

NetApp HCI Disaster Recovery with Cleondris

NetApp HCI Solutions

NetApp August 29, 2024

This PDF was generated from https://docs.netapp.com/us-en/hcisolutions/cleondris_installing_cleondris.html on August 29, 2024. Always check docs.netapp.com for the latest.

Table of Contents

TR-4830: NetApp HCI Disaster Recovery with Cleondris	. 1
Overview of Business Continuity and Disaster Recovery	. 1
Business Impact Assessment	. 1
Application Catalog	. 1
What Not to Protect	. 1
Product Overview	. 1
Installing Cleondris: NetApp HCI DR with Cleondris	. 2
Configuring Cleondris: NetApp HCI DR with Cleondris	. 7
Replication	9
Disaster Recovery Pairing: NetApp HCI DR with Cleondris	9
Recovery organization	13
Failover: NetApp HCI DR with Cleondris	19
Where to Find Additional Information: NetApp HCI DR with Cleondris	24

TR-4830: NetApp HCI Disaster Recovery with Cleondris

Michael White, NetApp

Overview of Business Continuity and Disaster Recovery

The business continuity and disaster recovery (BCDR) model is about getting people back to work. Disaster recovery focuses on bringing technology, such as an email server, back to life. Business continuity makes it possible for people to access that email server. Disaster recovery alone would mean that the technology is working, but nobody might be using it; BCDR means that people have started using the recovered technology.

Business Impact Assessment

It is hard to know what is required to make a tier 1 application work. It is usually obvious that authentication servers and DNS are important. But is there a database server somewhere too?

This information is critical because you need to package tier 1 applications so that they work in both a test failover and a real failover. An accounting firm can perform a business impact assessment (BIA) to provide you with all the necessary information to successfully protect your applications: for example, determining the required components, the application owner, and the best support person for the application.

Application Catalog

If you do not have a BIA, you can do a version of it yourself: an application catalog. It is often done in a spreadsheet with the following fields: application name, components, requirements, owner, support, support phone number, and sponsor or business application owner. Such a catalog is important and useful in protecting your applications. The help desk can sometimes help with an application catalog; they often have already started one.

What Not to Protect

There are applications that should not be protected. For example, you can easily and cheaply have a domain controller running as a virtual machine (VM) at your disaster recovery site, so there is no need to protect one. In fact, recovering a domain controller can cause issues during recovery. Monitoring software that is used in the production site does not necessarily work in the disaster recovery site if it is recovered there.

It is usually unnecessary to protect applications that can be protected with high availability. High availability is the best possible protection; its failover times are often less than a second. Therefore, disaster recovery orchestration tools should not protect these applications, but high availability can. An example is the software in banks that support ATMs.

You can tell that you need to look at high-availability solutions for an application when an application owner has a 20-second recovery time objective (RTO). That RTO is beyond replication solutions.

Product Overview

The Cleondris HCI Control Center (HCC) adds disaster recovery capabilities to new and existing NetApp HCI deployments. It is fully integrated with the NetApp SolidFire storage engine and can protect any kind of data and applications. When a customer site fails, HCC can be used to recover all data at a secondary NetApp HCI

site, including policy-based VM startup orchestration.

Setting up replication for multiple volumes can be time consuming and error prone when performed manually. HCC can help with its Replication Wizard. The wizard helps set up the replication correctly so that the servers can access the volumes if a disaster occurs. With HCC, the VMware environment can be started on the secondary system in a sandbox without affecting production. The VMs are started in an isolated network and a functional test is possible.

Installing Cleondris: NetApp HCI DR with Cleondris

Prerequisites

There are several things to have ready before you start with the installation.

This technical report assumes that you have your NetApp HCI infrastructure working at both your production site and your disaster recovery site.

