCP server in AD DS.

Use the following user's credentials  
User Name:

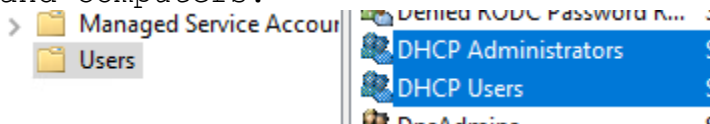
Use alternate credentials  
UserName:

Skip AD authorization

The status of the post install configuration steps are indicated below:

Creating security groups ..... Done  
Please restart the DHCP server service on the target computer for the security groups to be effective.

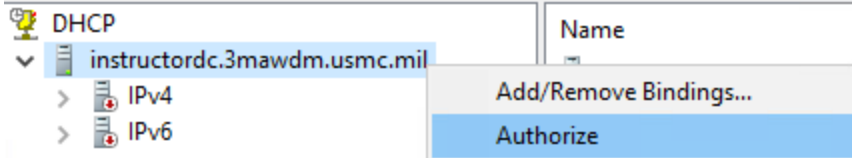
The security groups were created under the Users OU in AD Users and Computers.



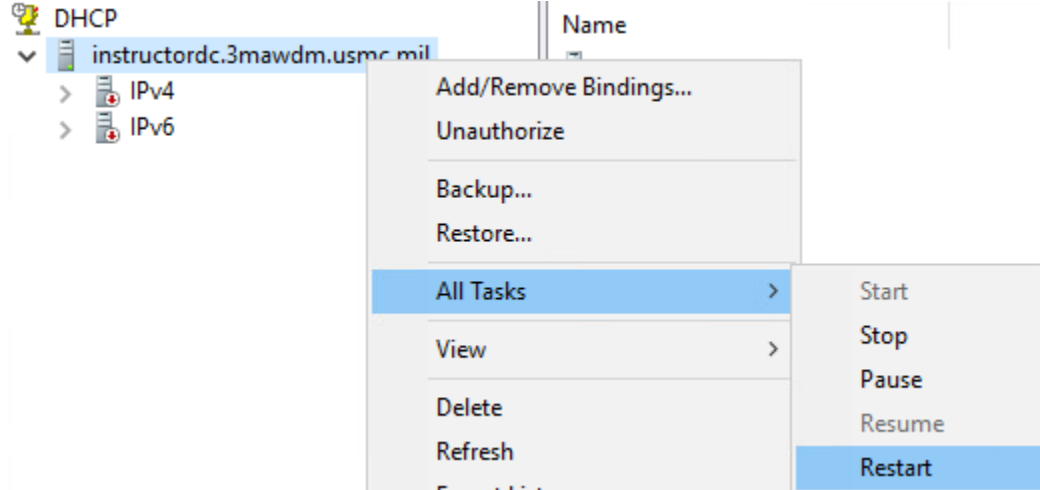
Using the DHCP snapin.



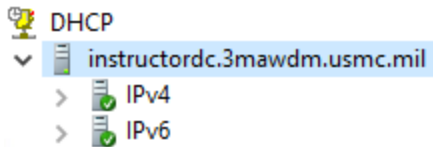
## Domain Controllers



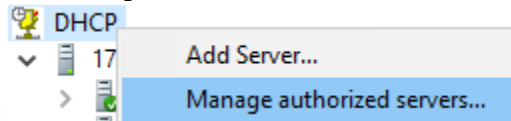
The authorization takes place in Active Directory. Depending on your replication topology, it may take some time for the server to receive the authorization. Once the server is authorized, you will need to restart the DHCP Server service.



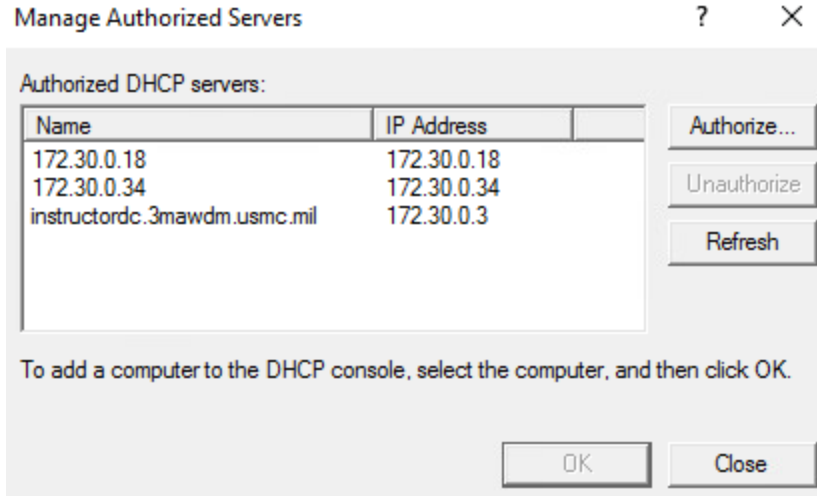
Once it has been restarted, the red down arrows will change to the green checkboxes.




To view all of the authorized DHCP servers in your forest, you can right click on DHCP and select Manage Authorized Servers.



## Domain Controllers

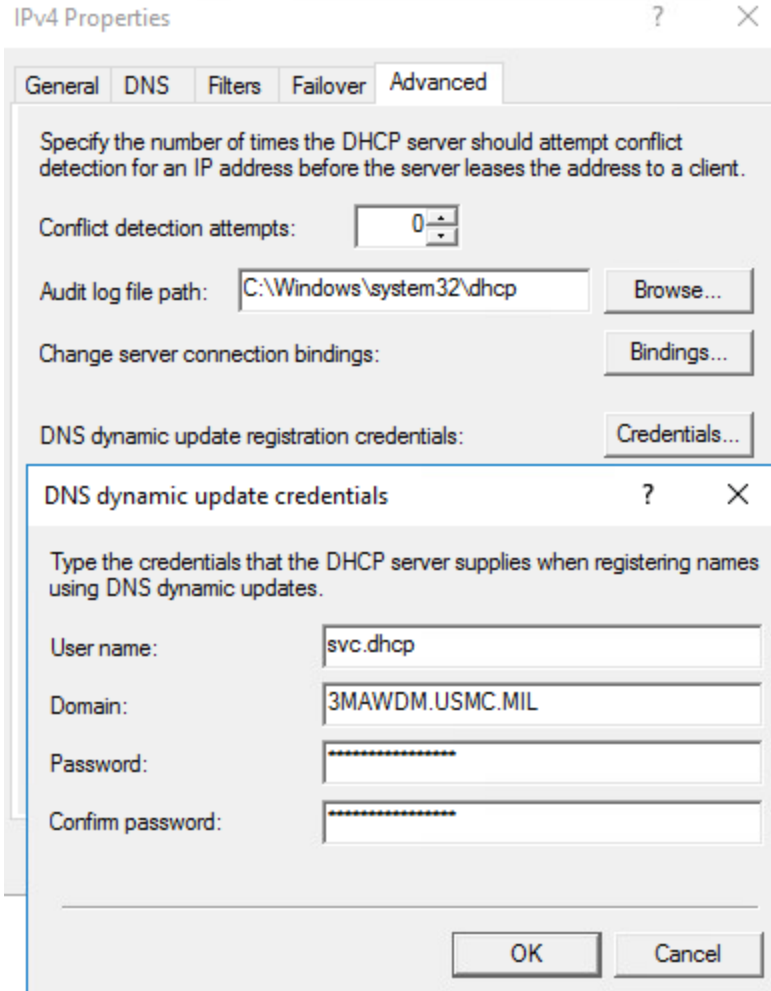


The service account for DHCP is a standard user account. Your organization will dictate the naming standards. This account becomes important when it comes to DHCP failover. If this account is not defined, the DHCP server which registered the DNS record is the only one with permissions to change the record. By defining the service account across the DHCP servers, all of the DHCP servers can then modify the DNS record for the host whenever the host changes networks and receives a new address.

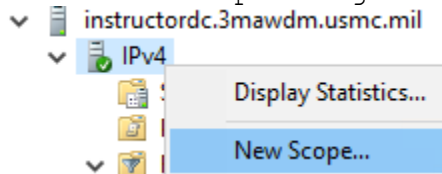
Name	Type
 DHCP Service Account	User

To add the service account to the DHCP server, right click on the IPv4 and select properties. Go to the Advanced Tab, click credentials.





Now that the DHCP servers are set to register the host records for the hosts using the service account. The next step is to create a scope. Right click the IPv4, select New Scope.



New Scope Wizard

**Scope Name**

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

Define the IP address range and subnet.

New Scope Wizard

**IP Address Range**

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

If you defined the entire address range, you will need to add exclusions for your default gateway and other statically defined devices.



New Scope Wizard

**Add Exclusions and Delay**

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:  End IP address:

Excluded address range:

Define the lease time.  
New Scope Wizard

**Lease Duration**

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:  Hours:  Minutes:

A Microsoft DHCP client will attempt to renew its lease at the 50%, 75% and 100% mark. If it is unsuccessful in reaching a DHCP server, but it can still reach its default gateway, it will continue to use the current IP.





New Scope Wizard

**Configure DHCP Options**

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

Add the router / default gateway IP address, and click Add.

**Router (Default Gateway)**

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

Add

172.30.0.1

Remove

Set the DNS servers and the order for the scope. You can define multiple DNS servers, it is not restricted to just two.



### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value="  . . ."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="172.30.0.18"/> <input type="text" value="172.30.0.3"/> <input type="text" value="172.30.0.34"/>	<input type="button" value="Remove"/> <input type="button" value="Up"/> <input type="button" value="Down"/>

WINS is only used in specific cases. Leave it blank.

### WINS Servers

Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.



Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Activate the scope.

### Activate Scope

Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

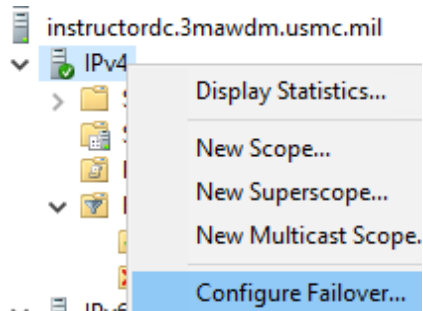
Yes, I want to activate this scope now

No, I will activate this scope later

Normally, you will only want to configure DHCP failover between servers that are at the same site. Right click on either the IPv4 or on one of the configured scopes and select Configure Failover.



Domain Controllers



DHCP Failover enables high availability of DHCP services by synchronizing IP address lease information between two DHCP servers. DHCP failover also provides load balancing of DHCP requests.

This wizard will guide you through setup of DHCP failover. Select from the following list of scopes which are available to be configured for high availability. Scopes which are already configured for high availability are not displayed in the list below.

Available scopes:  Select all.

172.30.0.0

Click on add server and select one of your authorized DHCP servers.

Provide the host name or IP address of the partner DHCP server with which failover should be configured. You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers. Alternatively, you can type the host name or IP address of the partner server. Partner Server: [dropdown] [Add Server]

Add Server dialog box. Select a server you want to add to your console. Radio buttons for 'This server:' and 'This authorized DHCP server:'. Table with columns Name and IP Address. Row 1: 172.30.0.18, 172.30.0.18. Row 2: 172.30.0.34, 172.30.0.34. Row 3: instructordc.3mawdm.usmc.mil, 172.30.0.3.

In the drop down you can change it from Load Balance to Hot Standby if preferred. Enter a shared secret for the servers.



## Domain Controllers

Create a new failover relationship with partner 172.30.0.18

Relationship Name:

Maximum Client Lead Time:  hours  minutes

Mode:

Load Balance Percentage

Local Server: %

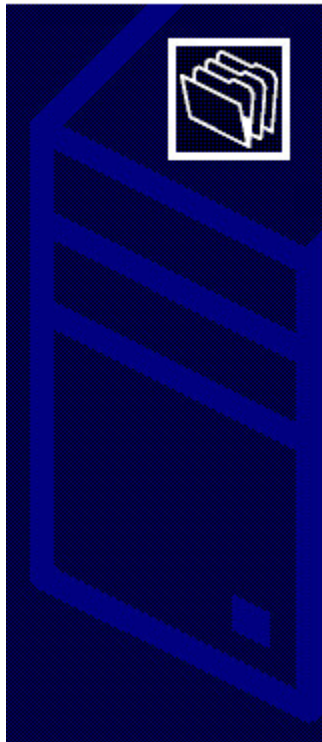
Partner Server: %

State Switchover Interval:  minutes

Enable Message Authentication

Shared Secret:

Review the summary and click finish.  
Configure Failover



Failover will be set up between instructordc.3mawdm.usmc.... and 172.30.0.18 with the following parameters.

Scopes:

172.30.0.0

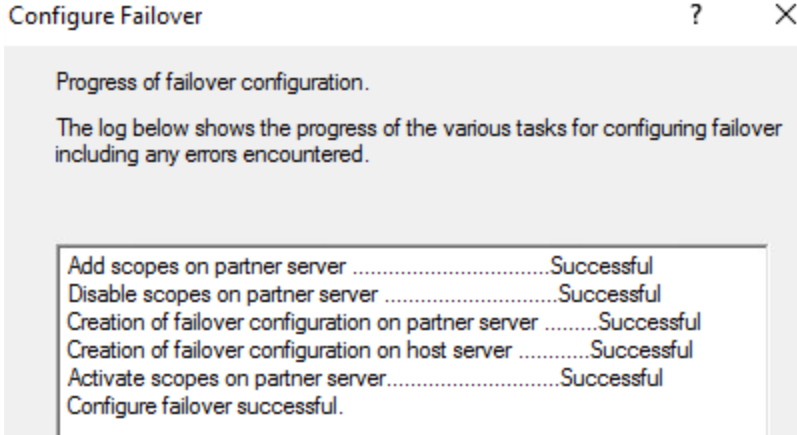
Relationship Name:	instructordc.3mawdm.usmc.mil-1
Maximum Client Lead Time:	1 hrs 0 mins
Mode:	Load balance
State Switchover Interval:	Disabled

Load Balance Percentage

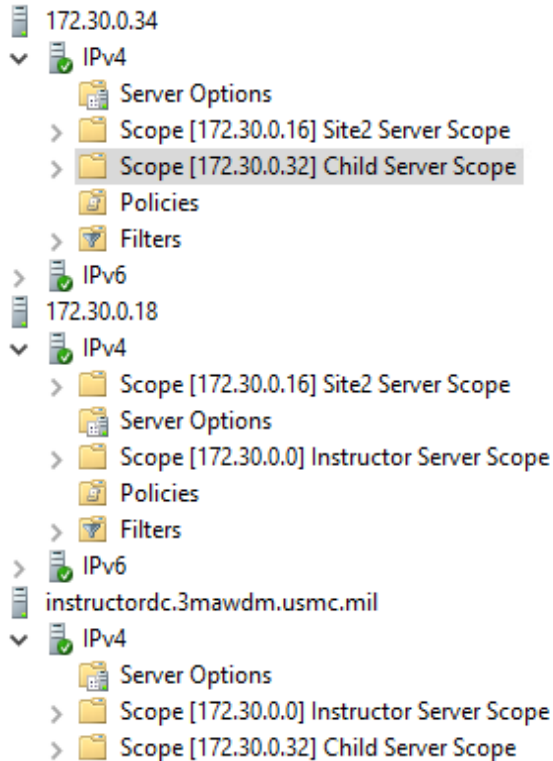
Local Server:	50 %
Partner Server:	50 %



Jade Falcon LLC



Each scope can be configured for failover on two servers. But, each scope can be configured separately. Ideally, the two servers are at the site which is providing the services for the subnet, and not going over a WAN link.



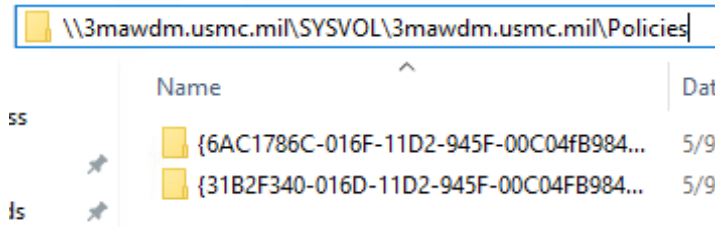
## Policy Store:

Group policy is a powerful tool and can save an administrator from having to perform touch labor and every device. Configure the policy, test it, and then deploy it out and watch Active Directory take care of all the work. The problem is, the end device may not know what that specific defined setting in the policy is referring to. The templates (.adml) and (.admx) files are used to define the setting. By default, they are stored locally on each device (C:\Windows\PolicyDefinitions). The solution, create a centralized policy store.

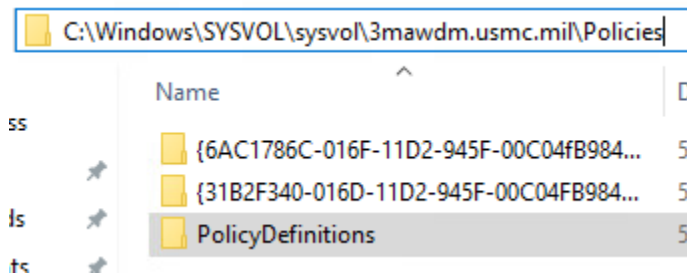
If you are not on the domain controller, ie working off a workstation which is joined to the domain, browse to: \\<FQDN>\SYSVOL\<FQDN>\Polcies\ and create a folder called PolicyDefinitions.

