Securing your Active Directory environment with VMware cloud on AWS

History:

Securing an active directory environment is a very crucial consideration while designing a datacenter in a traditional datacenter environment to secure an AD environment we keep a primary domain controller at the primary site and secondary domain controller in some other site, so that in any unwanted situation we make sure our directory services are available and users/resources are getting authenticated with the available domain controller.

Introducing VMware Cloud to the Scenario:

With the increased usage of VMware cloud on AWS, customers are liking the idea of using VMware cloud as a DR site for their on-prem environment. Adding to the same idea we will demonstrate how can we secure the on-prem Active directory environment by deploying a secondary domain controller in VMware cloud on aws , and if needed how can we promote it as a primary domain controller (DR or on-prem datacenter's Maintenance/Upgradation) .

General Info for this demonstration:

There could be multiple active directory scenarios however for the purpose of this demonstration we are using following configuration.

# 1 Primary domain controller named ad-dns.homelab.lab (preconfigured)

# 1 on-prem DNS server (Preconfigured)

# An Active and preconfigured CGW ipsec VPN

# Domain Name homelab.lab

# VMC DC Name : VMC-AD-DNS

Good to know information before we begin:

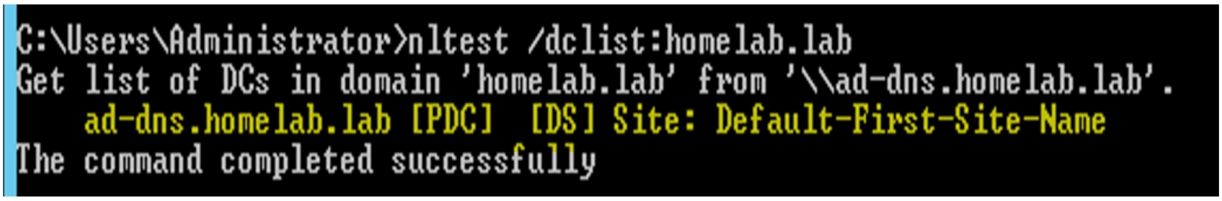
In an active directory environment, you typically have 1 Primary domain controller and some Secondary/Backup/additional domain controllers. Secondary domain controllers are used for load balancing and as a backup for primary DC in case of any failure.

Also, if there is a condition where we want to promote Secondary DC to primary we can do it by transferring/Seizing 5 FSMO roles to it.

Procedure:

To better understand the scenario Lets start with having a look at the current configuration.

In my on-prem DC I ran “nltest /dclist:homelab.lab” command and found that currently we have only 1 DC i.e. ad-dns.homelab.lab.



```
C:\Users\Administrator>nltest /dclist:homelab.lab
Get list of DCs in domain 'homelab.lab' from '\\ad-dns.homelab.lab'.
    ad-dns.homelab.lab [PDC]  [DS] Site: Default-First-Site-Name
The command completed successfully
```

Now we need to deploy a secondary DC (Server 2012 R2 for this demonstraion) in VMC environment and before that Some firewall configuration is needed and other settings need to be verified.

1) Opening Firewall rules on your onprem and CGW of VMC

- **TCP and UDP Port 88** – Kerberos authentication
- **TCP and UDP Port 135** – domain controllers-to-domain controller and client to domain controller operations.
- **TCP Port 139 and UDP 138** – File Replication Service between domain controllers.
- **UDP Port 389** – LDAP to handle normal queries from client computers to the domain controllers.
- **TCP and UDP Port 445** – File Replication Service
- **TCP and UDP Port 464** – Kerberos Password Change
- **TCP Port 3268 and 3269** – Global Catalog from client to domain controller.
- **TCP and UDP Port 53** – DNS from client to domain controller and domain controller to domain controller.
- **TCP Port 5722** – DFSR/RPC – Sysvol Replication between Domain Controllers.