- DNS. You should have DNS prepared for your HCC disaster recovery tool when you install it.
- FQDN. A fully qualified domain name for the disaster recovery tool should be prepared before installation.
- IP address. The IP will be part of the FQDN before it is put into DNS.
- **NTP.** You need a Network Time Protocol (NTP) server address. It can be either your own internal or external address, but it needs to be accessible.
- Storage location. When you install HCC, you must know which datastore it should be installed to.
- vCenter Server service account. You will need to have a service account created in vCenter Server on both the disaster recovery and production side for HCC to use. It does not require administrator-level permissions at the root level. If you like, you can find exactly what is required in the HCC user guide.
- **NetApp HCI service account.** You need a service account in your NetApp HCI storage for both the disaster recovery and production side for HCC to use. Full access is required.
- **Test network.** This network should be connected to all your hosts in the disaster recovery site, and it should be isolated and nonrouting. This network is used to make sure applications work during a test failover. The built-in test network that is temporary only is a one-host network. Therefore, if your test failover has VMs scattered on multiple hosts, they will not be able to communicate. I recommend that you create a distributed port group in the disaster recovery site that spans all hosts but is isolated and nonrouting. Testing is important to success.
- **RTOs.** You should have RTOs approved by management for your application groups. Often it is 1 or 2 hours for tier 1 applications; for tier 4 applications, it can be as long as 12 hours. These decisions must be approved by management because they will determine how quickly things work after a critical outage. These times will determine replication schedules.
- **Application information.** You should know which application you need to protect first, and what it needs to work. For example, Microsoft Exchange needs a domain controller that has a role of Global Catalog to start. In my own experience, a customer said that they had one email server to protect. It did not test well, and when I investigated, I discovered the customer had 24 VMs that were part of the email application.

Download Information

You can download HCC from the Cleondris site. When you buy it, you receive an email with a download link as well.

License

Your license will arrive in an email when you purchase or if you get a not-for-resale (NFR) version. You can get a trial license through the Cleondris Support Portal.

Deployment

You download an OVF file, so it is deployed like many other things.

1. Start by using the Actions menu available at the cluster level.

🗊 NetApp-HCI-Cluster-01 🛛	ACTIONS ~
ummary Monitor Configure Perm	Actions - NetApp-HCI-Cluster-01
Total Processors: 64 Total vMotion Migrations: 21	 Add Hosts New Virtual Machine New Resource Pool Deploy OVF Template

2. Select the file.

1 Select an OVF template	Select an OVF template
2 Select a name and folder	Select an OVF template from remote URL or local file system
3 Select a compute resource	
4 Review details	Enter a URL to download and install the OVF package from the Internet, or bro
5 Select storage	location accessible from your computer, such as a local hard drive, a network
5 Ready to complete	CD/DVD drive.
	OURL
	http://remoteserver-address/filetodeploy.ovf .ova
	O Local file
	Choose Files cleondris-appliance-1705.ova

3. Name the appliance and select the location for it in the vCenter infrastructure.

Deploy OVF Template 1 Select an OVF template Select a name and folder Specify a unique name and target location 3 Select a compute resource Virtual machine name: dr-hcc 4 Review details 5 Select storage Select a location for the virtual machine. 6 Ready to complete sfps-cbacon-vcsa.rtp.openenglab.netapp.com V NetApp-HCI-Datacenter-01 > Appliances > 🚞 Backup > The FinBot App > SQL > Templates > 🗀 Windows

- 4. Select the Compute location.
- 5. Confirm the details.
- 6. Accept the license details.
- 7. Select the appropriate storage location.
- 8. Select the network that our appliance will work on.
- 9. Review the details again and click Finish.
- 10. Now wait for the appliance to be deployed, and then power it up. As it powers up, you might see a message saying that VMware tools are not installed. You can ignore this message; it will go away automatically.

Initial Configuration

To start the initial configuration, complete the following steps:

 This phase involves doing the configuration in the Appliance Configurator, which is the VM console. So, after the appliance powers up, change to work in the console by using the VMware Remote Console (VMRC) or the HTML5 VMRC version. Look for a blue Cleondris screen.