The example for this lab would be:

\\3mawdm.usmc.mil\SYSVOL\3mawdm.usmc.mil\policies\PolicyDefinitions\



If you are logged onto the domain controller, you can browse to the (C:\Windows\SYSVOL\sysvol\3mawdm.usmc.mil\Policies\



Once the directory is created, copy the files from the C:\Windows\PolicyDefinitions into the new PolicyDefinitions directory. One copy from each version of the OS will be needed. For example, one copy from Windows Server 2016, and one copy from Windows 10. If you intend to use group policy to control Office, you will need to copy a set into there.



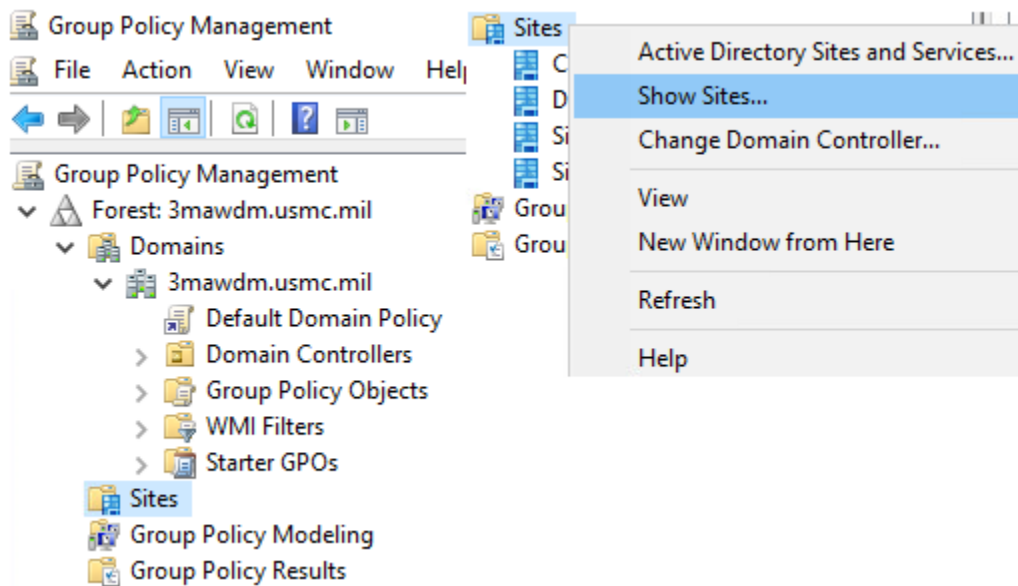
With the feature updates, the existing files will change occasionally or have additional content added. After installing a new update, it may be best to see if anything has changed.

Once the policy store is created, when the endpoints are checking for the defined objects, they will automatically check the Policy Store. Being part of the SYSVOL, it will replicate to every domain controller, and will be widely available.

### Basic Group Policy:

This is not going to be an expansive lesson on group policy. It will just cover a couple of the basic, general principles.

By default, the sites are not shown, you will need to right click on the Sites, and select show sites.



Group policy objects are processed in the following order.

1. Local Group Policy
2. Linked to the site.
3. Linked to the domain.
4. Linked to the OU.

The Enforced setting on a group policy object will prevent any other setting downstream from changing it. It will also be applied to OUs that have broken inheritance.

A good example for this is WSUS.



## Domain Controllers

A good administrator wants to ensure that all the systems on their network have access to the required updates. Having a couple hundred machines pull each update over a WAN link is not the best solution, when they can host a local copy of the update repository.

A GPO defining the location of the master server, would be linked to the domain.

A GPO defining the location of the Replica server would be linked to each site, and enforced.

A GPO would NOT be defined at the OU level, as the OU is there to logically organize the systems, and doesn't dynamically change based on their current location.

The screenshot shows the Group Policy Management console for the domain 3mawdm.usmc.mil. The left pane shows the hierarchy: 3mawdm.usmc.mil > 3MAWDM > Helpdesk Permissions. The right pane shows the 'Helpdesk Permissions' GPO configuration. The 'Linked Group Policy Objects' tab is active, displaying a table with two linked GPOs:

Link Order	GPO
1	User Group Policy
2	Computer Group Policy

The 'Computer Group Policy' row has a lock icon next to it, indicating it is enforced. The 'Link Order' column has up and down arrows for reordering. The 'Group Policy Inheritance' tab is also visible.

The link order listed on the Linked Group Policy Objects tab will allow the administrator to change which GPO will take effect when there is a conflict in the settings. The link order can be changed by clicking on the up and down arrows. The lock next to the GPO on the ChildSite1 means it is being enforced. To change the enforcement status, right click on the Link.

GPOs can be targeted several different ways. We will take a quick look at targeting a specific group of users.





**Security Filtering**

The settings in this GPO can only apply to the following groups, users, and computers:

Name
 Authenticated Users

**WMI Filtering**

This GPO is linked to the following WMI filter:

Under the settings for the GPO, this GPO will apply to all Authenticated users and is not targeted with a WMI filter. Select Authenticated Users and click remove. Read the warning carefully.

**Group Policy Management**




Group Policy requires each computer account to have permission to read GPO data from a domain controller in order for User Group Policy settings to be successfully applied. Removing the Authenticated Users group may prevent processing of User Group Policies. Please add the Domain Computers or the Authenticated Users security group with at least read-only permissions. For more information, please see <https://go.microsoft.com/fwlink/?linkid=843010>

The short breakdown is, the computer account needs to be able to read the GPO, before it can apply it to a user account.

Next, we will add the active directory group we want to target.

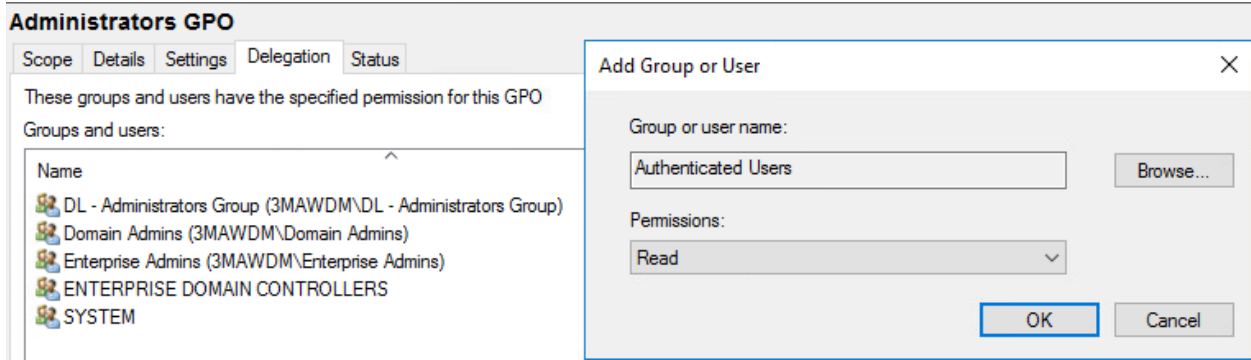
**Security Filtering**

The settings in this GPO can only apply to the following groups, users, and computers:

Name
 DL - Administrators Group (3MAWDM\DL - Administrators Group)

If you tried it now, it would not function, due to the warning message. On the Delegation Tab, click add, select Authenticated Users, and grant the group Read permissions.





Now the workstation will have read permissions on the GPO and apply the settings to the user objects.

### Flexible Single Master Operation (FSMO) Roles:

There are five key roles for the forest, and two sub roles which will affect the successful operation of a domain. These are known as the FSMO roles. First, the five that everyone knows:

- Schema Master (One per forest.)
- Domain Naming Master (One per forest.)
- RID Master (One per domain.)
- PDC Emulator (One per domain.)
- Infrastructure Master (\*\*One per domain.)

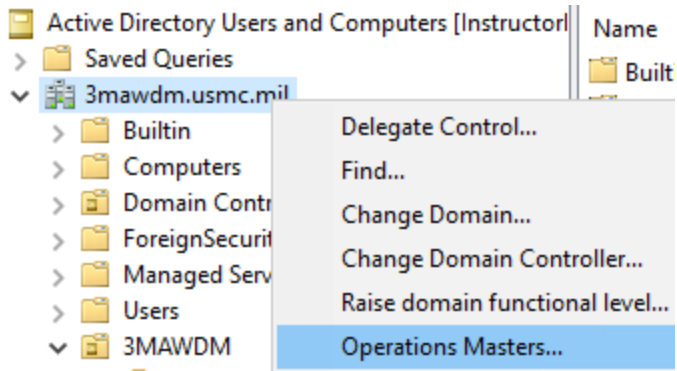
\*\*Technically the two sub roles are extra Infrastructure Master roles. There is one role per application partition. There is the Infrastructure Master, then another for the Forest DNS Zones Master, and a third for the Domain DNS Zones Master. The last two do not show up in a query, are not moved by the usual tool set, but can cause issues.

The FSMO roles can be located and moved through various tools. The first one is the GUI, the second is the command prompt, the third is through PowerShell. If you are attempting to move the role through the GUI, you will need to connect the snap-in to the server you want to move the role to.

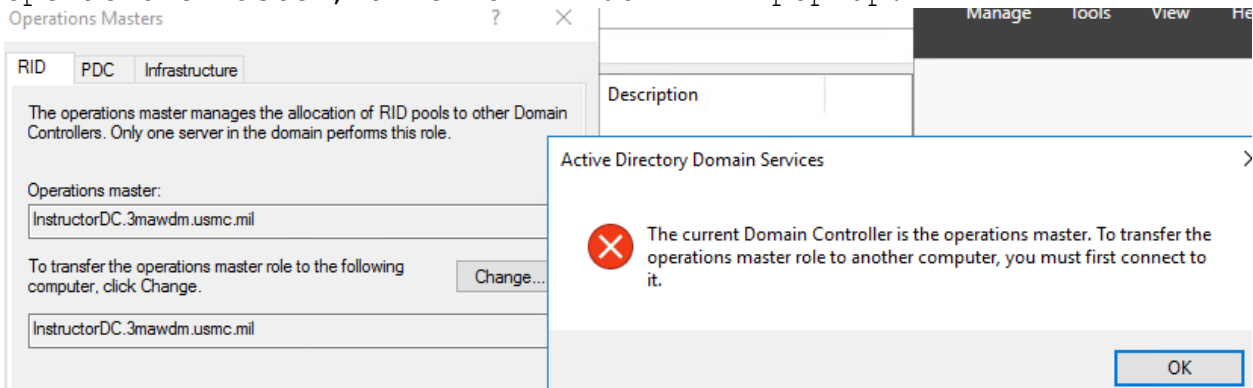
In Active Directory Users and Computers, right click on the domain, and select Operations Masters.



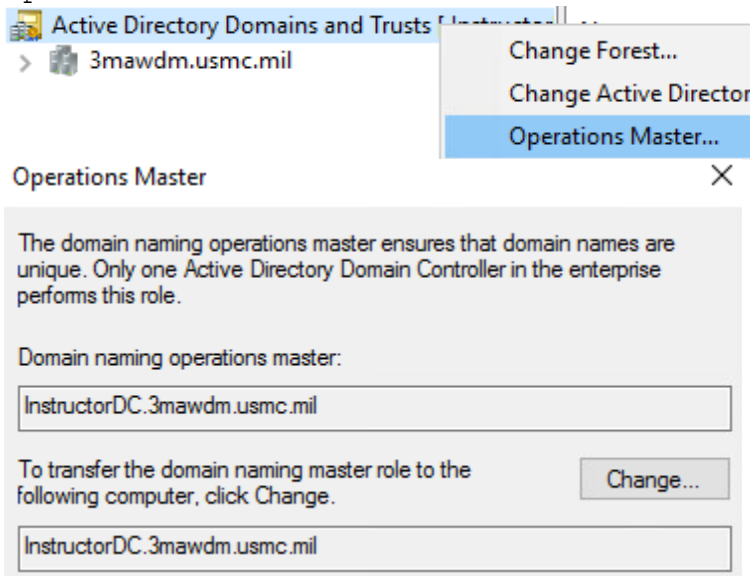
## Domain Controllers



The RID, PDC, and Infrastructure masters are located here. If the change button is hit while connected to the current operations master, an error window will pop up.



The domain naming master is located in AD Domains and Trusts. Right click on Active Directory Domains and Trusts, select Operations Master.



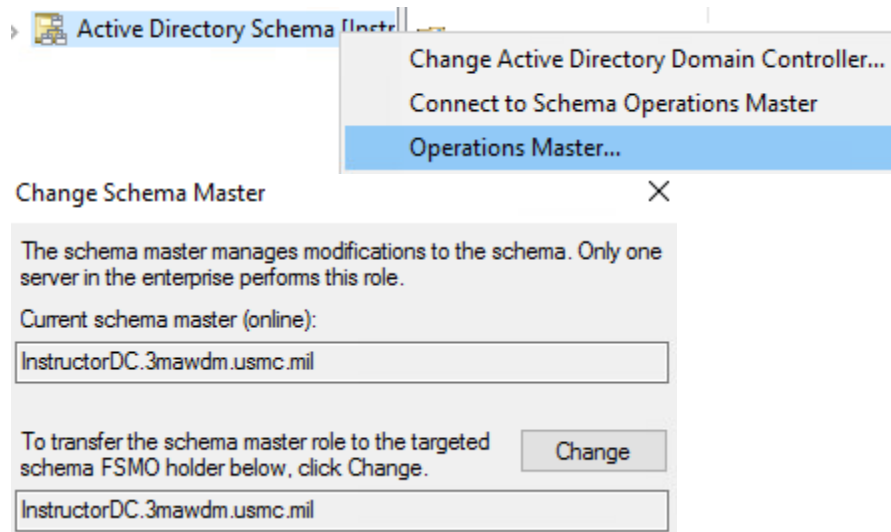
## Domain Controllers

The schema master GUI is not enabled by default. Before it can be accessed, the .dll needs to be registered. The command is:  
regsvr32 schmmgmt.dll



Depending on the security configuration of the server or workstation, it may or may not work from the run window. If it produces an error, open a command prompt as an administrator and register it that way.

Once the .dll is registered, open the Microsoft Management Console (MMC) and add the AD Schema snap-in. The Operations Master can then be located by right clicking on Active Directory Schema, and selecting Operations Master.



**Warning:** The schema contains the definitions for every object in Active Directory. It is not recommended to make manual changes to the schema. A mistake could brick the entire forest.



## Domain Controllers

Locating the FSMO roles through the command prompt is a single command. netdom query fsmo

```
Administrator: Command Prompt
C:\Windows\system32>netdom query fsmo
Schema master           InstructorDC.3mawdm.usmc.mil
Domain naming master    InstructorDC.3mawdm.usmc.mil
PDC                     InstructorDC.3mawdm.usmc.mil
RID pool manager        InstructorDC.3mawdm.usmc.mil
Infrastructure master    InstructorDC.3mawdm.usmc.mil
The command completed successfully.
```

PowerShell can be used to locate the roles; however, the quickest method is the `netdom query fsmo`, which can also be ran from within PowerShell.

For PowerShell there are two commands, and it will produce much more information than requested. There is more to type if the information needs to be filtered to just show the operations masters. `Get-ADForest` and `Get-ADDomain`.

