

# Disaster Recovery of Stretch Deployed VM (DCE) in vCloud Hybrid Service aka vCHS

Yesterday, I talked about the [Data Center Extension \(DCE\) to the vCHS](#) from your on Prem and a whole gamut of steps you need to perform for this. I have also talked about the DCE Use Case and the Service Overview of it. At the end of the article I have raised a point and that is how do you protect your DCE'd VM from disaster recovery. It may happen that accidentally you delete the DCE'd VM or it may become corrupted as well. Who has seen the worst? So, in that aspect you should know what you can do to restore the DCE'd VM or more appropriately restore the Service (SSL VPN Tunnel) extended to the vCHS. Well, we at vCHS R&D thought through this for you and we have implemented the solutions as well. You just need to consume that service and let other things being handled by those who build cloud since many years now. Before I proceed to show you the solution, let me ask you this, do you know [VMware offers a Freemium Data Protection Service with vCHS](#) and when I say its **Freemium**, I literally mean that it is a \$0 service. If you don't know the background of that Add On service, you should look at this article.

## Steps for Data Protection of DCE VM

Do you know it's the most easiest way to protect your cloud VM in vCHS. Perhaps if you don't know look at the above DPS article and you would be amazed to see a few click service activation and protecting your cloud workload. So, lets do it now.

1. Login to the vCHS Portal
2. Go to your VDC and Click on the Virtual Machines Tab
3. There you can see your DCE'd VM there. Click on the drop down combo at the right hand side and select "**Register for backup**"
4. In the next schedule vCHS Operator will back it up and FYI the RPO is 24 hours. That means in 24 hours only one time this VM will be backed up. So that means your responsibility ends there.
5. If you want to make sure that the backup registration is done, select the VM, click on the drop down combo and you should see "**Unregister for Backup**".

vmware vCloud Hybrid Service

VPC3 Admin Help

Dashboard Virtual Machines Gateways Users

DASHBOARD > VIRTUAL DATACENTER DETAILS

### DCE-TEST-VDC ON 26853-120836

Usage & Allocation Virtual Machines Gateways Networks Users

Showing 2 of 2

Manage in vCloud Director + Add One Power On Power Off See More

	Name	Owner	Resources		OS	vAPP	Virtual Datacenter	
			CPU	Memory				
	Memhog-VM2	d1p3v3vchsadmin1...	2 vCPUs	2 GB	Ubuntu Linux (32-bit)	Stretched_Memhog2	DCE-Test-VDC	
	test	psreekan@vmware....	1 vCPUs	1 GB	CentOS 4/5/6 (32-bit)	test-VApp	DCE-Test-VDC	View & Edit Details Power Off Suspend Reset Unregister for Backup Create Snapshot Revert Snapshot Delete Snapshot Launch Console

STATUS: Unlocked

VM QUOTA: Unlimited

Edit VDC Name & Description

Delete VDC

RELATED LINKS

Purchase More Resources  
Memory, Storage or CPU  
(Service ID: 26853)

vCloud Director URL

Manage Catalogs in vCloud Director

Ok, so your vApp (VM) is backed up in the back end. Now, let us simulate a disaster for this DCE VM and show you how do you get your service back and how seamless that is.

1. First of all login to the vCHS Portal if not already logged in.
2. Go to the VDC where your DCE VM is up and running.
3. Select the VM and using the drop down combo select Power Off.
4. Once this VM (vApp) is powered off, select the drop down again and select Delete.
5. You should see that the VM is gone from the vCHS Portal.
6. Go back to your On Prem Datacenter and login to the vSM Web Interface
7. Go to the Network Virtualization and click on Edge
8. Double click on the Edge and go to the VPN Tab.
9. You should see that VPN Tunnel is down, because your end point Edge is gone from vCHS as you deleted the vApp and indeed it will delete the Edge as well corresponding to the vApp network.

You are logged in as a System Administrator    Logged in as: admin    [Change Password](#)    [Logout](#)    [Help](#)    [About](#)

**CIS-R&D**

General    App Firewall    Endpoint    SpoofGuard    **Network Virtualization**

Preparation    Network Scopes    Networks    Edges    [Refresh](#)

**vSphere\_DCE\_Edge**

Settings    Statistics    Configure    Firewall    DHCP    NAT    **VPN**    Load Balancer

IPSec VPN | **SSL VPN-Plus**

IPSec VPN Service Status: Enabled [Disable](#)

Global configuration status: Not Configured [Change](#)

**Logging Policy**

☐ Enable logging

Log level: INFO ▼

+ ✎ ✕ | ✓ ✖

Search [↻](#) [🔍](#)