- 2. Press any key to proceed, and configure the following:
 - The web administrator password
 - $\circ\,$ The network configuration: IP, DNS, and so on
 - The time zone
 - NTP
- 3. Select the Reboot and Activate Network/NTP Settings. You will see the appliance reboot. Afterward, do a ping test to confirm the FQDN and IP.

Patching Cleondris

To update your Cleondris product, complete the following steps:

1. When you first log in to the appliance, you see a screen like the following:



2. Click Choose File to select the update you downloaded from the Cleondris website.

Almost done!	
ou have successfully installed this Cleondris appliance and configured it for	or network access.
o ensure the best experience, you now need to install the latest update on which you can download from the Cleondris website.	of your Cleondris product
lease select the .zip file containing the update:	
Choose File cdm-linux-x644.2001P6.zip	
	🚯 Update

3. Upload the patch. After the appliance reboots, the following login screen is displayed:

CLEONE	8.0.2004
login	
password	

4. You can now see the new version and build information; confirming that the update was successful. Now you can continue with the configuration.

Software Used

This technical report uses the following software versions:

- vSphere 6.5 on production
- vSphere 6.7 U3 on DR
- NetApp Element 11.5 on production
- NetApp Element 12.0 on DR
- Cleondris HCC 8.0.2007 Build 20200707-1555 and 8.0.2007X2 build 20200709-1936.

Configuring Cleondris: NetApp HCI DR with Cleondris

You now configure Cleondris to communicate with your vCenter Servers and storage. If you have logged out, returned, and log in again to start here, you are prompted for the following information:

- 1. Accept the EULA.
- 2. Copy and paste the license.
- 3. You are prompted to perform configuration, but skip this step for now. It is better to perform this configuration as detailed later in this paper.
- 4. When you log back in and see the green boxes, you must change to the Setup area.

Add vCenter Servers

To add the vCenter Servers, complete the following steps:

1. Change to the VMware tab and add your two vCenter Servers. When you are defining them, add a good description and use the Test button.

Hostname	10.193.139.52	se Update
Username	cadmin@vsphere.local	+ Add HCI/SolidFire
Password	Change Password	-n
Host filter	i	
Description	Prod	

This example uses an IP address instead of an FQDN. (This FQDN didn't work at first; I later found out that I had not entered the proper DNS information. After correcting the DNS information, the FQDN worked fine.) Also notice the description, which is useful.

2. After both vCenter Servers are done, the screen displays them.

VMware vCenter			+ Add v	Center
Hostname	Username	Descriptior	t.	
sfps-megatron- vcsa.rtp.openenglab.netapp.com	cadmin@vsphere.local	Prod	B	1
sfps-cbacon-vcsa.rtp.openenglab.netapp.com	administrator@vsphere.local	DR	1	會

Add NetApp HCI Clusters

To add the NetApp HCI clusters, complete the following steps:

1. Change to the NetApp tab and add your production and disaster recovery storage. Again, add a good description and use the Test button.

Register HCI/Solid	dFire	
Hostname	10.193.139.9	
Username	admin	
Password	•••••	
Description	DR	
✓ Credentials are OK!	Test Sa	ve Cancel
the second s		

2. When you have added your storage and vCenter Servers, change to the Inventory view so that you can see the results of your configuration.

Cleondris							inventory search	Q O Sett	tings	(+ Logout
0										
Status	HCI/SolidFire (2)		I# DR	Wizard	Dashboard	0	VCenter (2)			
	Hostname	Name	Vol	VM			▲ vCenter	Hosts	VMs	
Fallover	10.193.139.9	sfps-cbacon-cluster	12	12	2	-	sfps-cbacon-ucsa.rtp.openengiab.netapp.com	2	12	C
Setup:	10.193.139.58	sfps-megatron-cluster	26	134	0	4	sfps-megatron-vcsa.rtp.openenglab.netapp.com	5	130	C

Here you can see the number of objects, which is a good way to confirm that things are working.

