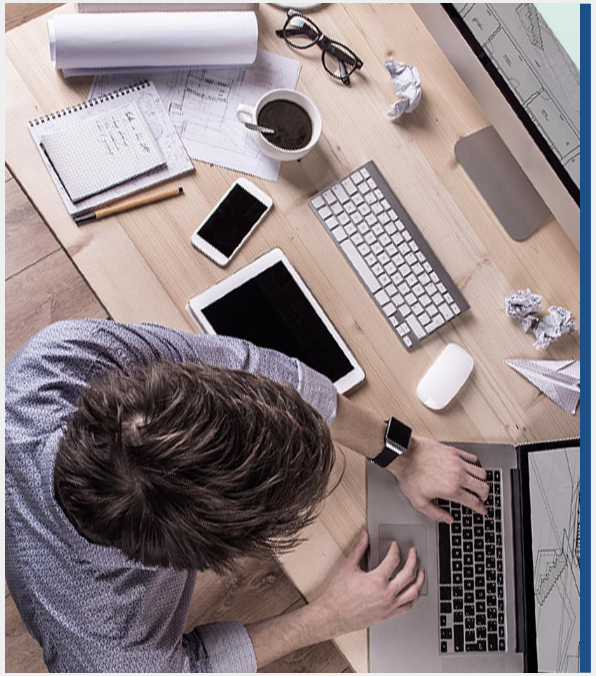
aCloud_5.8.6

Sangfor Disaster Recovery Solution

Blake Chen
20181023



1 Overview of disaster recovery needs

2 Sangfor Disaster Recovery Solution Introduction

3 aCloud586 Disaster Recovery Function Configuration Guide

4 Disaster tolerance POC

1. Overview of disaster recovery needs

SANGFOR
深信服科技

Overview of disaster recovery needs

- According to market conditions, many users are concerned about data security and business continuity of their services. Backup and CDP are no longer able to meet more scenarios, which has led to the need for disaster recovery. Customer service requires high security level data protection and service continuity protection. In addition to local backup and local CDP protection data, it also needs remote disaster recovery solution to prevent disasters (earthquakes, fires, etc.) in the entire equipment room, resulting in data loss or excessive business interruption.

- From the perspective of policy, banks, education, medical and other industries have clear regulations for disaster recovery. From the perspective of existing projects, some projects use backup and CDP to build disaster recovery plans, which cannot meet the policy requirements for fast recovery services.

- Not only from the perspective of user needs, but also the improvement of product competitiveness, or the evolution direction of aCloud, disaster tolerance is the most urgent value at present.

Key indicators of disaster tolerance - RPO and RTO

For information systems, disaster tolerance is the ability of information systems to respond to certain disasters and maintain systematic or intermittent operations. At present, everyone is more accustomed to using some technical indicators to measure the performance and needs of disaster recovery systems. RPO and PTO are the two most important indicators of disaster recovery

- **RTO（Recovery Time Objective）**， mainly refers to the longest time that the tolerable application stops the service, that is, the shortest time period required from the disaster occurrence to the service system recovery service function. RTO is an indicator reflecting the timeliness of business recovery, indicating the time required for the service to be interrupted to return to normal. The smaller the value of RTO, the stronger the data recovery capability of the disaster recovery system.

- **RPO（RPO: Recovery Point Objective）**，RPO is an indicator reflecting the integrity of data recovery. It takes data as the starting point and mainly refers to the amount of data loss that the business system can tolerate.

DR overview: Business prioritization

Business systems in data center are varying, so are the priorities. Considering O&M complexity, investment and system architecture, DR solutions for different business systems can differ. A good DR solution must be designed based on business architecture and priority.