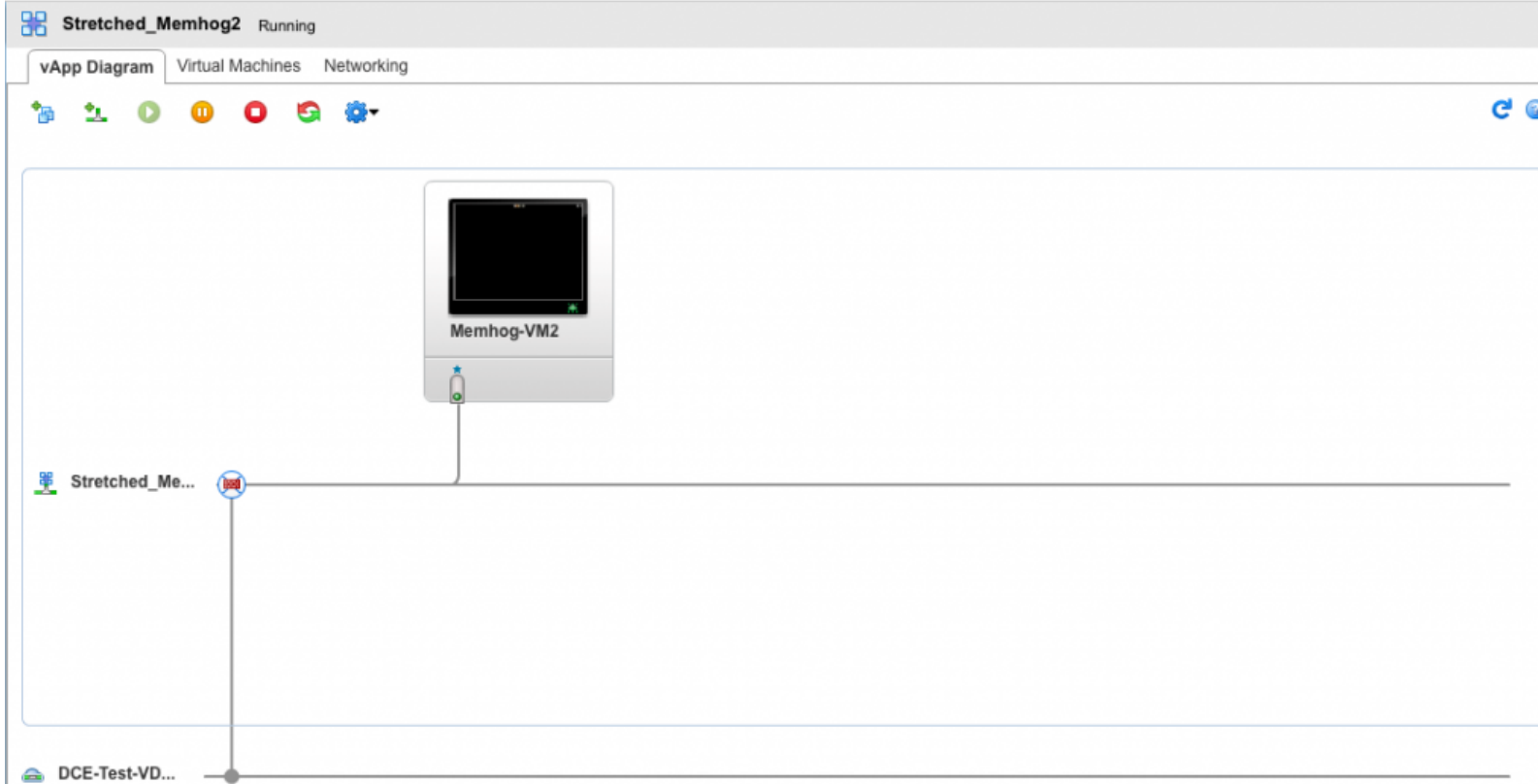
Name	Local Endpoint	Local Subnets	Peer Endpoint	Peer Subnets	Status	Channel Status	Tunnel Status
__SSL_VPN_SOURCE_	10.112.187.90	192.168.0.0/24	64.20.	192.168.0.0/24	✓	✗	0 UP 1 DOWN

So, at this time, you realize that you hit with the disaster situation. Your SSL VPN Tunnel is down and the VM (vApp) is also gone. But hey, you did register it for the backup right? Why don't you restore it from the backup? Yes you should.

## How do you restore the DCE Service?

1. Call up GSS (1-877-486-9273) and ask to restore your VM from backup in vCHS.
2. Provide them the name of the VM, VDC it was running and whether you need to Network also to be restored or not.
3. GSS guys will co-ordinate with vCHS Operations team guys and will have your VM restored at your destined VDC in the back end.
4. You should opt for these three options while you do restore.
  1. vApp Network Restore
  2. VM Network Connection Restore
  3. vApp Network Services Restore (e.g., NAT & Firewall)
5. Once they restore it to the VDC, through vCHS portal go inside the VDC and you can see the DCE'd VM there.
6. From the vCHS portal login to the vCD using SSO and straight a way go to the vApp which you just got recovered.

7. Make sure you can see that there is a vApp Network and it is connected to the Org Routed Network which you have chosen at the time of DCE.



8. Also make sure that you can see the NAT and Firewall service option selected there in the Networking properties page.

**Stretched\_Memhog2** Running

vApp Diagram Virtual Machines **Networking**

**Configure Networking**

Specify how this vApp, its virtual machines, and its vApp networks connect to the organization VDC networks that are accessed in this vApp.

☐ Fence vApp  
Fencing allows identical virtual machines in different vApps to be powered on without conflict by isolating the MAC and IP addresses of the virtual machines.