Replication

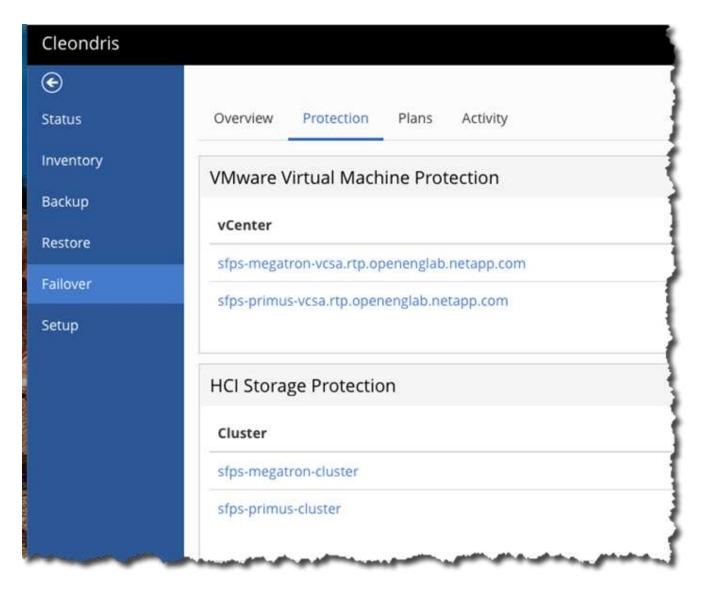
You can use HCC to enable replication between your two sites. This allows us to stay in the HCC UI and decide what volumes to replicate.

Important: If a replicated volume contains VMs that are in two plans, only the first plan that fails over works because it will disable replication on that volume.

I recommend that each tier 1 application have its own volume. Tier 4 applications can all be on one volume, but there should be only one failover plan.

Disaster Recovery Pairing: NetApp HCI DR with Cleondris

- 1. Display the Failover page.
- 2. On the diagram of your vCenter Servers and storage, select the Protection tab.



The far side of the screen displays some useful information, such as how many protected VMs you have. (In this example, none right now.) You can also access the Replication Wizard here.

Protected Datastores	Protected VMs
0/24	0/133
0/5	0/6
	 # Replication Wizard
Protected Datastores	Protected VMs
0/17	0/137
0/3	0/6
212	0/6

1 dei

This wizard makes the replication setup easy.

Source	Volum	nes Dest	tination vCenter Preview
Select the	e cluste	er you want	to protect:
Cluster:		sfps	s-megatron-cluster
	ID	Туре	Name
0	1	Primary	NetApp-HCI-Datastore-01
0	2	Primary	NetApp-HCI-Datastore-02
0	3	Primary	NetApp-HCI-Select-Install
0	4	Primary	NetApp-HCI-Select-Data-01
	5	Primary	NetApp-HCI-Select-Data-02
	6	Primary	NetApp-HCI-Select-Data-03
0	7	Primary	NetApp-HCI-Select-Data-04
	8	Primary	INFRASTRUCTURE
0	12	Primary	DESKTOP02
	15	Primary	DESKTOP03
	16	Primary	DESKTOP04
	569	Primary	workload-db-mongo-1

3. You can select the volumes that are important to you, but also make sure that you have the proper vCenter Server selected at the top in the cluster field.

At the far right, you see the pairing type, and only Sync is allowed or supported.

After you click Next, the destination area is displayed.

Source Volumes De	stination vCenter Preview	
ect the destination clu	ster:	
ister:	sfps-primus-cluster	\$
count:	NetApp-HCI	\$
ume Postfix:		i

4. The default information is normally right, but it's still worth checking. Then click Next.

Source Volumes De	stination vCent	ter Preview	
select the hosts on which	the DR volumes sh	nould be available:	
Center:	sfps-prim	nus-vcsa.rtp.openenglab.netapp.com	
 Im NetApp-HCI-Datace 	nter		
☞ 🛽 10.193.139.93			

It is important to make sure that the disaster recovery site vCenter Server is displayed and that all hosts are selected. After that is complete, use the Preview button.

5. Next you see a summary. You can click Create DR to set the volume pairing and start replication.

Depending on your settings, replication might take a while. I suggest that you wait overnight.