Business types and corresponding DR solutions are divided as below:

Business type	Description	Requirement	DR solution

Core business	Type A business, most business-critical applications such as ERP, finance, order system, etc.	RPO= seconds or 0,
		RTO= seconds or 0
			Provide local backup + off-site DR solution with minutes RTO and seconds RPO, or active active solution with RPO=0 and RTO=0

Major business	Type B business, improve employees' efficiency and support internal process, such as email, BI, OA, etc.	RPO= minutes, RTO= minutes	Provide local backup + off-site DR solution with minutes RTO and minutes RPO

Common business	Type C business, no big impact on production when failure occurs, examples are knowledge base, online learning system, testing business and such	RPO= hours
		RTO= hours
			Provide local backup + off-site DR solution with hours RTO and hours RPO

DR overview: Solution sizing

Minimum RPO and RTO that a DR solution is able to achieve can be known based on the resource types and technology characteristics on production and DR sites. However best outcome is not guaranteed under all circumstances. Generally speaking, RPO can be configured on DR management software, the factors that are actually influence RPO are always network bandwidth and data change rate within a RPO period

The table below shows some major DR types, users can choose the right DR solution considering RPO, RTO, manageability, bandwidth requirement and cost

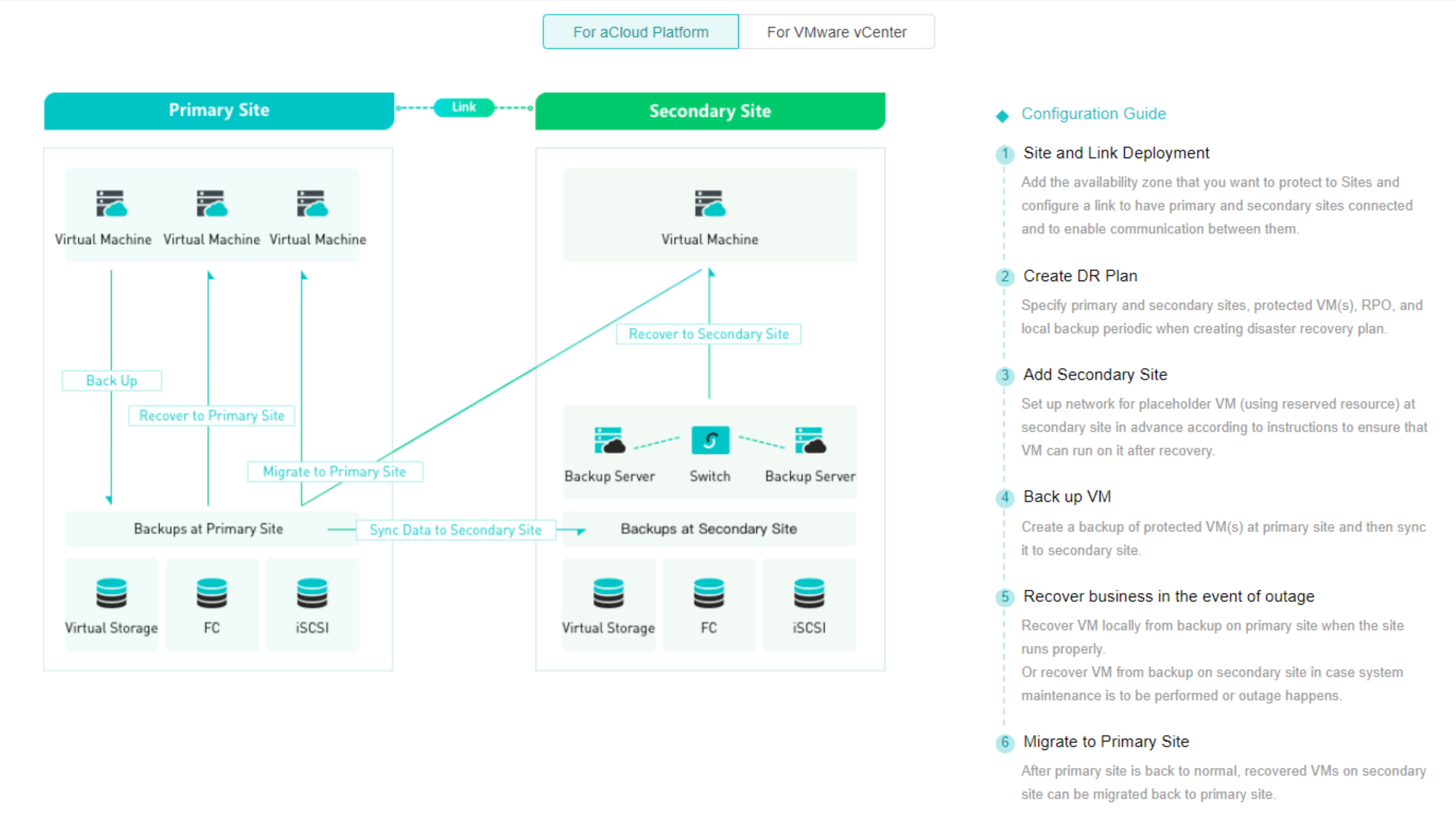
DR type	Target	Technology characteristics	Min. RPO	Min. RTO	Manageability	Bandwidth requirement	Cost
aCloud to aCloud	Application and middleware VM, and database VM	Local backup – offsite DR based on VM-level insant backup and CDP	1 second	5 mins	Easy to use, unified management	Low	Low, based on VM quantity
	Oracle、Oracle RAC10g and above	Oracle DataGuard	0	2 mins	Difficult to use, complex configuration with CLI	Low	Low, built in database
VMware to aCloud	Application and middleware VM, and standalone database VM	CBT based on VMware API	10 mins	5 mins	Easy to use, unified management	Medium high	Low, based on VM quantity
Active-active	Application, middleware and database all support clustering	Data sync technology based on traditional storage	0	0	Many middlewares with management silos, automatic failover	Very high	High cost, storage gateway needs ate least 2 high bandwidth links
	Application, middleware and database all support clustering	Data sync technology based on aCloud virtual storage	0	0	Unified management with automatic failover	Very high	High cost from virtual storage license and high bandwidth links
Physical to aCloud	Windows and Linux systems, depending on compatibility list of DR software	DR technology based on 3rd party DR software	Seconds-level		Relatively easy, separate DR management platform	Low	High cost from DR software licenses