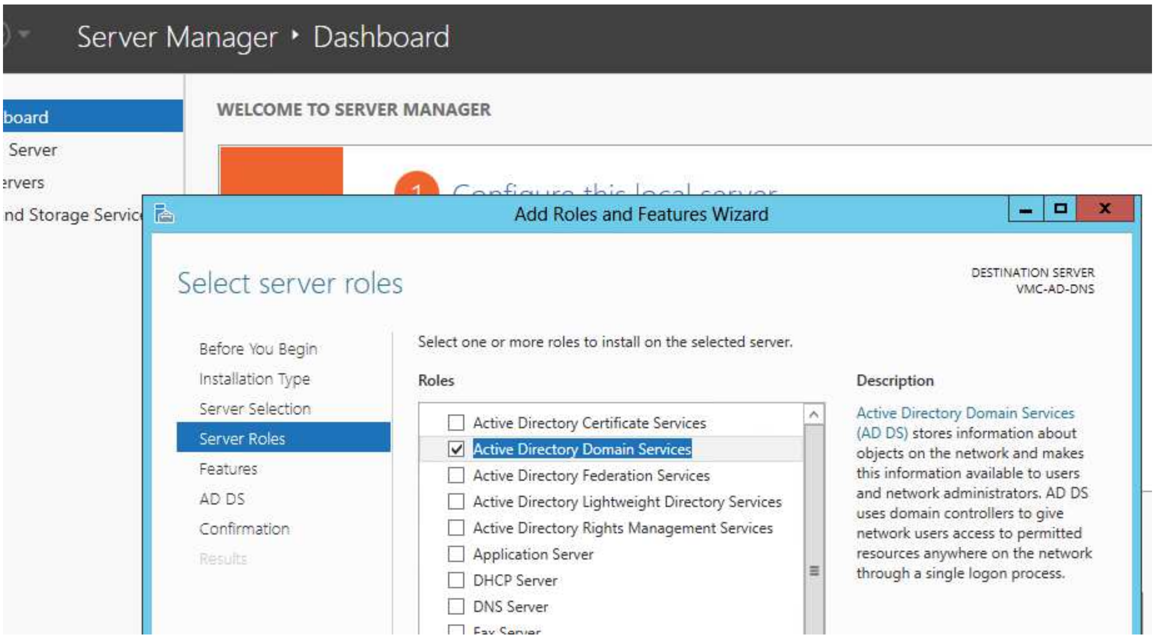
Other Consideration for the ports could be:

- **TCP Port Range 1025-5000** – If your network has any Server 2003 R2 or older domain controllers. This is the default dynamic range for RPC connections.
- **TCP Port Range 49152-65535** – If your network has any Server 2008 or newer domain controllers. This is the new dynamic port range for RPC connections

2) **Connectivity between the new VM in VMC to DC and DNS server (verify it with ping)**
3) **Change the DNS on VMC server to your on-prem DNS (If you are planning to install a secondary dns in VMC you can do that too)**

Install and Prepare the environment :

After all these checks we will install active directory role on the VMC server, The installation is simple, from server manager you click on add roles and features and select the box Active directory domain services and follow the wizard.



Select server roles

DESTINATION SERVER
VMC-AD-DNS

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

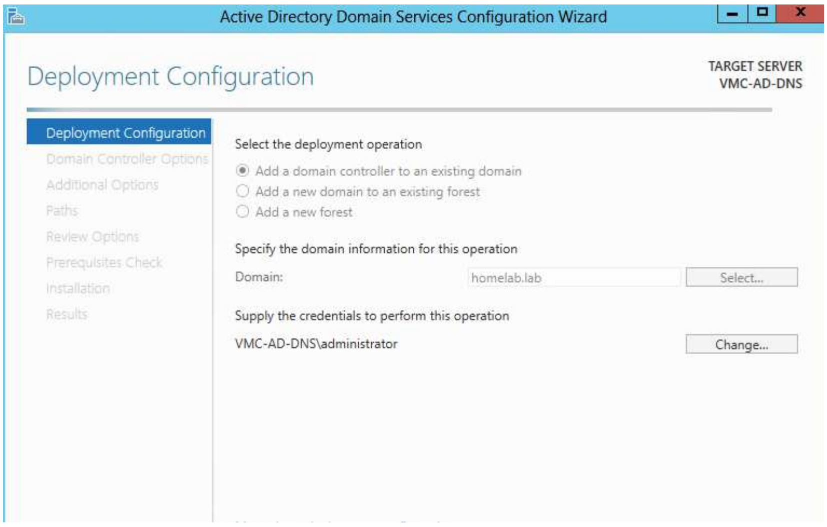
Roles

□ Active Directory Certificate Services
☑ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
□ DNS Server
□ Fax Server

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Once installed we need to configure it and the only difference in the configuration of Secondary Domain controller is you select add a domain controller to an existing domain and supply the domain name and domain admin username and password.