Recovery organization

Disaster Recovery Orchestration

This section discusses successful failover of applications in a crisis or in a planned migration. It first looks at protecting complex multitier applications, and then simpler applications. You can build disaster recovery plans that are slow or fast, so this section provides examples of the highest-performing plans.

Multitier Applications

1. From the Failover page, select the Plans tab.

Cleondris HCC	
e	
Status	Overview Protection Plans Activity
Inventory	Failover Plans
Backup	
Restore	Name
Failover	No failover plans have been defined
Setup	
	and the second

2. On the far right is an +Add Failover Group button.

an Name:			
eate temporary network when running sandbox mode:	0		
Failover Groups			+ Add Fallover Group
Prio Name VM Filter	Additional VMs Delay	Unregister Wait for Tools	
No failover groups have been defined ye		Storage Affinity	+ Add Storage Affinity
	 Edit Network Mapping DR Network 	Storage Affinity Storage System	+ Add Storage Affinity Hosts
Network Mapping	Edit Network Mapping DR Network		Hosts
Network Mapping Production Network	Edit Network Mapping DR Network	Storage System	Hosts

In this example, we called this plan Multi-tier. We will use the network mapping in the bottom left to change the virtual switch that is in use on production to the one in use on DR.

duction	DR	Mappings	
nter sfps-megatron-vcsa. 🖨	vCenter sfps-primus-vcsa.rtp 🖨	From	То
acente NetApp-HCI-Datacer 🖨	Datacent(NetApp-HCI-Datacer 🖨	Map 10.193.138.0_VL20	NetApp HCI VDS 01-
	NetApp HCI Uplinks 01		VM_Network
HCI_Internal_OTS_Network	O NetApp HCI VDS 01-		
K8S-PG	HCI_Internal_Storage_Network		
Desktops	 NetApp HCI VDS 01- HCI_Internal_mNode_Network 		
VM_Network	NetApp HCI VDS 01-		
HCI_Internal_vCenter_Network	Management Network		
NetApp HCI Uplinks	 NetApp HCI VDS 01- HCI_Internal_NKS_Managemen 		
10.193.138.0_VL20	NetApp HCI VDS 01-		
vMotion	HCI_Internal_NKS_Data		
Management Network	C TestNetwork		
	 NetApp HCI VDS 01- VM_Network 		
	O NetApp HCI VDS 01-vMotion		
	 NetApp HCI VDS 01- HCI_Internal_vCenter_Network 		

The previous screenshot shows how you can choose the network switch in production and then in DR, use the Map button to select them, and then use Save. You can have more than one mapping if necessary.

3. To select the VMs to protect, click Add Failover Group.

Because this plan will protect multitier applications, the first group will be for databases.

d Failover Group		
ame	Database	
elay	0	ž.
VMs Scripts Environr	ent Variables	
clude VMs by name		X
nregister source VMs		
ait for VMware Tools (if stalled)	0	
ax wait time	lm	ĩ
Additional VMs		+ Add VM
Name		
FinRptdb		8
crmdb		8
taxdb		8
		OK Cance

Notice how this example enables Wait for VMware Tools. This setting is important, because it helps make sure that the applications are running. We used the Add VM button to add VMs that are databases. We didn't enable Unregister Source VMs, because it will slow down the failover. We now use the Add Failover button to protect the applications.

4. Do the same thing for web servers. When that is done, the screen resembles the following example.

lan Nar	me:		MultiTier							
	emporary network ox mode:	when running	٥							
Failov	ver Groups							+ Add	Failove	r Group
Prio	Name	VM Filter	Additional VMs	Delay	Unregister	Wait for Tools				
1	Database		FinRptdb,crmdb,taxdb	0		~		*	1	ê
2	Apps		FinRptA,crmA,taxA	0		~	۴	+	1	ŝ
3	Web		FinRptW,crmW,taxW	0		*	1		1	8
Netw	ork Mapping			Storage Affini	ty			+ Add S	Storage	Affinity
Produ	uction Network	DR Net	work	Storage System	U.		Hosts			
10.19	3.138.0_VL20	NetApp	HCI VDS 01-VM_Network	No hosts are associated to specific storage cluster						
				- 5						Y
									Save	Cancel

The important part of this plan is to get all the databases working; then the applications start, find the databases, and start working. Then the web servers start, and the applications are complete and working. This approach is the fastest way to set up this sort of recovery.