2 Sangfor Disaster Recovery Solution Introduction

SANGFOR
深信服科技

Introduction to the DR plan

The Sangfor DR function adopts the "local backup - remote disaster recovery" solution, locally provided continuous data protection scheme in seconds. When a virtual machine fails, you can quickly restore the entire virtual machine from the local protection data， provides VM-level disaster recovery with different RPO (range 1 second to one week) in different locations.



◆ Configuration Guide

1 Site and Link Deployment

Add the availability zone that you want to protect to Sites and configure a link to have primary and secondary sites connected and to enable communication between them.

2 Create DR Plan

Specify primary and secondary sites, protected VM(s), RPO, and local backup periodic when creating disaster recovery plan.

3 Add Secondary Site

Set up network for placeholder VM (using reserved resource) at secondary site in advance according to instructions to ensure that VM can run on it after recovery.

4 Back up VM

Create a backup of protected VM(s) at primary site and then sync it to secondary site.

5 Recover business in the event of outage

Recover VM locally from backup on primary site when the site runs properly.

Or recover VM from backup on secondary site in case system maintenance is to be performed or outage happens.

6 Migrate to Primary Site

After primary site is back to normal, recovered VMs on secondary site can be migrated back to primary site.

Introduction to the DR plan

1) The primary site service data will first be backed up locally according to a pre-configured backup scheme (timed backup or CDP)

2) Then, through the data link, the backup data is synchronized to the standby site to provide data security. Because of this implementation, we can support the fast boot of the local virtual machine at the primary site and reduce the high dependence on the stability of the off-site data transmission link.

Advantages of the DR solution

Minute level RTO, second level PRO

- Provide local backup-site disaster recovery solution, which can be preferentially restored locally during service failure.