Deployment Configuration

TARGET SERVER
VMC-AD-DNS

Select the deployment operation

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

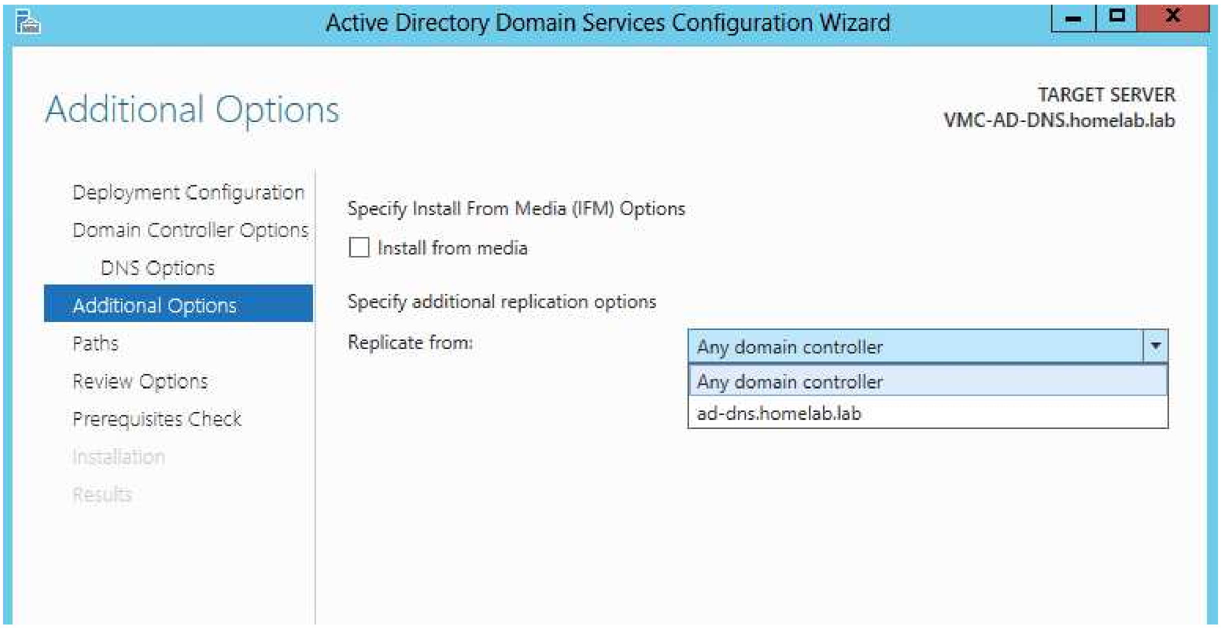
Specify the domain information for this operation

Domain: homelab.lab

Supply the credentials to perform this operation

VMC-AD-DNS\administrator

Follow the wizard for rest of the configuration. If all the config is correct AD will be installed and during the installation it-self, you will be able to contact and list out the other DC.