5. Click Save before you continue.

Simple or Mass Applications to Fail Over

The order in which the VMs start is important, so that they work; that is what the previous section accomplished. Now we will fail over a set of VMs for which order is unimportant.

Let's create a new failover plan, with one failover group that has several VMs. We still need to do the network mapping.

an Name:	Mass		
eate temporary network when runnin sandbox mode:	g 🖉		
Failover Groups			+ Add Failover Group
Prio Name VM Filter Addition	al VMs		
1 VMs mass01,	nass02,mass03,mass04,mass06,mass05,mass	07,mass08,mass09,mass10,mass11,mass12,n	nass13,mass14,mass15,mass16,mass17,mass1
2 - 19224	nass02,mass03,mass04,mass06,mass05,mass	07,mass08,mass09,mass10,mass11,mass12,m	hass13,mass14,mass15,mass16,mass17,mass1 + Add Storage Affinity
Network Mapping			
Network Mapping Production Network DR	Edit Network Mapping	Storage Affinity	Hosts

Notice that there are several VMs in this plan. They will also start at different times, but that is OK because they are not related to each other.

Planned Migration

Planned migration is similar to a disaster recovery failover, but because it is not a disaster recovery situation, it can be handled slightly differently. It is still good to practice the planned migration, but you can add something to your failover group: You can unregister the VM from the source. That takes a little more time, but in a planned migration that is not a bad thing.

A planned migration is usually a move to a new domain controller. Sometimes it is also used if destructive weather is approaching but has not yet arrived.

Plan of Plans

With a plan of plans, you can trigger one plan and it will take care of all the failover plans.

The Plans tab contains a Plan of Plans section. You can use the +Add Sub-Plan to start a plan and add other plans to it.

lan of Plans Name:	Master Plan	
Sub-Plan Name		
Mass		Ψ ×
MultiTier		* ×
		Save Cancel

In this example, the plan of plans is called Master Plan, and we added the two plans to it. Now when we execute a failover, or test failover, we will have the option for the Master Plan too.

This approach is good because it is best to test your application failovers in their own plan. Each plan is much easier to troubleshoot and fix, and when it is working well, you add it to your master plan.

Failover: NetApp HCI DR with Cleondris

Test Failover

A test failover is important, because it proves to you, your application owner, your manager, and the BCDR people that your disaster recovery plan works.

To test failover, complete the following steps:

1. From the Failover page, click Start Failover.

Cleondris H	CC Inventory search	۹	Settings	🗭 Logout
۲				
Status	Overview Protection Plans Activity			
Inventory	Overview		≓ Sta	art Failover
Backup	and the second	and second		

2. On the Failover page, you have some choices to make.

Failover Plan	MultiTier	\$
Source HCI Cluster	sfps-megatron-cluster	\$
Destination HCI Cluster	sfps-primus-cluster	\$
Destination vCenter	sfps-megatron-vcsa.rtp.openenglab.netapp.com	¢
Destination Datacenter	NetApp-HCI-Datacenter	\$

Carefully specify the plan, where the VMs came from, and where they are going to be recovered.

				From: sfps-meg	atron-cluster To:	sfps-primus-cluster 🛛 🗛 3 VMs not include	d in this plan will lose protection
Plan	Priority	Name	Datastore	Source Volume	Destination Volume	Current vCenter	Destination vCenter
MultiTier	1	taxdb	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	1	crmdb	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	1	FinRptdb	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	2	crmA	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	2	FinRptA	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	2	taxA	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	3	taxW	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	3	crmW	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
MultiTier	3	FinRptW	DESKTOP03	DESKTOP03 ID: 15	DESKTOP03 ID: 138	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-megatron-vcsa.rtp.openeng
						Failover	to Sandbox Start Cancel

The screen displays a list of the VMs that are in the plan. In this example, a warning at the top right says that three VMs are not included. That means there are three VMs we did not make part of the plan in the replicated volume.