`Get-ADForest` will show the Domain Naming Master and the Schema Master.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> Get-ADForest

ApplicationPartitions : {DC=ForestDnsZones,DC=3mawdm,DC=usmc,DC=mil,
                        DC=DomainDnsZones,DC=child,DC=3mawdm,DC=usmc,DC=mil,
                        DC=DomainDnsZones,DC=3mawdm,DC=usmc,DC=mil}
CrossForestReferences : {}
DomainNamingMaster     : InstructorDC.3mawdm.usmc.mil
Domains                : {3mawdm.usmc.mil, child.3mawdm.usmc.mil}
ForestMode             : Windows2016Forest
GlobalCatalogs        : {InstructorDC.3mawdm.usmc.mil, Site2DC.3mawdm.usmc.mil, ChildDC.child.3mawdm.usmc.mil}
Name                   : 3mawdm.usmc.mil
PartitionsContainer    : CN=Partitions,CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
RootDomain             : 3mawdm.usmc.mil
SchemaMaster           : InstructorDC.3mawdm.usmc.mil
Sites                  : {Default-First-Site-Name-Renamed, Site2, Site1, ChildSite1}
SPNSuffixes            : {}
UPNSuffixes            : {}
```

`Get-ADDomain` will show the Infrastructure Master, the PDC Emulator, and the RID Master.



## Domain Controllers

```
PS C:\Windows\system32> Get-ADDomain

AllowedDNSSuffixes           : {}
ChildDomains                 : {child.3mawdm.usmc.mil}
ComputersContainer          : CN=Computers,DC=3mawdm,DC=usmc,DC=mil
DeletedObjectsContainer     : CN=Deleted Objects,DC=3mawdm,DC=usmc,DC=mil
DistinguishedName           : DC=3mawdm,DC=usmc,DC=mil
DNSRoot                     : 3mawdm.usmc.mil
DomainControllersContainer  : OU=Domain Controllers,DC=3mawdm,DC=usmc,DC=mil
DomainMode                  : Windows2016Domain
DomainSID                   : S-1-5-21-2077987980-2596416506-3176031181
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=3mawdm,DC=usmc,DC=mil
Forest                      : 3mawdm.usmc.mil
InfrastructureMaster        : InstructorDC.3mawdm.usmc.mil
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects   : {cn={59A59207-09EA-4D77-8450-DD1C0C76AF18},cn=policies,cn=system,DC=3mawdm,DC=usmc,DC=mil, CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Polices,CN=System,DC=3mawdm,DC=usmc,DC=mil}
LostAndFoundContainer       : CN=LostAndFound,DC=3mawdm,DC=usmc,DC=mil
ManagedBy                  : 
Name                        : 3mawdm
NetBIOSName                 : 3MAWDM
ObjectClass                  : domainDNS
ObjectGUID                  : a4c01798-5a69-48c9-aa40-ff7d4b4f7b5e
ParentDomain                 : 
PDCEmulator                 : InstructorDC.3mawdm.usmc.mil
PublicKeyRequiredPasswordRolling : True
QuotasContainer             : CN=NTDS Quotas,DC=3mawdm,DC=usmc,DC=mil
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers     : {InstructorDC.3mawdm.usmc.mil, Site2DC.3mawdm.usmc.mil}
RIDMaster                   : InstructorDC.3mawdm.usmc.mil
SubordinateReferences       : {DC=child,DC=3mawdm,DC=usmc,DC=mil, DC=ForestDnsZones,DC=3mawdm,DC=usmc,DC=mil, DC=DomainDnsZones,DC=3mawdm,DC=usmc,DC=mil, CN=Configuration,DC=3mawdm,DC=usmc,DC=mil}
SystemsContainer            : CN=System,DC=3mawdm,DC=usmc,DC=mil
UsersContainer              : CN=Users,DC=3mawdm,DC=usmc,DC=mil
```

To view just the roles, use the following commands.

Get-ADForest | Format-List DomainNamingMaster, SchemaMaster  
and

Get-ADDomain | Format-List InfrastructureMaster, PDCEmulator, RIDMaster

```
PS C:\Windows\system32> Get-ADForest | Format-List DomainNamingMaster, SchemaMaster

DomainNamingMaster : InstructorDC.3mawdm.usmc.mil
SchemaMaster       : InstructorDC.3mawdm.usmc.mil

PS C:\Windows\system32> Get-ADDomain | Format-List InfrastructureMaster, PDCEmulator, RIDMaster

InfrastructureMaster : InstructorDC.3mawdm.usmc.mil
PDCEmulator         : InstructorDC.3mawdm.usmc.mil
RIDMaster           : InstructorDC.3mawdm.usmc.mil
```

PowerShell is the preferred method to relocate the FSMO roles. The cmdlet is `Move-ADDirectoryServerOperationMasterRole` and the parameters are listed in the screenshot below.



## Domain Controllers

```
PS C:\Windows\system32> help Move-ADDirectoryServerOperationMasterRole

NAME
    Move-ADDirectoryServerOperationMasterRole

SYNTAX
    Move-ADDirectoryServerOperationMasterRole [-Identity] <ADDirectoryServer> [-OperationMasterRole] {PDCEmulator |
    RIDMaster | InfrastructureMaster | SchemaMaster | DomainNamingMaster} [-WhatIf] [-Confirm] [-AuthType {Negotiate |
    Basic}] [-Credential <pscredential>] [-Force] [-PassThru] [-Server <string>] [<CommonParameters>]
```

An example of gracefully moving the roles is shown below.

```
Move-ADDirectoryServerOperationMasterRole -Identity
    <DestinationDC> -OperationMasterRole DomainNamingMaster,
    SchemaMaster, InfrastructureMaster, PDCEmulator, RIDMaster
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Move-ADDirectoryServerOperationMasterRole -Identity site2dc -OperationMasterRole DomainNamingMas
ter, SchemaMaster, InfrastructureMaster, PDCEmulator, RIDMaster

Move Operation Master Role
Do you want to move role 'DomainNamingMaster' to server 'Site2DC.3mawdm.usmc.mil' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Move Operation Master Role
Do you want to move role 'SchemaMaster' to server 'Site2DC.3mawdm.usmc.mil' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Move Operation Master Role
Do you want to move role 'InfrastructureMaster' to server 'Site2DC.3mawdm.usmc.mil' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Move Operation Master Role
Do you want to move role 'PDCEmulator' to server 'Site2DC.3mawdm.usmc.mil' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Move Operation Master Role
Do you want to move role 'RIDMaster' to server 'Site2DC.3mawdm.usmc.mil' ?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32>
```

Now all of the roles have been moved to the Site2DC.

```
PS C:\Windows\system32> Get-ADForest | Format-List DomainNamingMaster, SchemaMaster

DomainNamingMaster : Site2DC.3mawdm.usmc.mil
SchemaMaster       : Site2DC.3mawdm.usmc.mil

PS C:\Windows\system32> Get-ADDomain | Format-List InfrastructureMaster, PDCEmulator, RIDMaster

InfrastructureMaster : Site2DC.3mawdm.usmc.mil
PDCEmulator         : Site2DC.3mawdm.usmc.mil
RIDMaster           : Site2DC.3mawdm.usmc.mil
```

If, for whatever reason, a role needs to be seized, add a `-force` to the command.

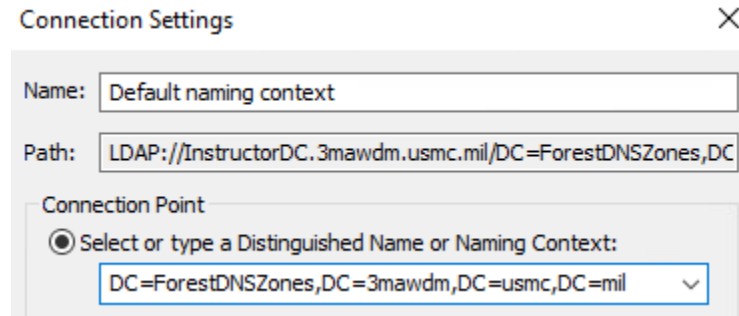
**Warning:** Never seize a role if unless the server hosting the role is unrecoverable. Once the role is seized, the original server hosting the role cannot be brought back online without causing issues.



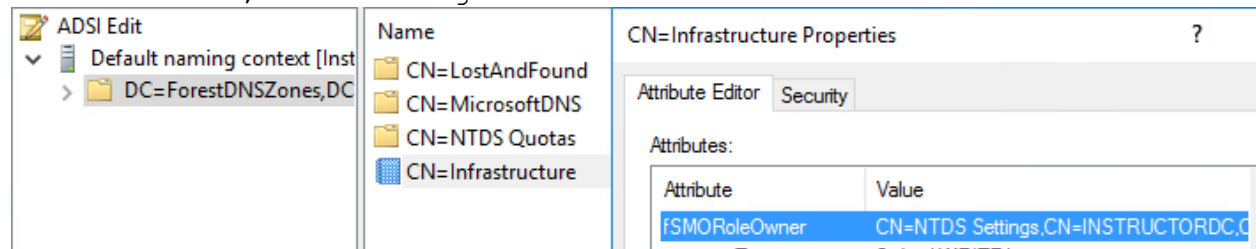
## Domain Controllers

Now remember the two other sub FSMO roles... the Forest DNS Zones Master and the Domain DNS Zones Master. Finding out which server holds them and relocating them are a bit more tricky. Open ADSI Edit, and connect to:

DC=ForestDNSZones,DC=<Domain>,DC=<TLD>

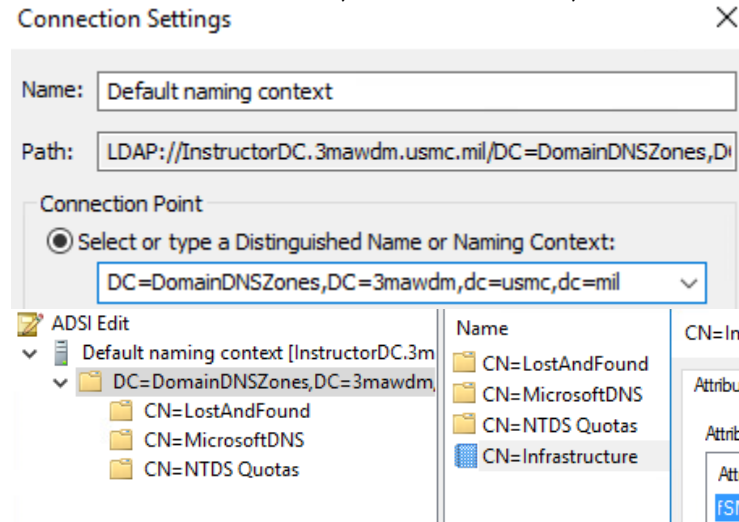


Double click on the CN=Infrastructure, and scroll down for the FSMO Role Owner. As seen below, it is still with the InstructorDC, even though the other roles were moved.



To connect to the DomainDNSZones use:

DC=DomainDNSZones,DC=<Domain>,DC=<TLD>





For each AD Application partition, there will be an Infrastructure Master. If the roles need to be moved, edit the settings reflect the new server, and let AD replicate the changes.

### User Principle Name (UPN) Suffix:

The UPN suffix is the piece which comes after the @ in the username; by default, it is just the namespace for your domain. Additional UPN suffix can be added. If two parties are claiming the same alternate UPN suffix, then a forest trust between those two entities will not work. A domain trust should still work.

To configure the alternate UPN suffix, open Active Directory Domains and Trusts. Right click on it, select properties.

Active Directory Domains and Trusts [ site2dc.3mawd... ? X

UPN Suffixes

The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

The alternate UPN suffix are primarily used to allow Token or Smart Card authentication via digital certificates. For example, the DoD uses the @mil UPN suffix for their tokens. This suffix has to be configured on the user accounts to enable the token authentication, which is why many entities add it to the alternate UPN suffix list. This has a tendency to cause issues with forest trusts. To resolve that issue, remove the common UPN suffix from the alternate list.

**Warning:** The best time to do this is when the forest is being built out. However, if can be done on a live network, complete the section below on adding the UPN suffix to an OU **first**.



Active Directory Domains and Trusts



Deleting a UPN suffix will affect user accounts that refer to it. Those users will not be able to log on to the network.

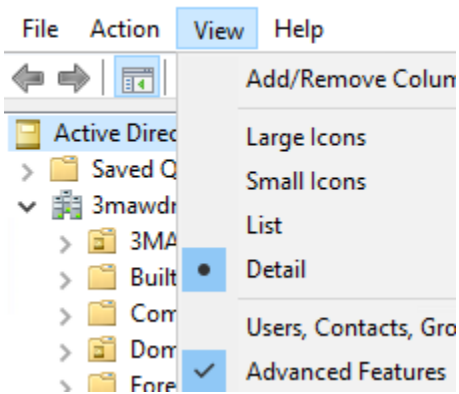
Are you sure you want to delete this UPN suffix?

Yes

No

To add a UPN suffix to an OU, open AD Users and Computers. Ensure you are viewing Advanced Features.

Active Directory Users and Computers



The UPN suffix will need to be added to each OU containing the user objects, as it is not inherited. Right click on the OU, properties, Attribute Editor tab, scroll down to the uPNSuffixes value, and add the UPN. The default value for this is <not set>. It is best practice to add the <domain> in addition to the desired UPN.

This picture shows a few different things, I have underlined each of the key window titles in green. It is a compilation of a couple different screen shots.

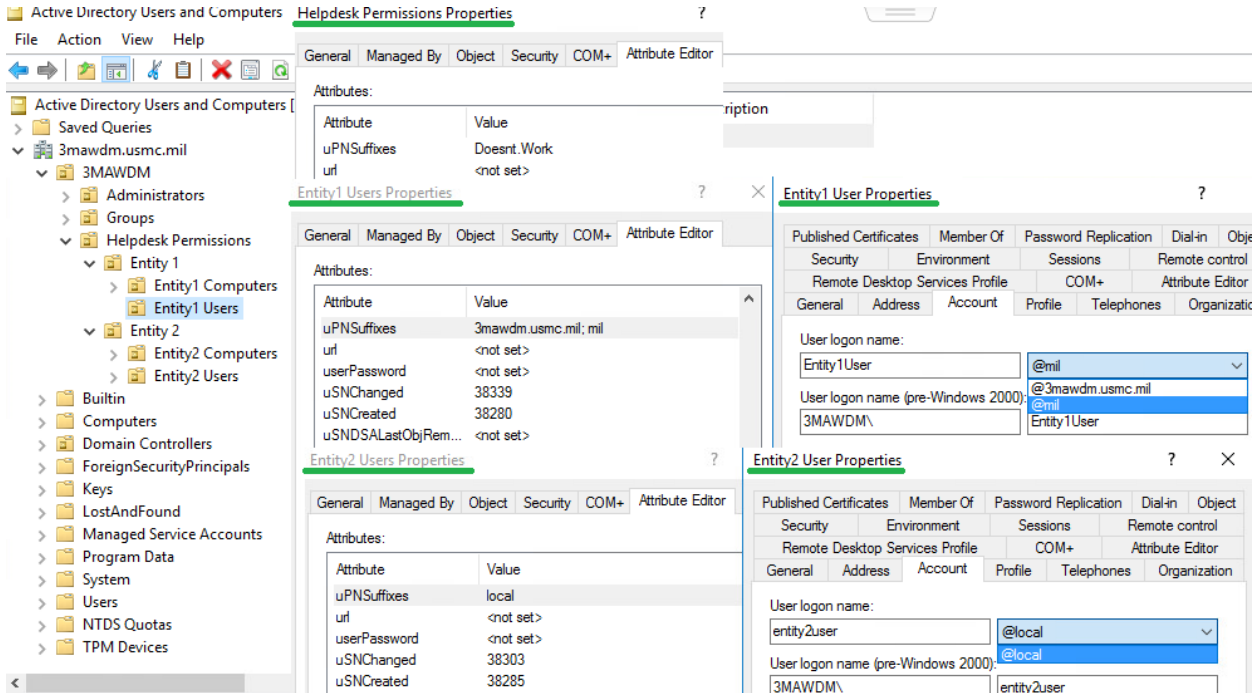
First, the AD Structure on the left, and the UPN suffix on the Helpdesk Permissions OU.

Second, the UPN suffix on the Entity1 Users OU, the UPN drop down on the Entity1 User account object.

Third, the UPN suffix on the Entity2 Users OU, the UPN drop down on the Entity2 User account object.



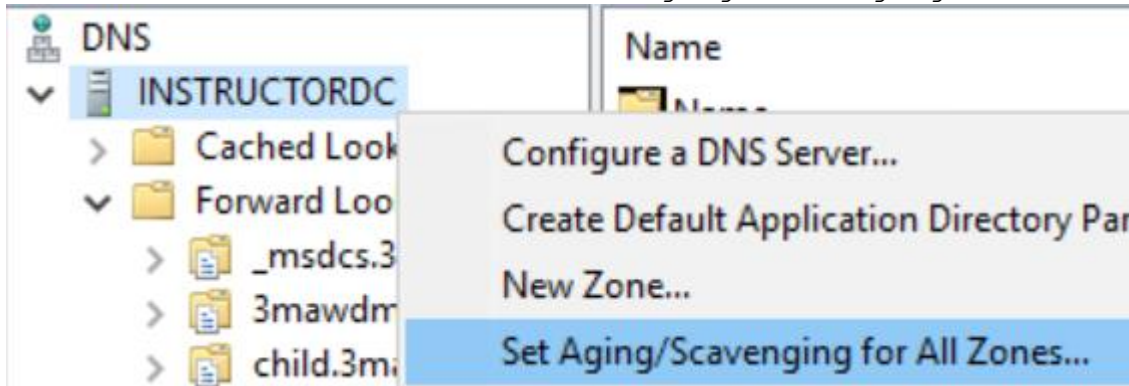
# Domain Controllers



## DNS Aging and Scavenging:

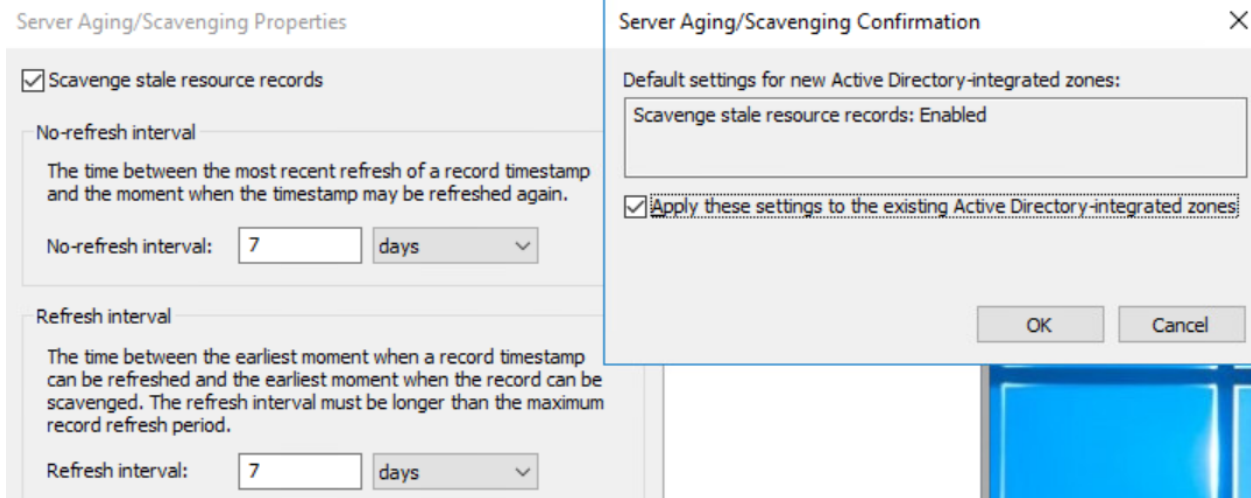
The dynamic DNS records, which are created when a machine joins the domain or receives an IP address via DHCP can sometimes become stale. The easiest way to resolve this is to enable your DNS servers to scavenge old records.

Open the DNS Manager and connect to your DNS server. Right click on the DNS server and select Set Aging/Scavenging for All Zones...

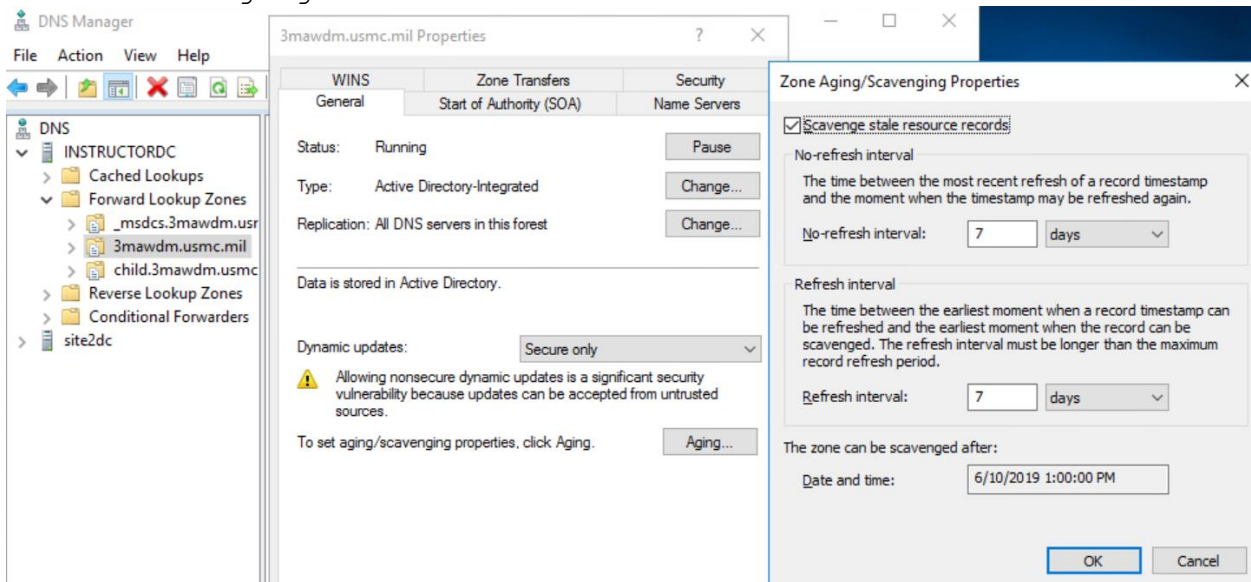


Check the box to enable Scavenging. The default values are fine for most situations.





The second step is to enable Scavenging on the Zone itself. The second window above may or may not pop up. To configure the zones, right click on the zone, Properties, on the General tab, select the Aging button near the bottom.



These settings are per DNS server. It is recommended to only scavenge a zone on a DNS server which is authoritative for it. For this parent / child domain relationship, the 3mawdm zone would be scavenged at the parent level. The child.3mawdm zone would be scavenged at the child level.

### Public Key Infrastructure (PKI) Script:

The following PowerShell script can be used to target specific OUs in Active Directory. It will forcibly Token Enforce all user



## Domain Controllers

accounts underneath that OU, provide a list of each user it enforced, and provide a count of how many users are enforced.

**Warning:** Adjust the script for your domain and test it before deploying it on a live, production forest. This script is provided as is. We bear no responsibility for any damage / outages caused due to misuse.

When this was written, PowerShell was and still is being learned. The lines could probably be broken apart better, but it is known to work as is. The Number and the : are to delineate lines which wrap. They are not part of the script. See the pictures.