Additional Options

TARGET SERVER
VMC-AD-DNS.homelab.lab

Specify Install From Media (IFM) Options

□ Install from media

Specify additional replication options

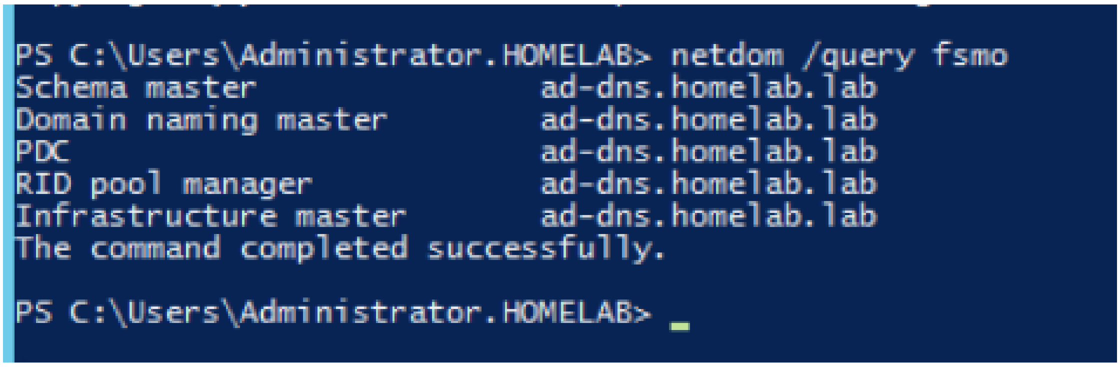
Replicate from: Any domain controller

Once the wizard completes the secondary DC will reboot and That’s It! you are ready with your secondary Functional DC.

Now we will talk about the second scenario where we need to transfer the roles from primary to secondary DC.

Let’s verify which Domain controller is holding the FSMO roles right now.

On any of the DC you run command “netdom /query fsmo” to check which DC holds what role



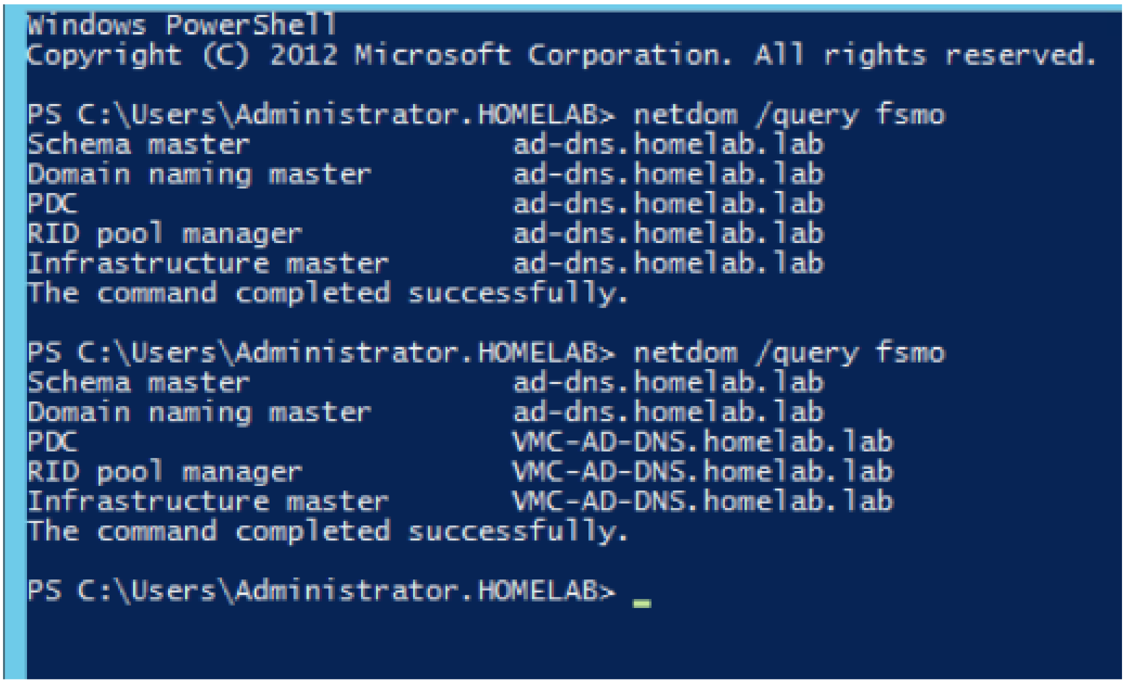
```
PS C:\Users\Administrator.HOMELAB> netdom /query fsmo
Schema master               ad-dns.homelab.lab
Domain naming master        ad-dns.homelab.lab
PDC                         ad-dns.homelab.lab
RID pool manager            ad-dns.homelab.lab
Infrastructure master       ad-dns.homelab.lab
The command completed successfully.

PS C:\Users\Administrator.HOMELAB> _
```

As we can see above right now the onprem DC contains all the 5 FSMO roles.