Name	Status	Gateway Address	Network Mask	Connection	Routing	DHCP	Retain IP/ MAC Resources
Stretched_Memhog2_network	✓	192.168.0.1	255.255.255.0	DCE-Test-VDC-defa	<input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> Firewall	--	<input type="checkbox"/>

9. Go to the right hand side combo box and select Power On this VM.

This would do the magic. Do you know what would happen at the backend? While taking the backup we backup the Networking properties as well for a VM (vApp). So that means we would also have the vApp network properties and it's services backed up. After you ask for restore, vCHS Operator will also make sure that they restore the vApp Networking properties too.

As designed or as expected behavior, when you power on a vApp, it will first deploy an Edge device first if there is a vApp Network associated with it. In this case, there were a vApp Network and it will spawn a Edge device first and get this configured automatically as per the standard vApp power on process. Once the network is ready then it will power on the VM there and reconfigure it to attach it to the vApp Network. At this stage, your vApp Edge will start communicating to your On Prem Edge and will automatically get the VPN Tunnel established. Once the tunnel is up, go back to your On Prem Edge and make sure that you see that the tunnel is up.

**CIS-R&D** You are logged in as a System Administrator Logged in as: admin [Change Password](#) [Logout](#) [Help](#) [About](#)

General App Firewall Endpoint SpoofGuard **Network Virtualization**

Preparation Network Scopes Networks Edges Refresh

**vSphere\_DCE\_Edge**

Settings Statistics Configure Firewall DHCP NAT **VPN** Load Balancer

IPSec VPN | **SSL VPN-Plus**

IPSec VPN Service Status: Enabled



Global configuration status: Not Configured [Change](#)

**Logging Policy**

☐ Enable logging

Log level: INFO

+ ✎ ✕ ✓ ✖

Search  

Name	Local Endpoint	Local Subnets	Peer Endpoint	Peer Subnets	Status	Channel Status	Tunnel Status
__SSL_VPN_SOURCE_	10.112.187.90	192.168.0.0/24	64.20.	192.168.0.0/24	✓	✓	1 UP 0 DOWN

At this time, go back to your VM in vCHS and from the drop down select the View and Edit Details. Go to the Networks tab and make sure that you get a DHCP IP Address from On Prem Edge DHCP Pools.

vmware vCloud Hybrid Service

VPC3 Admin ▾ Help ▾

Dashboard Virtual Machines Gateways Users

DASHBOARD > VIRTUAL DATACENTER DETAILS > VIRTUAL MACHINE DETAILS

## MEMHOG-VM2 ON DCE-TEST-VDC

Settings Networks

Showing 1 of 1 networks this VM connects to

Power Off VM to edit network assignment Power Off

**STRETCHED\_MEMHOG2\_NETWORK**  
Virtual Machine IP: **192.168.0.116**  
TYPE: **GATEWAY**  
GATEWAY: **DCE-Test-VDC**  
Gateway IP: **64.20.**

VAPP: **Stretched\_Memhog2**  
CLOUD: **26853-120836**  
OS: **Ubuntu Linux**  
GUEST OS CUSTOMIZATION: **Disabled**  
GUEST OS PASSWORD: **-**  
VMWARE TOOLS: **Installed**

Edit VM Name & Description  
 Manage VM in vCloud Director

Networking related questions? Call 1-877-486-9273 (toll-free) for assistance in US. For other locations, [click here](#)

Now open up the Console of your VM in vCHS and try to ping the On Prem VMs and make sure it is reachable over the network.

```
Terminal
File Edit View Search Terminal Help

RX packets:564 errors:0 dropped:0 overruns:0 frame:0
TX packets:564 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:35344 (35.3 KB) TX bytes:35344 (35.3 KB)

11/03/2019 - # ping 192.168.0.115
PING 192.168.0.115 (192.168.0.115) 56(84) bytes of data.
64 bytes from 192.168.0.115: icmp_req=1 ttl=64 time=265 ms
64 bytes from 192.168.0.115: icmp_req=1 ttl=64 time=265 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=2 ttl=64 time=261 ms
64 bytes from 192.168.0.115: icmp_req=2 ttl=64 time=261 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=3 ttl=64 time=274 ms
64 bytes from 192.168.0.115: icmp_req=3 ttl=64 time=274 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=4 ttl=64 time=270 ms
64 bytes from 192.168.0.115: icmp_req=4 ttl=64 time=270 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=5 ttl=64 time=260 ms
64 bytes from 192.168.0.115: icmp_req=5 ttl=64 time=260 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=6 ttl=64 time=262 ms
64 bytes from 192.168.0.115: icmp_req=6 ttl=64 time=262 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=7 ttl=64 time=261 ms
64 bytes from 192.168.0.115: icmp_req=7 ttl=64 time=261 ms (DUP!)
64 bytes from 192.168.0.115: icmp_req=8 ttl=64 time=259 ms
64 bytes from 192.168.0.115: icmp_req=8 ttl=64 time=259 ms (DUP!)
```

So you see how easy and seamless operation it is to make the DCE'd VM up and running in vCHS after any kind of disaster happens 😊