```
1: $date = (get-date)
2: $OU = "OU=Helpdesk
Permissions,OU=3MAWDM,DC=3mawdm,DC=usmc,DC=mil"
3: $date >> C:\SmartCard_Check.txt
4: $OU >> C:\SmartCard_Check.txt
5: Get-ADUser -filter * -SearchBase $OU -Properties
'SmartcardLogonRequired' | Where-Object {
!($_.smartcardLogonRequired); (Set-ADUser $_ -
SmartcardLogonRequired $True) } | Select-Object
DistinguishedName >> C:\SmartCard_Check.txt
6: $SCEEnabledCount = 0
7: Get-ADUser -filter * -SearchBase $OU -Properties
'SmartcardLogonRequired' | Where-Object {
($_.smartcardLogonRequired) } | select-object DistinguishedName
| foreach {$SCEEnabledCount++}
8: "Smart Card Enabled:" >> C:\SmartCard_Check.txt
9: $SCEEnabledCount >> C:\SmartCard_Check.txt
```

A really small picture showing the full script:

```
//----->
//---Smart Card Required Checks--->
//--- v2.2 ----->
//--- Updated: 20181008 ----->
//----->

$date = (get-date)
$OU = "OU=Helpdesk Permissions,OU=3MAWDM,DC=3mawdm,DC=usmc,DC=mil"
$date >> C:\SmartCard_Check.txt
$OU >> C:\SmartCard_Check.txt
Get-ADUser -filter * -SearchBase $OU -Properties 'SmartcardLogonRequired' | Where-Object { !($_.smartcardLogonRequired); (Set-ADUser $_ -SmartcardLogonRequired $True) } | Select-Object DistinguishedName >> C:\SmartCard_Check.txt
$SCEEnabledCount = 0
Get-ADUser -filter * -SearchBase $OU -Properties 'SmartcardLogonRequired' | Where-Object { ($_.smartcardLogonRequired) } | select-object DistinguishedName | foreach {$SCEEnabledCount++}
"Smart Card Enabled:" >> C:\SmartCard_Check.txt
$SCEEnabledCount >> C:\SmartCard_Check.txt
```

A picture showing the left half:



\_Smart Card Required Check Commands v2.2.txt - Notepad

File Edit Format View Help

```
//----->
//---Smart Card Required Checks--->
//--- v2.2 ----->
//--- Updated: 20181008 ----->
//----->

$date = (get-date)
$OU = "OU=Helpdesk Permissions,OU=3MAWDM,DC=3mawdm,DC=usmc,DC=mil"
$date >> C:\SmartCard_Check.txt
$OU >> C:\SmartCard_Check.txt
Get-ADUser -filter * -SearchBase $OU -Properties 'SmartcardLogonRequired' | Where-Object {
$SCEntabledCount = 0
Get-ADUser -filter * -SearchBase $OU -Properties 'SmartcardLogonRequired' | Where-Object {
"Smart Card Enabled:" >> C:\SmartCard_Check.txt
$SCEntabledCount >> C:\SmartCard_Check.txt
```

A: picture showing the right half with the two long lines:

```
!($_.smartcardLogonRequired); (Set-ADUser $_ -SmartcardLogonRequired $True) } | Select-Object DistinguishedName >> C:\SmartCard_Check.txt

($_.smartcardLogonRequired) } | select-object DistinguishedName | foreach {$SCEntabledCount++}
```

The walkthrough.

**Line 1**, get the current date and time.

**Line 2**, set the specific OU to target, it will also target anything underneath this OU.

**Lines 3 and 4**, append the date and OU to the file on the C:\.

**Line 5**, search AD for all user objects and their Smartcard Logon Required values. Send it to the check, where the value is not true, set it to true and grab the user's OU and account name, append the information to the file on the C:\.

**Line 6**, create a variable and set it to 0.

**Line 7**, search AD for all user objects and add 1 to the variable for each one that is Smartcard enabled.

**Lines 8 and 9**, append the count to the file on the C:\.

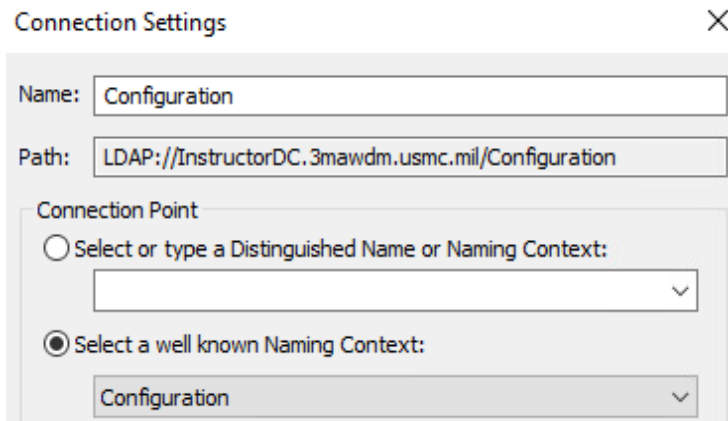
The environment where this script was written for required all user accounts, with very few exemptions to be Smartcard enabled. Administrators from different entities were responsible for creating their own user accounts, and occasionally would "forget" to Smartcard enable them. The script was ran once per shift and tracked the information. Because of the structure, of the OUs, it was easy to tell which user account belonged to which entity and their administrators were contacted with the information. If the desired result is to just check and get a count of who is not Smartcard enabled, and not enforce it, remove the: (Set-ADUser \$ -SmartcardLogonRequired \$True).



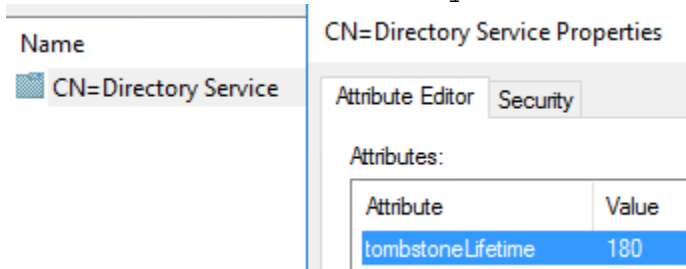
## Active Directory Tombstone:

The Tombstone value in Active Directory, as it relates to domain controllers, is how long they can be disconnected from the rest of the forest. It also determines how long your backup is valid for. The backup cannot be older than the tombstone value. In most corporate networks, this is not an issue, and there is no reason to change the default values. However, when you shut down your servers, physically ship them somewhere, expecting to power them on, say 120 days later, and work flawlessly; it may come into effect. At the least, the next section on DFSR and the SYSVOL will.

To check the current value and to make changes, open ADSI Edit and connect to the Configuration partition. (Dropdown in the middle, with a radio button.)



Expand CN=Configuration, expand CN=Services, click on CN=Windows NT. Underneath here is the CN=Directory Service. Right click on it and select properties. Scroll down to the tombstoneLifetime attribute. If the value is <not set>, the default is 60 days. When the first domain controller in this forest was promoted, it set the value to 180 days with this version of Server 2016.



Due to the example listed above, we will change the value to 730, which is the equivalent of 2 years. There are drawbacks to





doing this. The database will retain all of the older, deleted information for a much longer time. After several years, depending on how heavily the domain is used, it can cause the domain controllers to bloat in disk size.

## Distributed File System Replication (DFSR) and the SYSVOL:

Now that we have changed value on the tombstone above, we need to adjust the DFSR values. By default, the stale time is 60 days. After 60 days, it will mark its information as stale. After it is marked as stale, it will not replicate the information and the replication link will need to be rebuilt by an administrator. The SYSVOL contains all of the information regarding Group Policy, and needs to be consistent across the domain.

If you noticed, the default of 60 days is less than the default tombstone of 180 days. For the example of shipping the servers listed above, even if the tombstone lifetime isn't changed, DFSR would cause severe issues.

To change the DFSR time and to set DFS to use DNS, on the domain controller, open PowerShell or a command prompt as an administrator. The third command is the only one which will require PowerShell.

(The following is a single command)  
wmic.exe /namespace:\\root\microsofdfs path DfsrMachineConfig  
set MaxOfflineTimeInDays=730

To set DFS to use DNS, we run the following two commands:  
dfsutil.exe server registry dfsdnsconfig set <servername>  
and (The following is a single command.)  
Set-DfsnServerConfiguration -ComputerName <servername>  
-UseFQDN \$true





```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> wmic.exe /namespace:\\root\microsoftdfs path DfsrMachineConfig set MaxOfflineTimeInDays=730
Updating property(s) of '\\INSTRUCTORDC\root\microsoftdfs:DfsrMachineConfig=@'
Property(s) update successful.
PS C:\Windows\system32>
PS C:\Windows\system32> dfsutil.exe server registry dfsdnsconfig set InstructorDC

Done processing this command.
PS C:\Windows\system32>
PS C:\Windows\system32> Set-DfsnServerConfiguration -ComputerName InstructorDC -UseFqdn $true

ComputerName           : InstructorDC
LdapTimeoutSec         : 30
PreferLogonDC          : False
EnableSiteCostedReferrals : True
EnableInsiteReferrals  : False
SyncIntervalSec        : 3600
UseFqdn                : True

PS C:\Windows\system32>
```

**Extra:** If DFSR is used between file servers elsewhere, the default is still 60 days. If a DFS Namespace is used elsewhere, by default it does not use DNS. These commands can be ran on each of those machines to adjust the settings as desired.

### Active Directory Recycle Bin:

The Active Directory Recycle Bin is a feature which will allow an administrator to restore a deleted object. Some of the more advanced features such as Microsoft's BitLocker and Local Admin Password Solution (LAPS) can be configured to store information in Active Directory. If a Computer account was "accidentally" deleted, it can be restored to retrieve the information. If an administrator "accidentally" deleted an OU containing half of the user accounts while cleaning up Active Directory, they can also be restored.

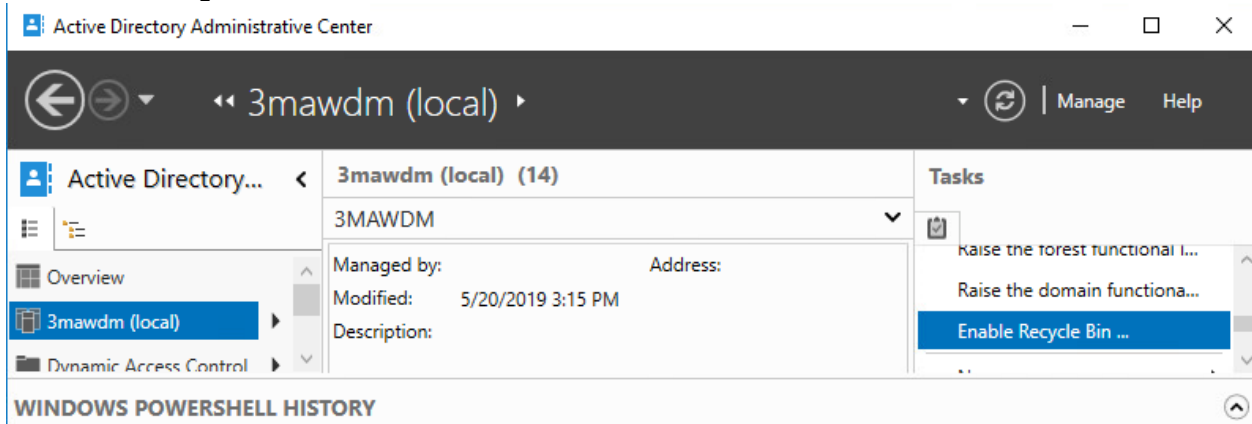
By default, the AD Recycle Bin is not enabled. Once it is enabled for the forest, it cannot be disabled. To enable it, the Domain Naming Master and Schema Master roles need to exist on the same domain controller. The reason it cannot be disabled is the schema is changed when it is enabled.

A good saying which was found on the internet: There are two types of administrators. Those who enable the AD Recycle Bin before something is accidentally deleted, and those who enable after something is accidentally deleted.



## Domain Controllers

Open the Active Directory Administration Center, on the left, select the domain, on the right side, scroll down and click the Enable Recycle Bin link.



Click ok, acknowledging that it cannot be disabled.

### Enable Recycle Bin Confirmation



Are you sure you want to perform this action? Once Recycle Bin has been enabled, it cannot be disabled.

### Active Directory Administrative Center



Please refresh AD Administrative Center now.

AD DS has begun enabling Recycle Bin for this forest. The Recycle Bin will not function reliably until all domain controllers in the forest have replicated the Recycle Bin configuration change.

Now the Recycle Bin is enabled for the forest. The information will replicate throughout the domain, based on the replication structure of your forest.

### Time:

Time and the system clocks are very important in a forest. By default, the maximum tolerance for computer clock synchronization is 5 minutes.

By default the domain controller holding the PDC role becomes the timing master. The PDC in the root of the forest passes the time to the other domain controllers that are part of its domain, who then pass time to the clients.



## Domain Controllers

The PDC for each child domain, will get its time from the forest root PDC, pass the time to the rest of the domain controllers in its child domain, which will then pass the time to the clients.

We say by default, because through group policy, you can specify a specific NTP server and have every device check there for time. The domain controllers are an NTP server, should a third party (i.e. router, switch, etc.) need time from an external source.

To view the current status and the configuration, w32tm is used.  
w32tm /query /status

```
C:\Windows\system32>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0034777s
Root Dispersion: 10.9995395s
ReferenceId: 0xAC1E0012 (source IP: 172.30.0.18)
Last Successful Sync Time: 5/22/2019 3:35:01 PM
Source: Site2DC.3mawdm.usmc.mil
Poll Interval: 10 (1024s)
```

w32tm /query /configuration

It will produce a list, near the bottom, the important line is  
Type: NT5DS.