If you see a red X in the first column on the left, you can click it and learn what the problem is.

3. At the bottom right of the screen, you must choose whether to test the failover (Failover to Sandbox) or start a real failover. In this example, we select Failover to Sandbox.

G								
Status	Over	view Protection Plans Activity						
Inventory	Failc	ver Plan Execution					Show	Historical
Backup								
Restore	Id	Description	User	Plan	Date	Status		
	2	Sandbox failover using plan Mass	admin	Mass	2020-04-14 13:21	Running	0	Q
etup								

4. A summary now lists plans in action. For more information, use the magnifying glass in the far left (described in "Monitoring," later in this document).

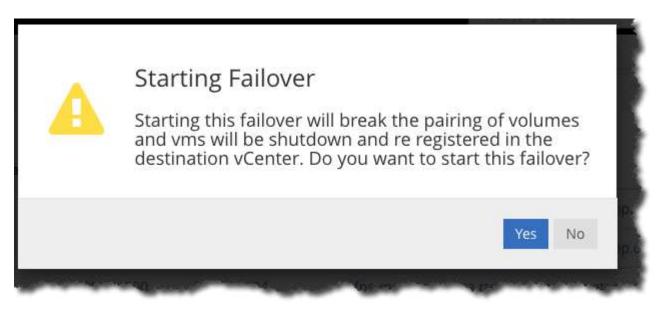
Running Failover

At first, the failover is the same as the test failover. But the procedure changes when you arrive at the point shown here:

1. Instead of selecting the Failover to Sandbox option, select Start.

IS	Failove	r Preview	1					
tory					From	sfps-megatron-cluste	r To: sfps-primus-cluster	
ıр	Plan	Priority	Name	Datastore	Source Volume	Destination Volume	Current vCenter	Destination vCenter
re	ABC	1	ABC01	ABC	ABC ID: 800	ABC ID: 134	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-primus-vcsa.rtp.openenglab.netapp.co
I r	ABC	1	ABC03	ABC	ABC ID; 800	ABC ID: 134	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-primus-vcsa.rtp.openenglab.netapp.co
	ABC	1	ABC02	ABC	ABC ID: 800	ABC ID: 134	sfps-megatron-vcsa.rtp.openenglab.netapp.com	sfps-primus-vcsa.rtp.openenglab.netapp.co
								Failover to Sandbox Start Cancel

2. Select Yes.



3. The screen shows that this is a failover, and it is running. For more information, use the magnifying glass (discussed in the "Monitoring" section).

	-						
lover Plan Executio	n					Show H	istorical
Description		User	Plan	Date	Status		
Failover using plan	ABC	admin	ABC	2020-04-15 08:25	Running	0	Q
	Description	over Plan Execution Description Failover using plan ABC	Description User	Description User Plan	Description User Plan Date	Description User Plan Date Status	Description User Plan Date Status

Monitoring During a Failover

1. When a failover or a test failover is running, you can monitor it by using the magnifying glass at the far right.

С			Inventory search		Q Se	ttings	🕩 Logou
Overv	iew Protection Plans Activity						
Failo	ver Plan Execution					Show I	Historical
, and							
Id	Description	User	Plan	Date	Status		
2	Sandbox failover using plan Mass	admin	Mass	2020-04-14 13:21	Running	\odot	Q
	Overv Failo	Overview Protection Plans Activity Failover Plan Execution Id Description	Overview Protection Plans Activity Failover Plan Execution User	Overview Protection Plans Activity Failover Plan Execution User Plan	Overview Protection Plans Activity Failover Plan Execution User Plan Date	Overview Protection Plans Activity Failover Plan Execution User Plan Date Status	Overview Protection Plans Activity Failover Plan Execution Show Plans Id Description User Plan Date Status