- Provides RPO configurable virtual machine level disaster recovery, the RPO range ranges from 1 second to 1 week.

- Provide one-click recovery from the standby site, you can configure the network in the standby site in advance, RTO can reach 2min

- Provides one-click function of relocating from the standby site to the primary site, and only moves back the difference data

- Support fast recovery of a single file (windows system) to avoid recovery of the entire system

Advantages of the DR solution

Easy to use, visualizing disaster tolerance status

- Simplify platform integration: Integrated in the platform, no need to purchase third-party software, provide disaster-to-rescue deployment wizard, easy to use, no learning cost, is a virtual machine level disaster recovery solution

- Monitoring operation and maintenance visualization： Provides large-screen display, which can be used to visually view the current disaster-tolerant configuration relationship and running status, and perform fault handling to facilitate operation and maintenance.

Advantages of the DR solution

Link bandwidth customization, data transmission is safe and efficient

- Guarantee data stability: provide breakpoint retransmission, encrypted transmission, and compressed transmission technology

- Protect the main service operation: customize the bandwidth of the DR link according to the RPO requirements, without affecting the main service operation.

Disaster tolerance process

Disaster tolerance initialization

The initialization of disaster tolerance includes the following steps:

1. Configure a disaster recovery plan to synchronize configuration information on the active and standby sites.
2. Automatically perform the creation of the placeholder virtual machine and the synchronization of the virtual machine configuration at the recovery site
3. Pre-configure the network topology at the recovery site (user-selectable manual operation, it is recommended to pre-configure)
4. Split scene sync data (based on the set RPO interval)

Hour-level or day-level or week-level RPO: use the regular backup + disaster recovery transmission to achieve remote disaster recovery
Second-level or minute-level RPO: Using CDP + disaster recovery transmission to achieve remote disaster recovery

Disaster tolerance process

Service recovery

Service recovery includes planned recovery, post-disaster recovery, and local virtual machine recovery

Planned recovery:

Service recovery under customer planning， at this point, the protected site is in a normal online state. Suitable for disaster recovery drills, planned shutdown, cross-site service recovery needs to be performed within the plan.

Recovery step:
1） Manually shut down the site virtual machine
2） Synchronize unsynchronized data to the recovery site
3） After the data synchronization is completed, the virtual machine is pulled up at the recovery site; the service data is not lost.

Disaster tolerance process

Service recovery

Recovery after disaster :

After sending an unexpected disaster, some unsynchronized data has been lost. The recovery site restores by default according to the latest recovery point. First, ensure that the service is online as soon as possible.

Recovery under the local VM service in unavailable:

Benefit from the support of the local backup system, support the direct boot up from the local backup when the local virtual machine is abnormal, and quickly and efficiently restore the service operation.