```
SpecialPollInterval: 3600 (Local)
Type: NT5DS (Local)
```

This line means the system, whether it is another server, or a workstation is set to use the Domain Hierarchy as its time source.

Before an external time source is configured, it is advised to check the time source, to ensure it is accessible and providing valid time. The command to do that is:

w32tm /stripchart /computer:<ntp.fqdn> /dataonly /samples:<#>  
The /packetinfo as show below can be added to show additional information.



## Domain Controllers

```
Administrator: Command Prompt
C:\Windows\system32>w32tm /stripchart /computer:Site2DC.3mawdm.usmc.mil /dataonly /samples:1 /packetinfo
Tracking Site2DC.3mawdm.usmc.mil [172.30.0.18:123].
Collecting 1 samples.
The current time is 5/22/2019 3:35:05 PM.
15:35:05, -00.0005661s
[NTP Packet]
Leap Indicator: 0(no warning)
Version Number: 3
Mode: 4 (Server)
Stratum: 2 (secondary reference - syncd by (S)NTP)
Poll Interval: 0 (unspecified)
Precision: -23 (119.209ns per tick)
Root Delay: 0x0000.007B (+00.0018768s)
Root Dispersion: 0x000A.FA58 (10.9779053s)
ReferenceId: 0xAC1E0003 (source IP: 172.30.0.3)
Reference Timestamp: 0xE0904ABB7D843F95 (152812 22:24:59.4902992s - 5/22/2019 3:24:59 PM)
Originate Timestamp: 0xE0904D1941A8B4BF (152812 22:35:05.2564805s - 5/22/2019 3:35:05 PM)
Receive Timestamp: 0xE0904D19419C8AE5 (152812 22:35:05.2562949s - 5/22/2019 3:35:05 PM)
Transmit Timestamp: 0xE0904D19419CE3D0 (152812 22:35:05.2563002s - 5/22/2019 3:35:05 PM)
[non-NTP Packet]
Destination Timestamp: Roundtrip Delay: 761100 (+00.0007611s)
Local Clock Offset: -566100 (-00.0005661s)

C:\Windows\system32>w32tm /stripchart /computer:Site2DC.3mawdm.usmc.mil /dataonly /samples:2
Tracking Site2DC.3mawdm.usmc.mil [172.30.0.18:123].
Collecting 2 samples.
The current time is 5/22/2019 3:35:43 PM.
15:35:43, -00.0003183s
15:35:45, -00.0002908s
```

Due to the maximum time skew, it is recommended that only the forest root PDC sync time from an external source, and everything else be left at the default of using the domain hierarchy.

To configure an external time source, w32tm is also used. For this lab, there is no external connection, so the configuration will be academic only. The command is: (Single command.)  
w32tm /config /manualpeerlist:"ntp1.fqdn,0x8 ntp2.fqdn,0x8"  
/syncfromflags:MANUAL /reliable:yes /update

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>w32tm /config /manualpeerlist:"ntp1.fqdn,0x8 ntp2.fqdn,0x8" /syncfromflags:MANUAL /reliable:yes /update
The command completed successfully.
```

w32tm now shows a different configuration for SiteDC2.

```
SpecialPollInterval: 3600 (Local)
Type: NTP (Local)
NtpServer: ntp1.fqdn,0x8 ntp2.fqdn,0x8 (Local)
```

When running the command, the /config tells it to change its settings. /manualpeerlist: is a space separated list of NTP



## Domain Controllers

servers, each followed by a ",0x8". To specify multiple servers, encase them in quotes like the example. /syncfromflags: has two modes, either MANUAL because an external time source is being specified, or DOMHIER to use the domain's time. /reliable: sets the machine to be a reliable time source. /update: notifies the time service there have been changes, causing the changes to take effect.

Time configuration can be automated with a GPO and a WMI filter. The WMI filter is used to target the domain controller holding the PDC Emulator role, the GPO is used to configure the time.

Using PowerShell to determine domain roles.

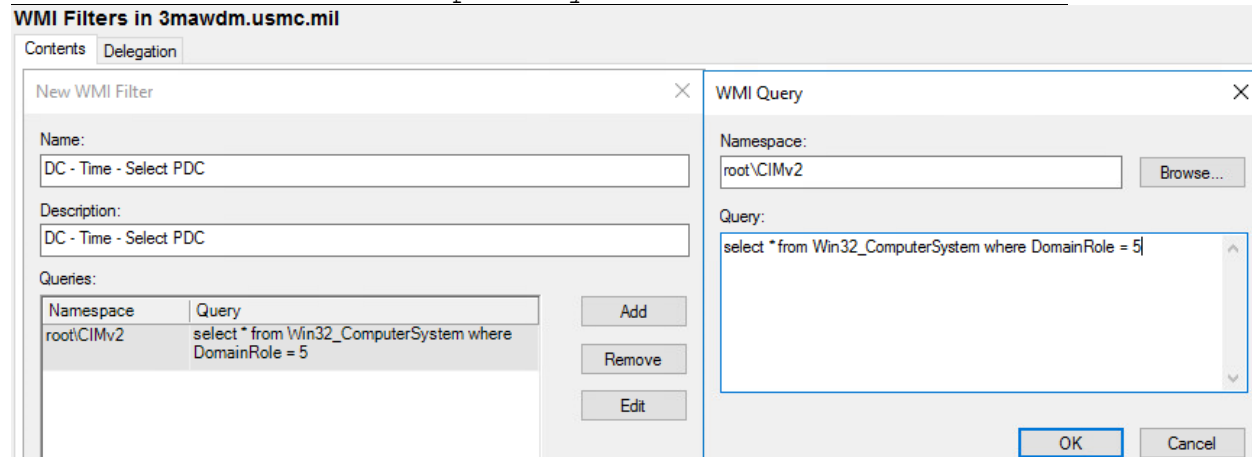
```
PS C:\Windows\system32> Get-WmiObject Win32_ComputerSystem | Select-Object -ExpandProperty DomainRole
4
PS C:\Windows\system32> Get-WmiObject -ComputerName site2dc.3mawdm.usmc.mil Win32_ComputerSystem | select-object -ExpandProperty DomainRole
5
PS C:\Windows\system32> _
```

Domain Role value meaning:

- 0: Standalone Workstation
- 1: Member Workstation
- 2: Standalone Server
- 3: Member Server
- 4: Domain Controller
- 5: Primary Domain Controller

Open Group Policy Management and select the WMI folder. Create a new WMI filter with the query:

```
select * from Win32_ComputerSystem where DomainRole = 5
```



## Domain Controllers

- > Domain Controllers
- > Group Policy Objects
- ▼ WMI Filters
  - DC - Time - Select PDC
- > Starter GPOs

For the group policy objects, there will only be one for the PDC.

**Side Note:** By default, all domain joined machines use the DOMHIER or NT5DS time source and get their time from the PDC. If the time settings have been manually configured (as above), the command to revert them to the default is:  
w32tm /config /manualpeerlist:peers /syncfromflags:DOMHIER /update

Create a new GPO. The settings are located under Computer Configuration \ Administrative Templates \ System \ Windows Time Service \ Time Providers

Set the Enable Windows NTP Client to enabled.  
Enable Configure Windows NTP Client.

For the settings, the NTP server block is the same as setting it manually above. <ntp1.fqdn>,0x9 <ntp2.fqdn>,0x9  
Change the type to NTP.

NtpServer	ntp1.fqdn,0x9 ntp2.fqdn,0x9
Type	NTP
CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	3600

**SpecialPollInterval**  
This NTP client value, expressed in seconds, controls how often a manually configured time source is polled when the time source is configured to use a special polling interval. If the SpecialInterval flag is enabled on the NTPServer setting, the client uses the value that is set as the SpecialPollInterval, instead of the MinPollInterval and MaxPollInterval values, to determine how frequently to poll the time source. The default value is 3600 seconds (1 hour).

**EventLogFlags**  
This value is a bitmask that controls events that may be logged to the System log in Event Viewer. Setting this value to 0x1

Why 0x9? There are four bitmask values which can be combined.  
0x01 SpecialInterval (Description on the right side of picture.)  
0x02 UseAsFallbackOnly  
0x04 SymmetricActive \*\*  
0x08 Client

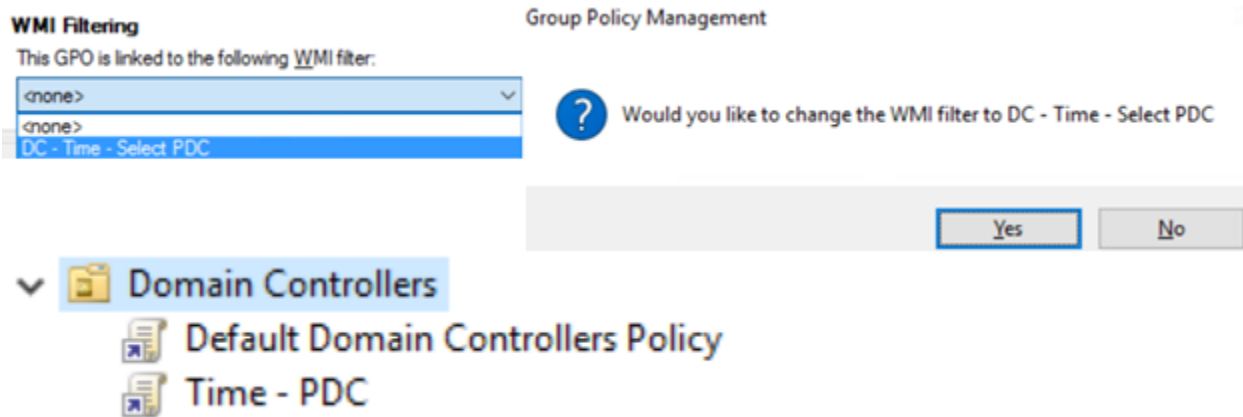
\*\* Get time from a source, and provide time to that source.



## Domain Controllers

For this configuration, 0x9 was used, to combine 0x8 and 0x1. Another common configuration is 0xa. Using the fallback setting will tell the server to all other time sources before you try this one.

Once the settings on the GPO are configured, double click it, and at the bottom, under WMI Filtering, select the filter and click Yes acknowledging you would like to change the WMI filter on the GPO.



If the time on the PDC changes, while the domain is powered on, replication will break for a couple of hours. This is due to all of the domain controllers being out of sync. They should come back into sync when they query to get the time from the PDC. To manually sync the time on each server, the following command can be used. w32tm /resync /force

## Preventing Standard Users from Joining Computers to the Domain:

With Microsoft's default settings, an Authenticated User can join up to 10 computers to the domain. While there may be some benefit to this, in a controlled environment, it is undesirable. There are two basic methods to prevent this from happening. We recommend both be put into place.

**Preface:** There are very few settings which require modifying the default domain or the default domain controllers policy. Unless it is one of those specific settings, it is always best to create a new GPO with a description of what it is doing.

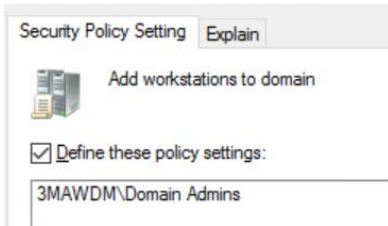


## Domain Controllers

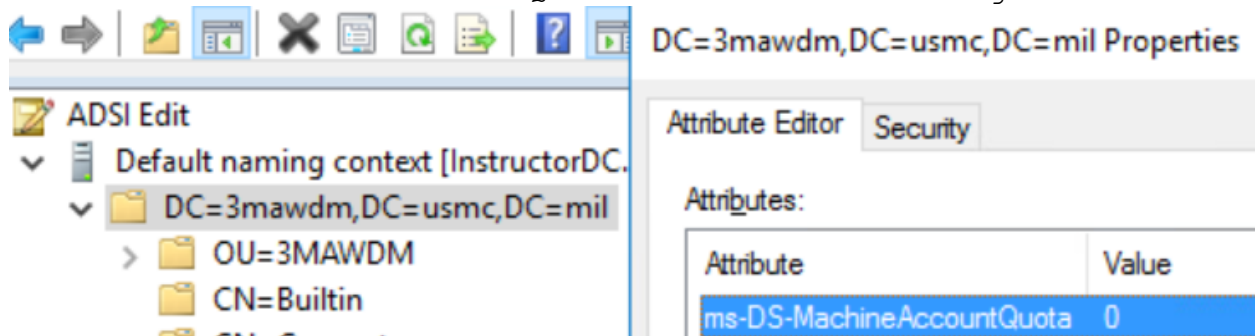
First, the Default Domain Controllers Policy.

Open Group Policy Management Editor, and edit the Default Domain Controllers Policy. The setting will be under, Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ User Rights Assignment. The setting to change is "Add workstations to domain". Remove Authenticated Users and add Domain Admins.

Add workstations to domain Properties



The second method is to change the ms-DS-MachineAccountQuota. Open ADSI Edit, and connect to the Default Naming Context. Right click on the DC=<domain>,DC=<TLD>, and select edit. Scroll down to the ms-DS-MachineAccountQuota attribute and change it to 0.



This quota does not apply to domain admins. This will force other administrators to create the computer account in Active Directory before they are able to attach a computer to said account.

**Note:** These settings are per domain. Because there is a child domain, they will need to be done twice. Once to prevent users from adding computers to the parent domain, once to prevent users from adding computers to the child domain.

### Replication:

One of the more popular questions we receive from end users is: Why do I have to wait <x> amount of time, then log off and log back on? Why doesn't it take affect now?

The usual answer, replication.



Jade Falcon LLC



## Domain Controllers

Depending on the replication topology and schedule, a change made within Active Directory can take a few minutes, a few hours, or maybe a few days to replicate across the forest. The change made to prevent users from joining workstations to the domain, could take a day to replicate across a forest spread around a country or the globe.

What if we wanted to pull everything into sync, all at once?

repadmin /syncall /<options> <Target DC FQDN>

This command will cause the current domain controller to sync with its partners. If we add a ? to the options, we get a list.

```
C:\Windows\system32>repadmin /syncall /?
DsReplicaSyncAll commandline interface.
repadmin /SyncAll [/adehijpPsS] <Dest DSA> [<Naming Context>]
/a: Abort if any server is unavailable
/A: Perform /SyncAll for all NC's held by <Dest DSA> (ignores <Naming Context>)
/d: ID servers by DN in messages (instead of GUID DNS)
/e: Enterprise, cross sites (default: only home site)
/h: Print this help screen
/i: Iterate indefinitely
/I: Perform showreps on each server pair in path instead of syncing
/j: Sync adjacent servers only
/p: Pause for possible user abort after every message
/P: Push changes outward from home server (default: pull changes)
/q: Quiet mode, suppress callback messages
/Q: Very quiet, report fatal errors only
/s: Do not sync (just analyze topology and generate messages)
/S: Skip initial server-response check (assume all servers are available)
If <Naming Context> is omitted DsReplicaSyncAll defaults to the Configuration NC.
```

The two sets of options we will be focusing on are /edA and /ePdA. The options can be placed in any order. This particular order was how it was learned and memorized by us. Once again, a domain controller can be targeted by adding it to the end of the command.

d: Identify DC via name instead of GUID.

With d:

```
From: CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
To : CN=NTDS Settings,CN=INSTRUCTORDC,CN=Servers,CN=Site1,CN=Sites,CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
From: CN=NTDS Settings,CN=SITE2DC,CN=Serv
To : CN=NTDS Settings,CN=INSTRUCTORDC,CN
```

Without d:

```
From: 1254b9b1-1f7b-4186-8bb6-2f0442be05a8._msdcs.3mawdm.usmc.mil
To : f2b6d5b8-aef4-46ad-afe4-d8ca98f49edb._msdcs.3mawdm.usmc.mil
```



Jade Falcon LLC

## Domain Controllers

e: Will cause the replication to occur at every AD site.

A: Without A, a partition will need to be specified, with A, it will sync all partitions held.

The difference, without the **P**, it means pull the current AD information from its partners. With the **P** it will push the AD information from this domain controller to its partners.

Without P, it starts the replication at the distant end, and works its way back towards the target. Without P:

```
Syncing partition: CN=Schema,CN=Configuration,DC=3mawdm,DC=usmc,DC=
CALLBACK MESSAGE: The following replication is in progress:
  From: CN=NTDS Settings,CN=CHILDDC,CN=Servers,CN=ChildSite1,CN=S
  To : CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,
CALLBACK MESSAGE: The following replication completed successfully:
  From: CN=NTDS Settings,CN=CHILDDC,CN=Servers,CN=ChildSite1,CN=S
  To : CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,
CALLBACK MESSAGE: The following replication is in progress:
  From: CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,
  To : CN=NTDS Settings,CN=INSTRUCTORDC,CN=Servers,CN=Site1,CN=S
CALLBACK MESSAGE: The following replication completed successfully:
  From: CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,
  To : CN=NTDS Settings,CN=INSTRUCTORDC,CN=Servers,CN=Site1,CN=S
```

Sync ChildDC to Site2DC, then Site2DC to InstructorDC.