You can find the process of Transferring or Seizing the role from primary to secondary in this blog

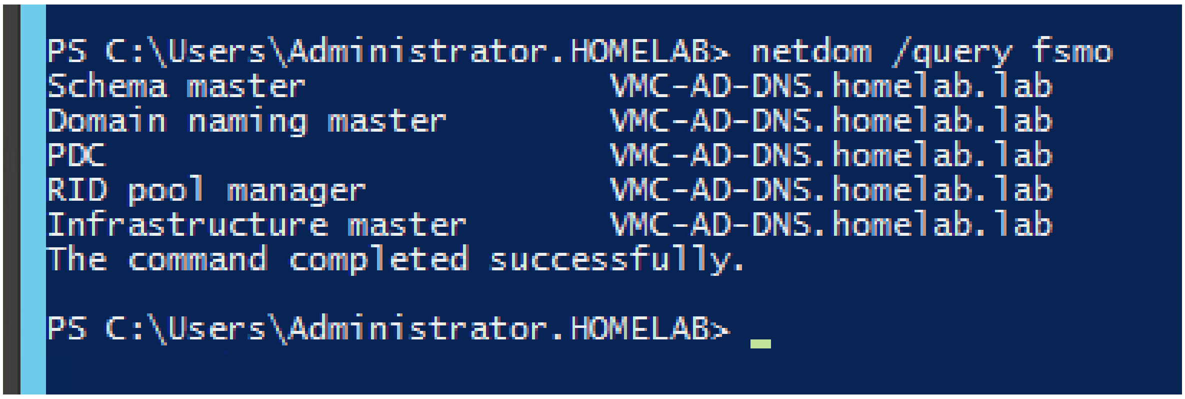
http://www.computertechblog.com/migrating-windows-server-2012-r2-fsmo-roles-to-another-dc/

It was easy and quick I first transferred the domain wide role you can see the before and after transfer status of the Domain wide role transfer.



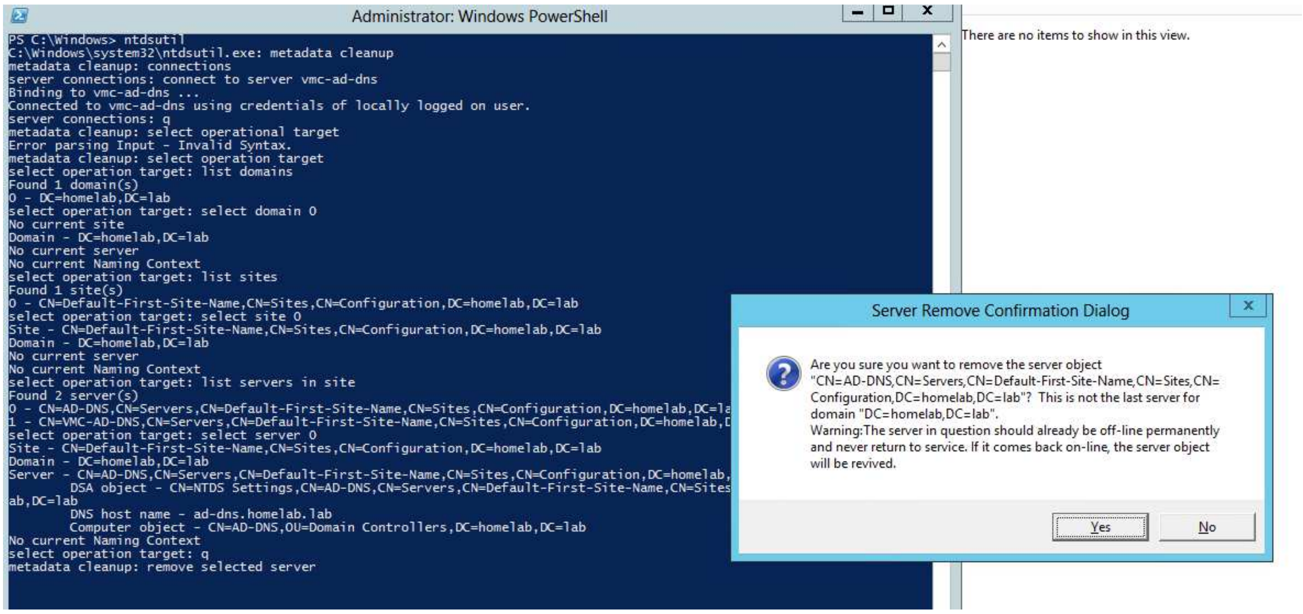
```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.HOMELAB> netdom /query fsmo
Schema master               ad-dns.homelab.lab
Domain naming master        ad-dns.homelab.lab
PDC                         ad-dns.homelab.lab
RID pool manager            ad-dns.homelab.lab
Infrastructure master       ad-dns.homelab.lab
The command completed successfully.

PS C:\Users\Administrator.HOMELAB> netdom /query fsmo
Schema master               ad-dns.homelab.lab
Domain naming master        ad-dns.homelab.lab
PDC                         VMC-AD-DNS.homelab.lab
RID pool manager            VMC-AD-DNS.homelab.lab
Infrastructure master       VMC-AD-DNS.homelab.lab
The command completed successfully.

PS C:\Users\Administrator.HOMELAB> _
```