2. Click the magnifying glass to see much more detail.

Cleondris H	ICC			Inventory search	۹	🖨 Settings	🕩 Logout
۲							
Status						📥 Downlo	ad Report
Inventory	Ticket: Started:		idbox failover using plan Mass 10-04-14 12:30				
Backup	Status:	Fini	shed				
Restore	Log Details						
	Date	Туре	Message				
Setup	2020-04-14 12:30	Log	Starting failover activity using plan 'Mass'				
	2020-04-14 12:30	Log	Sandbox mode = on				
	2020-04-14 12:30	Log	Creating clone of volume 137				
	and the second se	مىر	and a second	and and an and a second second second	man	-	and an and

3. As the failover or test failover progresses, a VM Screenshots option appears.

Cleondris H	ICC					
۲	H					
Status			(
Inventory	Ticket: Started:	Sandbox failover using plan Mass 2020-04-14 13:29				
Backup	Status:	WaitRe	lease			
Restore	Log Details	VM Screenshots				
Failover	Date	Туре	Message			
Setup	2020-04-14 13:29	Log	Starting failover activity using plan 'Mass'			
	2020-04-14 13:29	Log	Sandbox mode = on			

Sometimes it is useful to see the screenshots to confirm that the VM is running. It is not logged in, so you cannot tell if the applications are running, but at least you know that the VM is.

Looking at History When No Failover Is Running

To view past tests or failovers, click the Show Historical button on the Activity tab. Use the magnifying glass for more detail.

€								
tatus	Oven	view Protection Plans Activity						
nventory	Failo	ver Plan Execution					Show H	Historical
lackup								
Restore	Id	Description	User	Plan	Date	Status		
	2	Sandbox failover using plan Mass	admin	Mass	2020-04-14 13:21	Running	¢	Q
tup								

e	16							
status	Overv	view Protection Plans Activity						
nventory	Failo	ver Plan Execution					Hide I	Historical
Backup				24		-		
lestore	Id	Description	User	Plan	Date	Status		
ailover	2	Sandbox failover using plan Mass	admin	Mass	2020-04-14 13:21	Running	ं	Q
allover	1	Sandbox failover using plan Mass	admin	Mass	2020-04-14 12:30	Finished		Q
etup								

You can also download a report with the details.

Cleondris H	ICC			Inventory search	Q	Settings	🕞 Logout
۲							
Status						📥 Downloa	ad Report
Inventory	Ticket: Started:		dbox failover using plan Mass 0-04-14 12:30				
Backup	Status:	Fini	shed				
Restore	Log Details						
Failover	Date	Туре	Message				
Setup	2020-04-14 12:30	Log	Starting failover activity using plan 'Mass'				
	2020-04-14 12:30	Log	Sandbox mode = on				
	2020-04-14 12:30	Log	Creating clone of volume 137				
	and the second second	مىر. مى	and the second and a strend address of the second as	an and the second se	maan	-	and and and

These reports have various uses: for example, to prove to an application owner that you tested the failover of that application. Also, the report can provide details that might help you troubleshoot a failed failover.

You can add text to a report by adding the text to the plan in the comment field.

Failover Plan Editor	
Plan Name:	ABC
Comment (Added to the report)	App expert is Joe Smith.
Create temporary network when running in sandbox mode:	
Network to use for sandbox mode	TestNetwork

Where to Find Additional Information: NetApp HCI DR with Cleondris

To learn more about the information that is described in this document, review the following websites:

- NetApp HCI Documentation Center https://docs.netapp.com/hci/index.jsp
- NetApp HCI Documentation Resources page https://www.netapp.com/us/documentation/hci.aspx
- NetApp Product Documentation https://www.netapp.com/us/documentation/index.aspx
- Cleondris HCC product page
 https://www.cleondris.com/en/hci-control-center.xhtml
- Cleondris Support Portal https://support.cleondris.com/

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.