With P, it starts at the target, and works its way toward the distant ends of the forest. With P:

```
Syncing partition: CN=Schema,CN=Configuration,DC=3mawdm,DC=usmc,DC=n
CALLBACK MESSAGE: The following replication is in progress:
  From: CN=NTDS Settings,CN=INSTRUCTORDC,CN=Servers,CN=Site1,CN=Si
  To : CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,C
CALLBACK MESSAGE: The following replication completed successfully:
  From: CN=NTDS Settings,CN=INSTRUCTORDC,CN=Servers,CN=Site1,CN=Si
  To : CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,C
CALLBACK MESSAGE: The following replication is in progress:
  From: CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,C
  To : CN=NTDS Settings,CN=CHILDDC,CN=Servers,CN=ChildSite1,CN=Si
CALLBACK MESSAGE: The following replication completed successfully:
  From: CN=NTDS Settings,CN=SITE2DC,CN=Servers,CN=Site2,CN=Sites,C
  To : CN=NTDS Settings,CN=CHILDDC,CN=Servers,CN=ChildSite1,CN=Si
```

Sync InstructorDC to Site2DC, then Site2DC to ChildDC.



## KDS Root Key and Managed Service Accounts:

Some services, such as MSSQL, will allow a proper AD Managed Service account to be used. Unlike the DHCP service account, these accounts are controlled by Active Directory. In order to create a managed service account, the KDS root key must exist.

By default, the key cannot be used for 10 hours after it is created. This time frame is to allow it to replicate across the topology.

The PowerShell cmdlets to view and create the root key are Get-KdsRootKey and Add-KdsRootKey.

Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

```
PS C:\Windows\system32> Get-KdsRootKey
PS C:\Windows\system32> Add-kdsRootKey -EffectiveTime (get-date).AddHours(-10)

Guid
----
6650acb1-0d61-ff40-e2e7-66828eccc9ab

PS C:\Windows\system32> Get-KdsRootKey

AttributeOfWrongFormat :
KeyValue                 : {158, 64, 190, 26...}
EffectiveTime            : 6/2/2019 10:34:35 PM
CreationTime             : 6/3/2019 8:34:35 AM
IsFormatValid           : True
DomainController         : CN=SITE2DC,OU=Domain Controllers,DC=3mawdm,DC=usmc,DC=mil
ServerConfiguration      : Microsoft.KeyDistributionService.Cmdlets.KdsServerConfiguration
KeyId                    : 6650acb1-0d61-ff40-e2e7-66828eccc9ab
VersionNumber            : 1
```

Even though we bypassed the default 10 hour wait, every domain controller in the forest still needs to know about it.  
repadmin /syncall /ePdA

With a KDS root key pushed throughout the forest, we can create Active Directory Managed Service Accounts.

**Notes:** A server with the name MemberServer has been deployed and joined to the domain for this example. The Microsoft Windows Server 2016 baseline template used only permits AES 128 and AES 256 Kerberos encryption types. If a default install of Server 2016 is used, the -KerberosEncryptionType option may be different than the example used.

The cmdlet used is New-ADServiceAccount.



## Domain Controllers

```
New-ADServiceAccount -Name svc.MbrSvrSvc  
-DNSHostName svc.MbrSvrSvc.3mawdm.usmc.mil  
-KerberosEncryptionType AES128,AES256  
-PrincipalsAllowedToRetrieveManagedPassword  
MemberServer$
```




```
PS C:\> New-ADServiceAccount -Name svc.MbrSvrSvc -DNSHostName svc.MbrSvrSvc.3mawdf.usmc.mil -KerberosEncryptionType AES128,AES256 -PrincipalsAllowedToRetrieveManagedPassword MemberServer$
```

The name must be 15 characters or less. The DNS name should be the <name>.FQDN where the account is being created. The encryption types specified must be available from the domain controllers. Principals allowed to retrieve managed password is where you let AD know which computer(s) are allowed to use this account. AD will store the password for the account, and will only give that password to the computers on the list. The computer names listed need to end in a \$.

To see which service accounts exist,  
Get-ADServiceAccount -Filter \*

```
PS C:\> Get-ADServiceAccount -Filter *  
  
DistinguishedName : CN=svc.MbrSvrSvc,CN=Managed Service Accounts,DC=3mawdm,DC=usmc,DC=mil  
Enabled           : True  
Name              : svc.MbrSvrSvc  
ObjectClass       : msDS-GroupManagedServiceAccount  
ObjectGUID        : 08b2ba0f-d892-45a8-8c29-8a1eac820ff3  
SamAccountName    : svc.MbrSvrSvc$  
SID               : S-1-5-21-2077987980-2596416506-3176031181-1604  
UserPrincipalName :
```

The account was created under the Managed Service Accounts OU, underneath the domain in AD Users and Computers.

>  LostAndFound	Name	Type
>  Managed Service Accounts	svc.MbrSvrSvc	msDS-GroupManagedServiceAccount
>  Program Data		

On MemberServer, we will install and test the newly built service account to ensure it is functioning. It is recommended to test the access to the service account before trying to associate it to any service, to eliminate the possibility of there being a typo somewhere causing errors.

The steps for this are, locate the service account we desire using the Get-ADServiceAccount cmdlet above. Add it to a variable. Install-ADServiceAccount and then Test-ADServiceAccount.





```
PS C:\> $SvcAct = Get-ADServiceAccount svc.MbrSvrSvc
PS C:\> Install-ADServiceAccount $SvcAct
PS C:\> Test-ADServiceAccount svc.MbrSvrSvc
True
PS C:\>
```

When this sequence is ran on the MemberServer, it returns True. This means the MemberServer can access the password for the account and it is working.

When the test is ran against one of the domain controllers, it returns False, with an error.

```
PS C:\> Test-ADServiceAccount svc.mbrsvrsvc
False
WARNING: Test failed for Managed Service Account svc.MbrSvrSvc. If standalone Managed Service Account, the account is linked to another computer object in the Active Directory. If group Managed Service Account, either this computer does not have permission to use the group MSA or this computer does not support all the Kerberos encryption types required for the gMSA. See the MSA operational log for more information.
PS C:\>
```

## Granting Permissions:

AGDLP

Accounts go into Global Groups.  
Global Groups go into Domain Local Groups.  
Permissions get applied to Domain Local Groups.

There is a variation on this one for large organizations, AGUDLP. This involves using a Universal group.

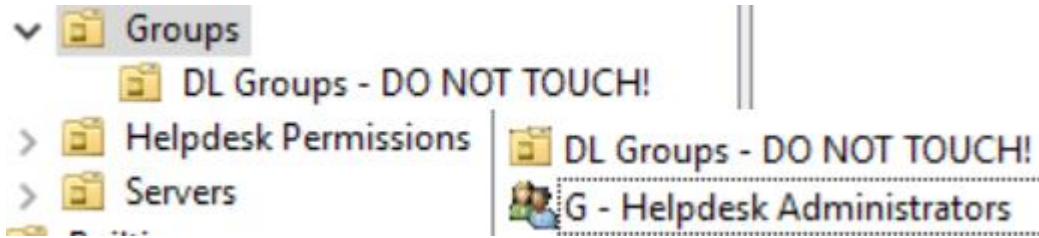
So these groups, what are they?  
The names can be a little confusing.

Global groups can only contain objects from the local domain, but can be granted permissions Globally.

Domain Local groups can contain objects from other domains, but can only be granted permissions in the Local Domain.

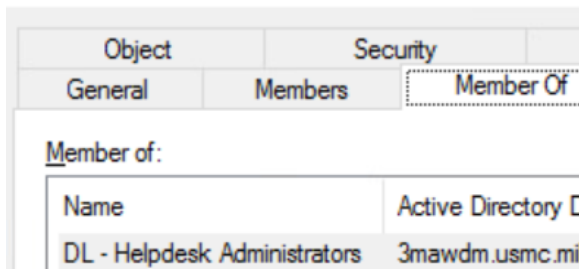
Our preference for the naming standard is to start the global groups with a "G - " and the domain local groups with a "DL - " to assist with searching. Descriptive names help.





Here we have a global group named Helpdesk Administrators. It is a member of a domain local group by the same name.

**G - Helpdesk Administrators Properties**

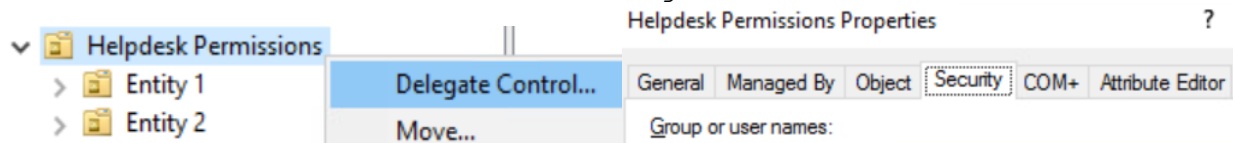


We are going to grant permissions over the "Helpdesk Permissions" OU to the domain local group. The administrators will be members of the global group.

**Note:** Each organization has its own guidelines on which permissions should be granted and to whom. This is the basic permission set we grant to the Helpdesk, which covers each entity.

There are two ways of granting permissions to an OU. The first is to right click the OU, and select Delegate Control. Walk through the wizard and viola, permissions granted.

The second is to right click, select properties, go to the Security tab, and specify the permissions manually. This is the method we will show as it is more granular.



Owner Rights. When someone creates an object, they "own" that object. If they are denied permissions to that object, they can take back their control over the object because they "own" it. To prevent this from happening, Microsoft has created Owner



Rights. The permissions applied to this override the Creator Owner permission set. Our first step is to add Owner Rights to the top level OU, and grant it read only permissions.

The screenshot shows the Active Directory console with the '3MAWDM Properties' dialog box open. The 'Security' tab is selected. In the 'Group or user names' list, 'OWNER RIGHTS' is highlighted. Below the list are 'Add...' and 'Remove' buttons. A table titled 'Permissions for OWNER RIGHTS' shows the following permissions:

Permissions for OWNER RIGHTS	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>

Ensure you go into the Advanced and change the second drop down to This object and all descendant objects...

**Permission Entry for 3MAWDM**

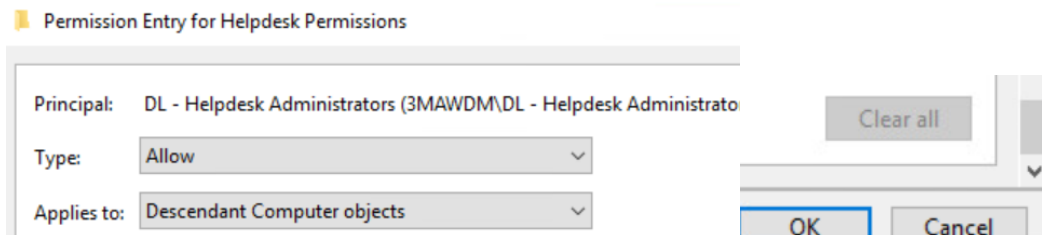
The screenshot shows the 'Permission Entry for 3MAWDM' dialog box with the following settings:

- Principal: OWNER RIGHTS [Select a principal](#)
- Type: Allow
- Applies to: This object and all descendant objects

Next, we will go to the properties of the Helpdesk Permissions OU, Security tab, Advanced. Click add, select the DL - Helpdesk Administrators.

Change the second drop down to Descendant Computer objects. Scroll all the way to the bottom and click the clear all button.





The permissions we are going to grant over computer objects are:

- List contents (left side)
- Read all properties (left side)
- Write all properties (left side)
- Read permissions (left side)
- All validated writes (left side)
- Reset password (right side)
- Validated write to computer attributes (right side)
- Validated write to DNS host name (right side)
- Validated write to MS DS Additional DNS Host Name (right side)
- Validated write to service principle name (right side)

Click ok, apply, then add.

Applies to:

Descendant User objects. (Clear all)

- List contents (L)
- Read all properties (L)
- Write all properties (L)
- Read permissions (L)
- All validated writes (L)
- All extended rights (L)
- Create ms-net-ieee... (both, R)
- Allowed to authenticate (R)
- Change password (R)
- Receive as (R)
- Reset password (R)
- Send as (R)

Click ok, apply, add.

Principal: DL - Helpdesk Administrators (3MAWDM\DL - Helpd

Type:

Applies to:

Descendant OU objects. (Clear all)

- List contents (L)
- Read all properties (L)
- Write all properties (L)





- Read permissions (L)
- All validated writes (L)

Click ok, apply, add.








Applies to: **Descendant Group objects**

Descendant Group objects. (Clear all)

- List contents (L)
- Read all properties (L)
- Write all properties (L)
- Read permissions (L)
- Modify permissions (L)
- Modify owner (R)
- All validated wrights (R)
- All extended rights (R)
- Create all child objects (R)
- Add/remove self as member (R)
- Send to (R)

\*\*\*Send as (R) - Requires Exchange.

Click ok, apply. Now we end up with something that looks like this. This should be more than enough permissions for a helpdesk to create users, computers, groups, and OUs. Preventing them from being able to delete objects, etc.

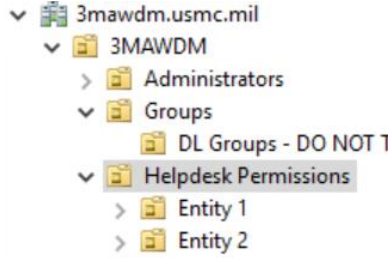
 Allow	DL - Helpdesk Administrator...	Reset password	None	Descendant Computer objects
 Allow	DL - Helpdesk Administrator...	Create ms-net-ieee-80...	None	Descendant User objects
 Allow	DL - Helpdesk Administrator...	Create ms-net-ieee-80...	None	Descendant User objects
 Allow	DL - Helpdesk Administrator...	Special	None	Descendant Computer objects
 Allow	DL - Helpdesk Administrator...	Special	None	Descendant Organizational U...
 Allow	DL - Helpdesk Administrator...	Special	None	Descendant User objects
 Allow	DL - Helpdesk Administrator...	Special	None	Descendant Group objects

Depending on the situation, it may be necessary to go one step further and create specific permissions restricted to each entity underneath the Helpdesk's control. We tend to allow all entities to assist each other with the helpdesk functions. In addition, the entities being supported by our organization change on a very regular basis. This basic permission set allows us to add them to the G - Helpdesk Administrators when they join, and remove them when they depart.

**Word to the wise:** Never place an administrative account or group, which is granted permissions, in a place where they can modify it. It could lead to privilege escalation and compromise your forest. For this example, the Helpdesk Administrator



accounts would exist under the Administrators OU, which is outside of their ability to modify.



## Basic Troubleshooting and Maintenance:

The most important thing to remember is to check your replication.

We have seen replication issues cause issues related to user authentication, certificate validation, email, DNS resolution, etc. When an issue arises, the first thing we usually check is replication and move from there.

Meet repadmin, your new best friend. The command can be targeted by adding the fully qualified domain name of the domain controller to the end.

repadmin /replsum  
repadmin /replsum <DC FQDN>

```
C:\Windows\system32>repadmin /replsum
Replication Summary Start Time: 2019-05-30 08:44:46

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA          largest delta    fails/total %%    error
CHILDDC             12m:27s         0 / 4    0
INSTRUCTORDC       12m:27s         0 / 6    0
SITE2DC             07m:47s         0 / 10   0

Destination DSA    largest delta    fails/total %%    error
CHILDDC            05m:25s         0 / 4    0
INSTRUCTORDC       07m:47s         0 / 6    0
SITE2DC            12m:28s         0 / 10   0
```

The output on this one can be tricky to read. The key takeaway is none of the times should be greater than your configured



## Domain Controllers

replication interval on the AD Sites and Services Inter-Site Transports.

Source, this means that for each DC that should be receiving information from the listed server, this is the greatest interval of one of the partitions.

Destination, for each partition it should receive from its replication partners, this is the largest interval on its receive.

If some of your DC are offline, disconnected, or unreachable, the command will take a few minutes to complete. Depending on what is offline the delta could become quite large and it becomes required to see exactly which partition has the large delta.

For this example, the ChildDC has been shutdown, and is currently offline.

```
Source DSA      largest delta  fails/total  %%  error
CHILDDC        56m:10s      4 / 4       100 (1722) The RPC server is unavailable.
INSTRUCTORDC   09m:46s      0 / 6        0
SITE2DC        06m:30s      0 / 6        0

Destination DSA largest delta  fails/total  %%  error
INSTRUCTORDC   06m:31s      0 / 6        0
SITE2DC        56m:11s      4 / 10      40 (1722) The RPC server is unavailable.

Experienced the following operational errors trying to retrieve replication information:
58 - ChildDC.child.3mawdm.usmc.mil
```

Remember the site link structure.

InstructorDC replicates only with Site2DC.

ChildDC only replicates with Site2DC.

Reading the screen:

At the bottom, there is an issue reaching the ChildDC.

At the top, source, at least one destination has not received information from ChildDC for an hour and there is an error.

InstructorDC, as a source and destination appears to be in sync.

Site2DC as a source, is in sync, as a destination, it has not received something in an hour and shows an error.

Notice how the largest source delta on ChildDC and the destination delta on Site2DC mirror up.