Once that was done we can transfer the forest wide roles as well, so all the 5 roles were now present on the DC hosted in VMware cloud.



```
PS C:\Users\Administrator.HOMELAB> netdom /query fsmo
Schema master               VMC-AD-DNS.homelab.lab
Domain naming master        VMC-AD-DNS.homelab.lab
PDC                         VMC-AD-DNS.homelab.lab
RID pool manager            VMC-AD-DNS.homelab.lab
Infrastructure master       VMC-AD-DNS.homelab.lab
The command completed successfully.

PS C:\Users\Administrator.HOMELAB> _
```

Optionally you can perform a cleanup task to clear out the original DC entry (only if you don’t want to bring it back in the environment) demonstrated here.


Administrator: Windows PowerShell
There are no items to show in this view.
Server Remove Confirmation Dialog

```
PS C:\Windows> ntdsutil
C:\Windows\system32\ntdsutil.exe: metadata cleanup
metadata cleanup: connections
server connections: connect to server vmc-ad-dns
Binding to vmc-ad-dns ...
Connected to vmc-ad-dns using credentials of locally logged on user.
server connections: q
metadata cleanup: select operational target
Error parsing Input - Invalid Syntax.
metadata cleanup: select operation target
select operation target: list domains
Found 1 domain(s)
0 - DC=homelab,DC=lab
select operation target: select domain 0
No current site
Domain - DC=homelab,DC=lab
No current server
No current Naming Context
select operation target: list sites
Found 1 site(s)
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=homelab,DC=lab
select operation target: select site 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=homelab,DC=lab
Domain - DC=homelab,DC=lab
No current server
No current Naming Context
select operation target: list servers in site
Found 2 server(s)
0 - CN=AD-DNS,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=homelab,DC=la
1 - CN=VMC-AD-DNS,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=homelab,D
select operation target: select server 0
Site - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=homelab,DC=lab
Domain - DC=homelab,DC=lab
Server - CN=AD-DNS,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=homelab,
        DSA object - CN=NTDS Settings,CN=AD-DNS,CN=Servers,CN=Default-First-Site-Name,CN=Sites
ab,DC=lab
        DNS host name - ad-dns.homelab.lab
        Computer object - CN=AD-DNS,OU=Domain Controllers,DC=homelab,DC=lab
No current Naming Context
select operation target: q
metadata cleanup: remove selected server
```

Are you sure you want to remove the server object "CN=AD-DNS,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN= Configuration,DC=homelab,DC=lab"? This is not the last server for domain "DC=homelab,DC=lab".
Warning:The server in question should already be off-line permanently and never return to service. If it comes back on-line, the server object will be revived.

And your new Primary DC in VMC cloud is ready for use 😌

Document Created By: Atul Srivastava (srivastavaat@vmware.com)