## Domain Controllers

We can dig into Site2DC by targeting it.  
repadmin /showrepl site2dc.3mawdm.usmc.mil

This command will produce a list of every Active Directory partition, each partner it is supposed to replicate with, and the status of the replication.

```
C:\Windows\system32>repadmin /showrepl site2dc.3mawdm.usmc.mil
Site2\SITE2DC
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 1254b9b1-1f7b-4186-8bb6-2f0442be05a8
DSA invocationID: a52a5f45-36ba-4d81-aa34-d6d3f7030792
```

It is part of Site2 and the IS\_GC means it is a Global Catalog.

```
DC=3mawdm,DC=usmc,DC=mil
  Site1\INSTRUCTORDC via RPC
    DSA object GUID: f2b6d5b8-aef4-46ad-afe4-d8ca98f49edb
    Last attempt @ 2019-05-30 09:48:43 was successful.
```

Shows that the 3mawdm partition is replicating with Site1\InstructorDC and the last attempt was successful.

```
CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
  ChildSite1\CHILDDC via RPC
    DSA object GUID: 04488d43-f5b5-43e6-994c-1089f8631d62
    Last attempt @ 2019-05-30 09:48:01 failed, result 1722 (0x6ba):
      The RPC server is unavailable.
    4 consecutive failure(s).
    Last success @ 2019-05-30 08:47:19.
  Site1\INSTRUCTORDC via RPC
    DSA object GUID: f2b6d5b8-aef4-46ad-afe4-d8ca98f49edb
    Last attempt @ 2019-05-30 09:48:43 was successful.
```

The Configuration partition contains all of the site links among other things.

Replication with ChildSite1\ChildDC failed. This is where the error message next to the Site2DC in the replsum comes from. Replication with InstructorDC was successful.



## Domain Controllers

```
CN=Schema,CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
ChildSite1\CHILDDC via RPC
  DSA object GUID: 04488d43-f5b5-43e6-994c-1089f8631d62
  Last attempt @ 2019-05-30 09:48:43 failed, result 1722 (0x6ba):
    The RPC server is unavailable.
  4 consecutive failure(s).
  Last success @ 2019-05-30 08:47:19.
Site1\INSTRUCTORDC via RPC
  DSA object GUID: f2b6d5b8-aef4-46ad-afe4-d8ca98f49edb
  Last attempt @ 2019-05-30 09:48:43 was successful.
```

Same as the above. The key take away is ChildDC is intentionally offline. While the replsum makes it seem as if there are major issues, by digging a little, we can see there are no issues with replication. The following zones were also on the list.

```
DC=DomainDnsZones,DC=3mawdm,DC=usmc,DC=mil
DC=ForestDnsZones,DC=3mawdm,DC=usmc,DC=mil
DC=child,DC=3mawdm,DC=usmc,DC=mil
```

ChildDC was powered on, there are still some errors showing, however, one partition has successfully synced. This means that the replication interval probably has not triggered for the other partitions yet. If the configuration or schema have changed since the DC was offline, it may take even longer for it to automatically sync back in. For the most part, the automatic process is rather resilient.



```
DC=ForestDnsZones,DC=3mawdm,DC=usmc,DC=mil
  ChildSite1\CHILDDC via RPC
    DSA object GUID: 04488d43-f5b5-43e6-994c-1089f86310
    Last attempt @ 2019-05-30 10:33:01 failed, result 1
      The remote system is not available. For information
    7 consecutive failure(s).
    Last success @ 2019-05-30 08:47:19.
  Site1\INSTRUCTORDC via RPC
    DSA object GUID: f2b6d5b8-aef4-46ad-afe4-d8ca98f49e
    Last attempt @ 2019-05-30 10:33:43 was successful.

DC=child,DC=3mawdm,DC=usmc,DC=mil
  Site1\INSTRUCTORDC via RPC
    DSA object GUID: f2b6d5b8-aef4-46ad-afe4-d8ca98f49e
    Last attempt @ 2019-05-30 10:33:43 was successful.
  ChildSite1\CHILDDC via RPC
    DSA object GUID: 04488d43-f5b5-43e6-994c-1089f86310
    Last attempt @ 2019-05-30 10:41:57 was successful.
```

When a DC is disconnected for an extended period, or has been offline and is being powered back on, one of the more common errors is: **The target principle name is incorrect.**

This is easy enough to resolve. The basic steps are, log into the DC, set the KDC service to disabled, restart, log back in, and use repadmin to force a replication for each of the partitions we saw above, change the KDC service back to automatic, restart, give it about 10 minutes and it should be working again.

**Warning:** If an error occurs between the parent and child domain, a different set of commands will be required. A working KDC on the domain is required. When the KDC service is set to disabled, it will not issue the Kerberos tickets to permit authentication.

While the error is not currently showing, we will walk through the process, with a new domain controller which has been added to the child domain for this purpose.

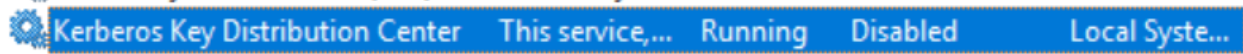




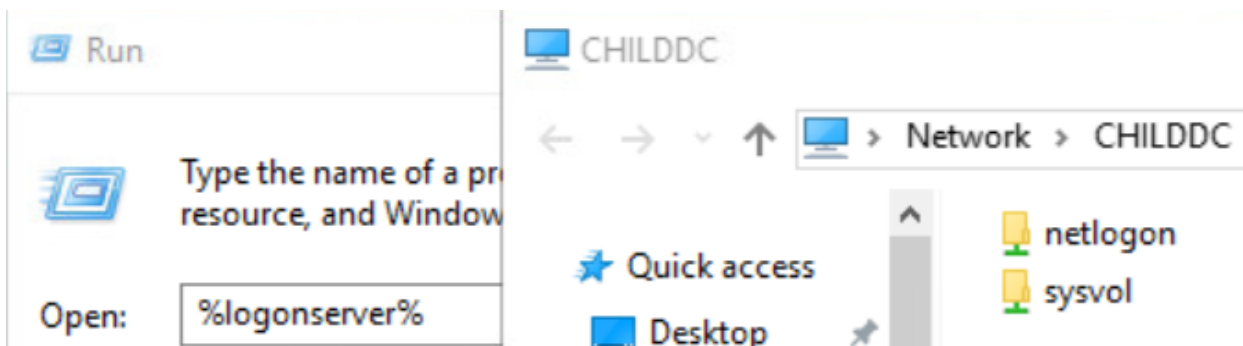
**Kerberos Key Distribution Center** Description:  
This service, running on domain controllers, enables users to log on to the network using the Kerberos authentication protocol. If this service is stopped, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

[Stop the service](#)  
[Restart the service](#)

The first step is to set the KDC service to disabled.



Then restart the server and log back in. Check to see which server you have authenticated off of by using `%logonserver%`.



Shown is logging into ChildDC2, but the credentials were validated from ChildDC.

Next is to forcibly replicate the current information from ChildDC to ChildDC2. The command will need to be ran once for each AD partition. The command to do this is `repadmin /replicate <DestinationDC> <SourceDC> <Partition>`

```
The following command will replicate the Contoso NC from source-dc01 to dest-dc01  
repadmin /replicate dest-dc01 source-dc01 DC=contoso,DC=com
```

Based on the list of partitions above, the following commands will be ran.



## Domain Controllers

```
repadmin /replicate ChildDC2 ChildDC  
CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
```

```
repadmin /replicate ChildDC2 ChildDC  
CN=Schema,CN=Configuration,DC=3mawdm,DC=usmc,DC=mil
```

```
repadmin /replicate ChildDC2 ChildDC  
DC=ForestDnsZones,DC=3mawdm,DC=usmc,DC=mil
```

```
repadmin /replicate ChildDC2 ChildDC  
DC=child,DC=3mawdm,DC=usmc,DC=mil
```

```
repadmin /replicate ChildDC2 ChildDC  
DC=DomainDnsZones,DC=child,DC=3mawdm,DC=usmc,DC=mil
```

```
repadmin /replicate ChildDC2 ChildDC DC=3mawdm,DC=usmc,DC=mil
```

```
C:\>repadmin /replicate ChildDC2 ChildDC CN=Configuration,DC=3mawdm,DC=usmc,DC=mil  
Sync from ChildDC to ChildDC2 completed successfully.  
C:\>repadmin /replicate ChildDC2 ChildDC CN=Schema,CN=Configuration,DC=3mawdm,DC=usmc,DC=mil  
Sync from ChildDC to ChildDC2 completed successfully.  
C:\>repadmin /replicate ChildDC2 ChildDC DC=ForestDnsZones,DC=3mawdm,DC=usmc,DC=mil  
Sync from ChildDC to ChildDC2 completed successfully.  
C:\>repadmin /replicate ChildDC2 ChildDC DC=child,DC=3mawdm,DC=usmc,DC=mil  
Sync from ChildDC to ChildDC2 completed successfully.  
C:\>repadmin /replicate ChildDC2 ChildDC DC=DomainDnsZones,DC=child,DC=3mawdm,DC=usmc,DC=mil  
Sync from ChildDC to ChildDC2 completed successfully.  
C:\>repadmin /replicate ChildDC2 ChildDC DC=3mawdm,DC=usmc,DC=mil  
Sync from ChildDC to ChildDC2 completed successfully.
```

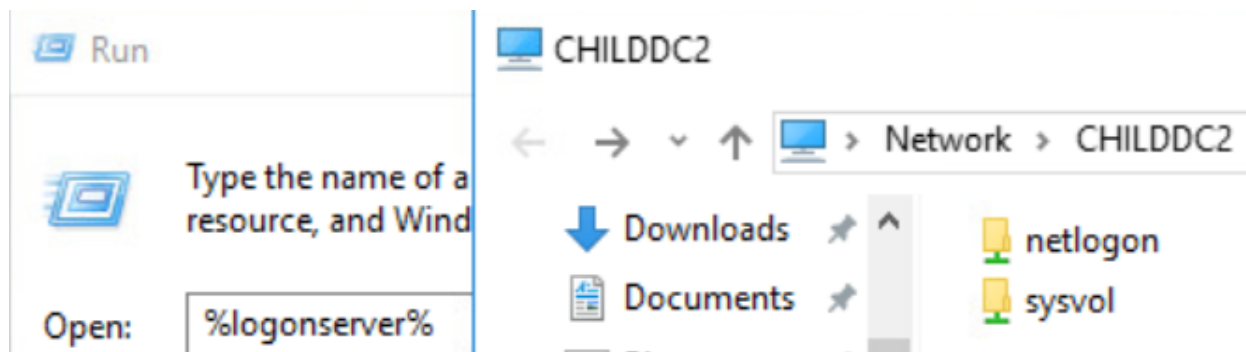
If one partition will not take the first time, try another partition. If a Schema change occurred, the Schema partition may need to be the first one replicated etc. After replication is complete, change the KDC service back to automatic and restart.



Log into the DC and validate it is performing authentication again.







The next step is give it some time and ensure the replication interval which was set is automatically triggering and replication is occurring as intended.

Source DSA	largest delta	fails/total	%	error
CHILDDC	:09s	0 / 6	0	
CHILDDC2	03m:27s	0 / 10	0	
INSTRUCTORDC	03m:27s	0 / 6	0	
SITE2DC	13m:47s	0 / 10	0	

Destination DSA	largest delta	fails/total	%	error
CHILDDC	:09s	0 / 10	0	
CHILDDC2	:10s	0 / 6	0	
INSTRUCTORDC	13m:48s	0 / 6	0	
SITE2DC	03m:28s	0 / 10	0	

If there is an issue between the parent and child domain, it is most likely a trust relationship issue. This is also easy enough to fix from either the parent domain or the child domain. It will require a domain administrator account on both domains. Log into one of the domain controllers and run the following command: (Long one.)

```
netdom trust <Local Domain.fqdn> /Domain:<Remote Domain.fqdn>
/Under:<Remote Domain>\<Remote Domain Admin>
/PasswordD:<Remote Domain Admin Password>
/PasswordO:<Local Domain>\<Local Domain Admin>
/PasswordO:<Local Domain Admin Password>
/reset /twoway
```



## Domain Controllers

```
C:\>netdom trust child.3mawdm.usmc.mil /Domain:3mawdm.usmc.mil /UserD:3mawdm\domainadmin /PasswordD:!QAZ@WSX3edc4rfv /UserO:child\childda /PasswordO:!QAZ@WSX3edc4rfv /reset /twoway
Resetting the trust passwords between child.3mawdm.usmc.mil and 3mawdm.usmc.mil

The trust between child.3mawdm.usmc.mil and 3mawdm.usmc.mil
has been successfully reset and verified

The command completed successfully.
```

For this example, while signed into the ChildDC as a domain administrator, from an elevated command prompt, the following command was ran:

```
netdom trust child.3mawdm.usmc.mil /Domain:3mawdm.usmc.mil  
/UserD:3mawdm\domainadmin /PasswordD:!QAZ@WSX3edc4rfv  
/UserO:child\childda /PasswordO:!QAZ@WSX3edc4rfv  
/reset /twoway
```

The KCC will check its site configuration every 15 minutes, and will attempt to rebuild site links (when a DC is offline) every two hours. While this automated timeline is great for keeping things up and running; sometimes, it needs to happen now. Using the following command an administrator can force a DC to check and rebuild the connections with its partners.

```
repadmin /kcc <Target DC>
```

A common error, which tends to occur is when a machine falls off the domain. Computer accounts, like user accounts, have passwords associated with them. The computer, by default will change its password every 30 days. In addition, the computer account will store the last two known good passwords.

The old method of resolving the issue was to take the computer off the domain, reset the computer, and rejoin it to the domain. This is still a valid fix, however, due to some modern features, it is not the preferred fix. The preferred method is to use the Reset-ComputerMachinePassword.

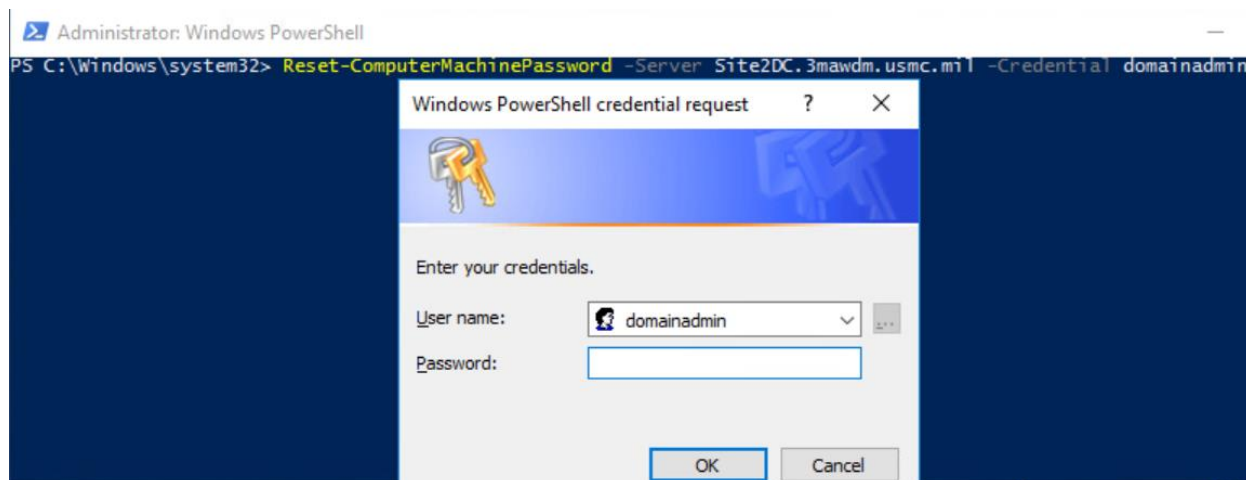
The first step is to log into the computer with any administrative account. Whether you are breaking into the computer, pulling its local administrative password out of AD, or using a cached account.

Then we need to reset the password, and we can choose to direct this to a specific domain controller.

```
Reset-ComputerMachinePassword -Server <TargetDC.FQDN>
```



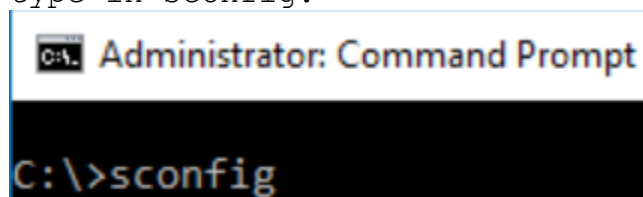
-Credential <Administrator>



Enter the password and voila, the computer is back on the domain. If there is a mass occurrence, try to figure out what changed. This should only be needed occasionally.

### SCONFIG:

sconfig is a configuration tool which can be used when the server was installed in Core mode. It can also be useful when the GUI is installed. Open a command prompt as an administrator, type in sconfig.



While sconfig isn't just for updates, it is an easy tool to use to configure and check for Windows Updates.



```
Administrator: Command Prompt - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

=====
                          Server Configuration
=====

1) Domain/Workgroup:           Domain: 3mawdm.usmc.mil
2) Computer Name:             INSTRUCTORDC
3) Add Local Administrator
4) Configure Remote Management Enabled
5) Windows Update Settings:   DownloadOnly
6) Download and Install Updates
7) Remote Desktop:            Disabled
8) Network Settings
9) Date and Time
10) Telemetry settings         Basic
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option:
```

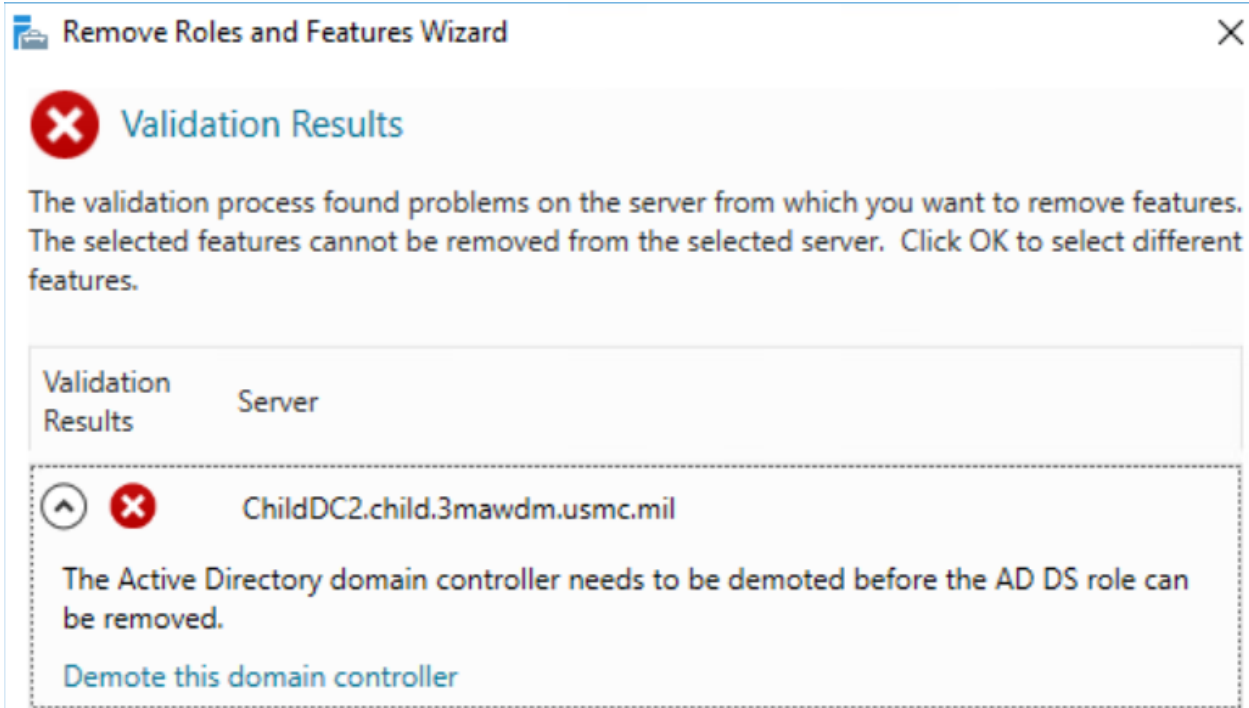
With the servers, there are two methods for manually checking for updates. Start, Settings, Updates and Security, then press the Check for Updates button, same as on a workstation.

### Demoting A Domain Controller:

Demoting a domain controller is similar to promoting it. In Server Manager, Manage, Remove Roles and Features, Uncheck the box for Active Directory Domain Services.

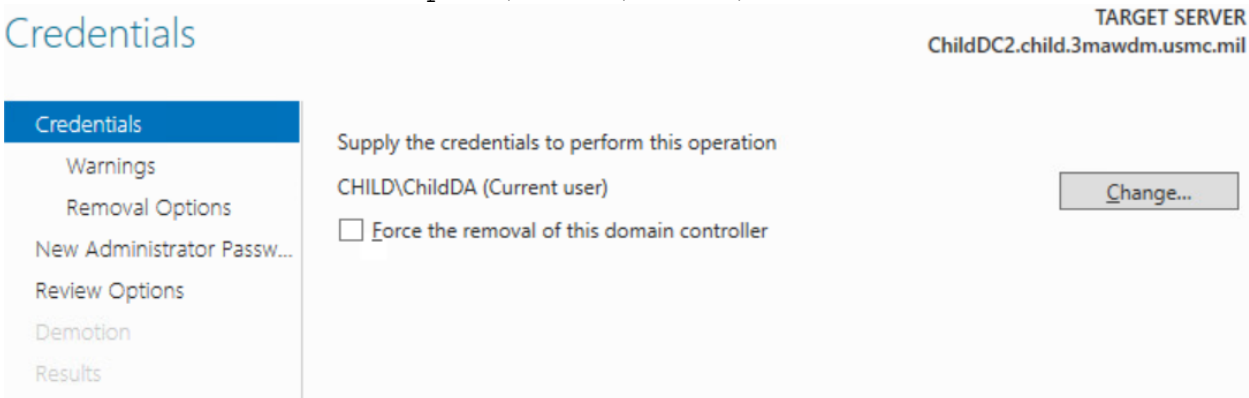
A box will pop up with an error, but the box will contain a link to demote the domain controller. Click the link.





The walk through for demoting a domain controller is very similar. For the most part, next, next, finish.

## Credentials



Check the box acknowledging the warnings.



## Warnings

TARGET SERVER  
ChildDC2.child.3mawdm.usmc.mil

Credentials

**Warnings**

Removal Options

New Administrator Passw...

Review Options

Demotion

Results

The domain controller currently hosts the following role(s):

- Domain Name System (DNS) Server
- Global Catalog

**⚠** The roles hosted by the domain controller are required for Active Directory Domain Services functionality. If you proceed, some Active Directory Domain Services operations may be impacted.

Proceed with removal

If this is the last domain controller in the child domain, it is safe to remove the DNS delegation. Otherwise, uncheck the box.

## Removal Options

TARGET SERVER  
ChildDC2.child.3mawdm.usmc.mil

Credentials

Warnings

**Removal Options**

New Administrator Passw...

Review Options

Demotion

Results

Remove DNS delegation

Enter the new local administrator password.

## New Administrator Password

TARGET SERVER  
ChildDC2.child.3mawdm.usmc.mil

Credentials

Warnings

Removal Options

**New Administrator Passw...**

Review Options

Demotion

Results

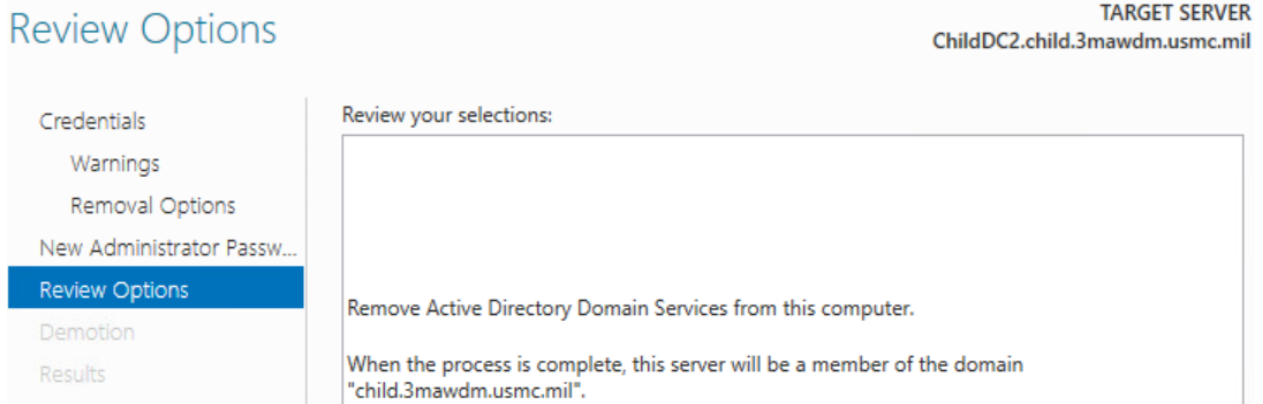
Password:

Confirm password:

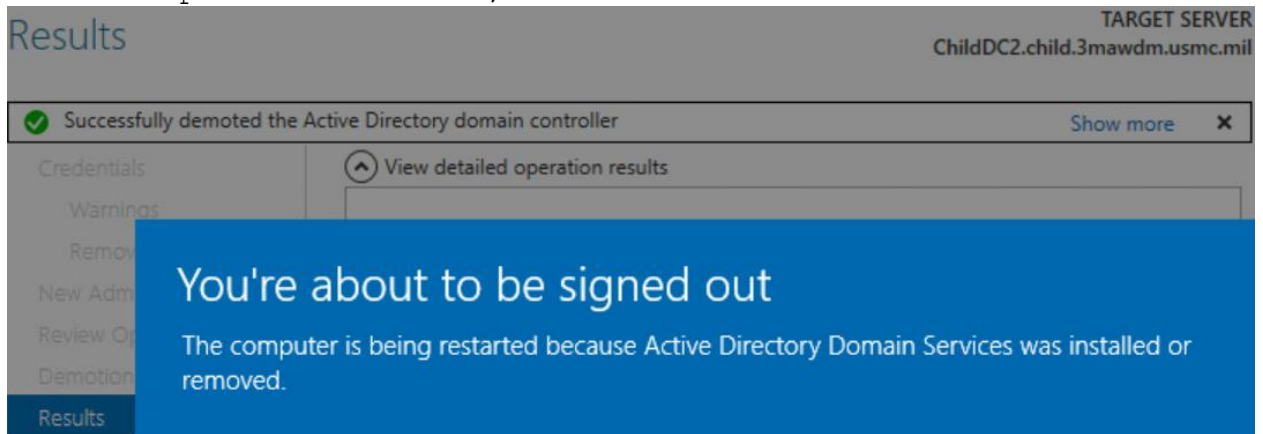
Confirm the summary and click the Demote button.



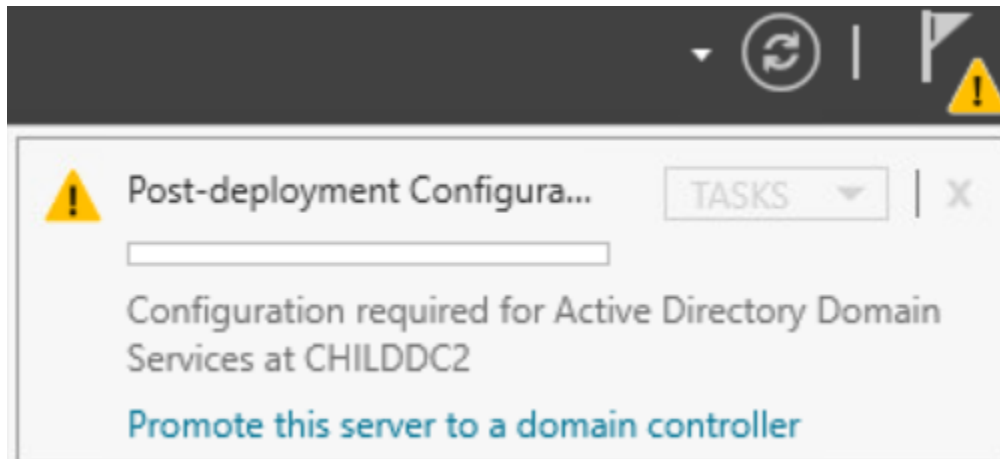
Domain Controllers



When the process finishes, the server will restart.



After the server restarts, the Server Manager will display the following message. Go back to the Remove Roles and Features, and uncheck the box for AD DS.



When the role has been removed, click close and restart the server.



## Domain Controllers

Remove Roles and Features Wizard

DESTINATION SERVER  
ChildDC2.child.3mawdm.usmc.mil

### Removal progress

Before You Begin  
Server Selection  
Server Roles  
Features  
Confirmation  
**Results**

View removal progress

**Feature removal**

A restart is pending on ChildDC2.child.3mawdm.usmc.mil. You must restart the destination server to finish removing features.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - AD DS Tools
        - Active Directory Administrative Center
        - AD DS Snap-Ins and Command-Line 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.

< Previous   Next >   Close   Cancel

Now it is safe to turn off the VM, delete it, and delete the computer account from Active Directory.

### **Backups (Never, ever, ever, use snapshots.):**

**Warning:** Use of snapshots can brick a domain controller, the domain, potentially the entire forest. Never, ever, ever use snapshots.

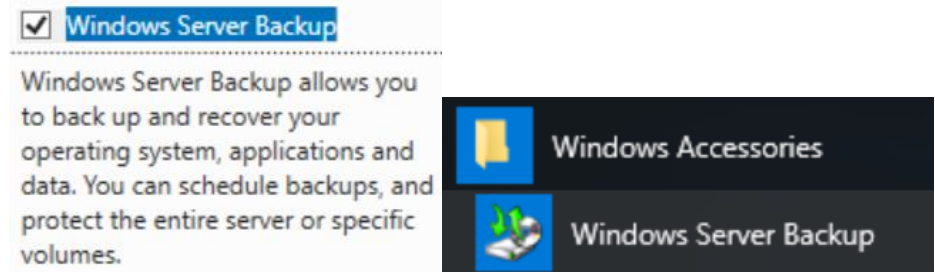
Please read the warning above.

The only supported method of recovering a domain controller is by using Microsoft's Windows Server Backup utility. As various roles and features each add in their pieces, it is one of the last features installed on a server. Unless of course, you want to potentially install it over, and over, and over, depending on what was installed on the server..



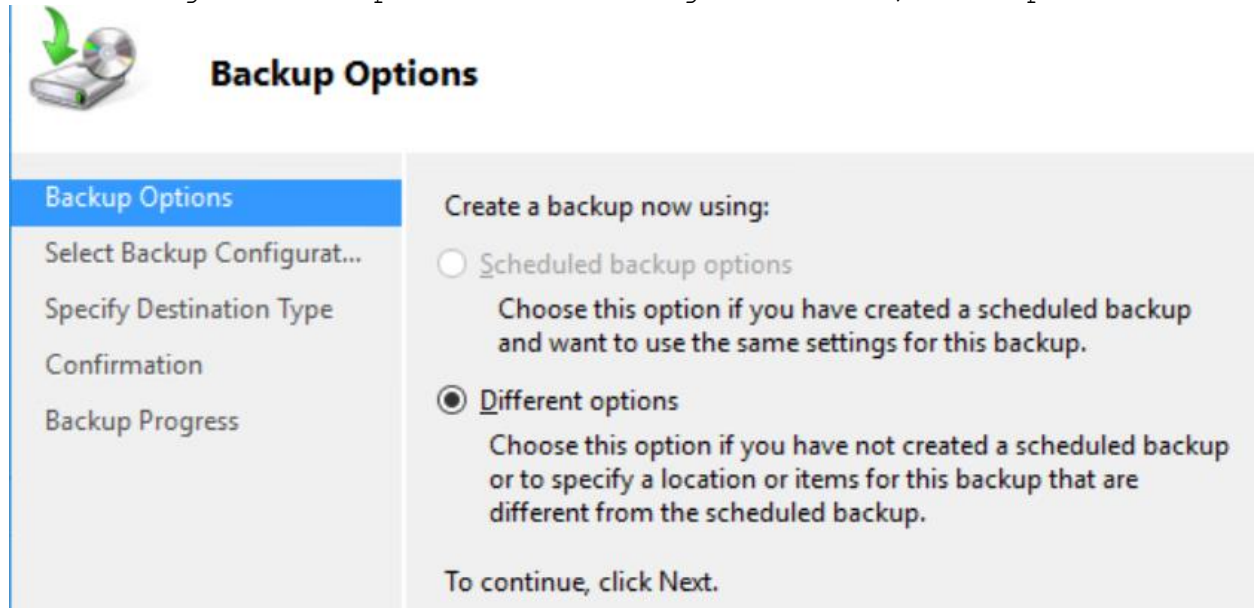


Open Server Manager, and select Add Roles and Features. It will be located under features, Windows Server Backup. The graphical interface will be located under Windows Accessories.

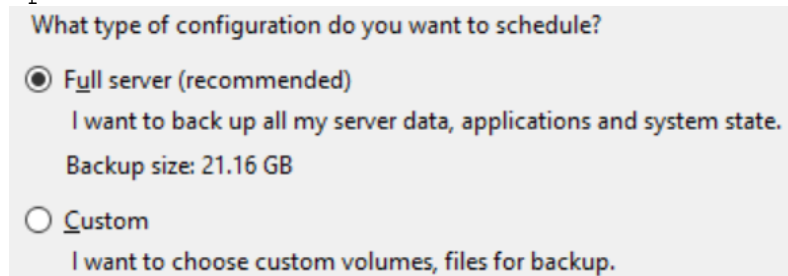


While the item is always on the list, if it is not installed first, it will say it needs to be installed before it can be used.

The tool will provide a listing of existing backups, along with the configuration options on the right. Select, Backup Once...



For most servers, the Full Backup option is good. It is a good option for the domain controllers.



## Domain Controllers

The only down side to the Full server, is it uses the VSS Copy Backup. This only affects services such as Exchange, MSSQL, and other services which log transactions to a disk before writing them into a database.

If disk space is not an issue, it is recommended to establish a backup schedule to a network drive.

This is about as far as we will go into backups for the moment.

There are a few things to keep in mind when backing up and restoring Active Directory, or a domain controller. The backup is only valid for the Tombstone lifetime. If the DFSR settings were not adjusted and the backup is older than 60 days, there will be errors showing up concerning the SYSVOL.

Every domain controller in the domain contains the information, and it is almost always easier to rebuild and replace a domain controller than it is to restore one from a backup.

Depending on who is signing the certificates used by the domain controller for PKI (not covered), the primary purpose we use backups for is to retain the ability to restore that certificate. (Our process can take a couple weeks to receive a new certificate.)