Disaster tolerance process

Service relocation

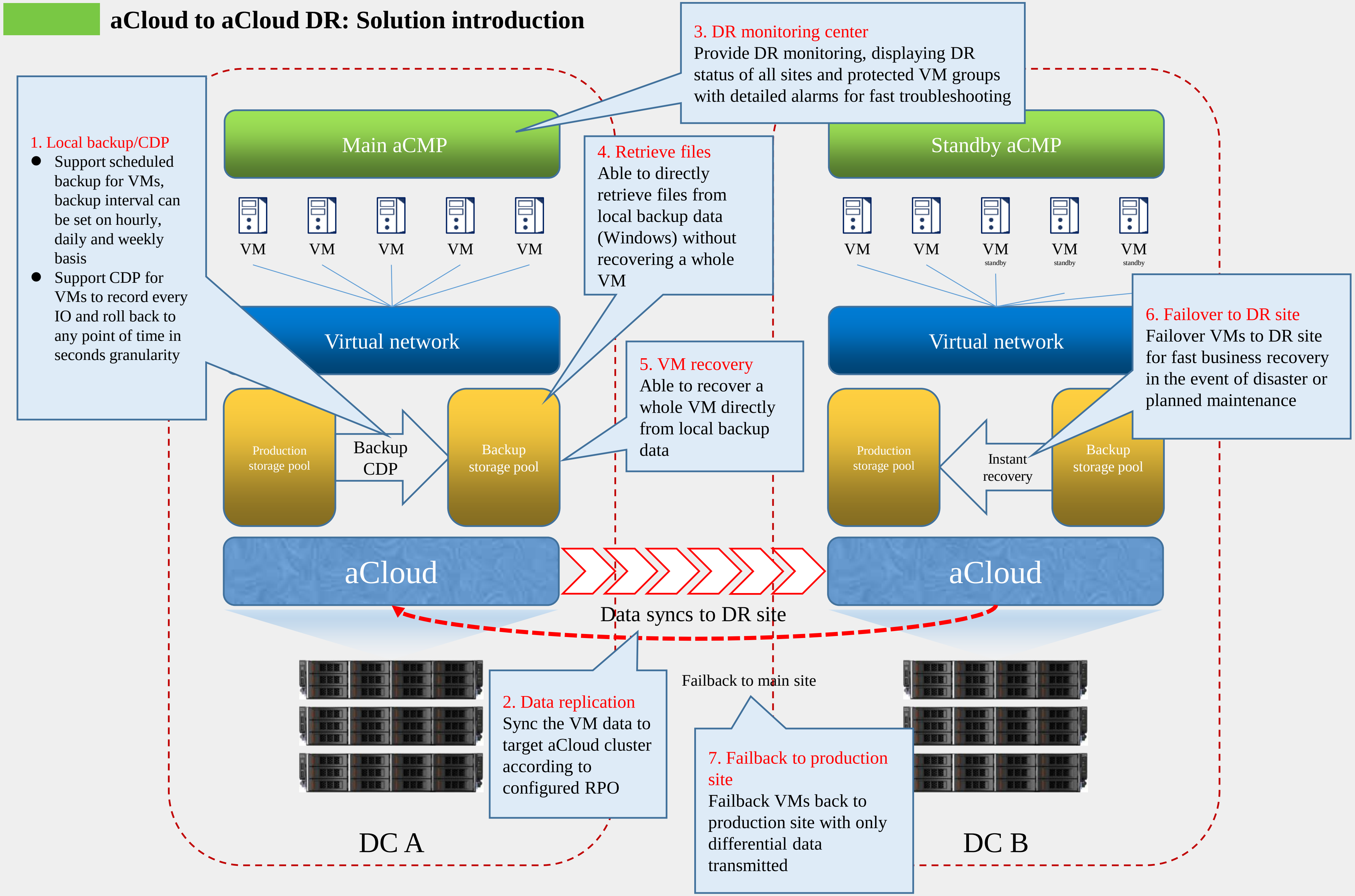
After the primary data center fails, the virtual machine can be migrated back to the primary data center.

The migration of the virtual machine to the backup is performed in the following order: full-image file, virtual machine configuration file, incremental backup file generated periodically, and iolog real-time data.

Sangfor disaster tolerance function induction

DR function type	Test item
Local disaster recovery test	Fast backup and recovery
	CDP backup and fast boot up
	CDP quick recovery accidentally deleted files
	CDP backup and fast recovery
aCloud disaster tolerance to aCloud	Planned host recovery to backup site
	Planned host moved back to the primary site
	Revert to the backup site after the disaster
	Host moves back to the primary site after disaster recovery
aCloud Vmware active and standby disaster recovery	After the plan, the host is restored to the backup site.
	Planned host moved back to the primary site
	Revert to the backup site after the disaster
	Host moves back to the primary site after disaster recovery

aCloud to aCloud DR: Solution introduction



1. Local backup/CDP

- Support scheduled backup for VMs, backup interval can be set on hourly, daily and weekly basis
- Support CDP for VMs to record every IO and roll back to any point of time in seconds granularity

2. Data replication

Sync the VM data to target aCloud cluster according to configured RPO

3. DR monitoring center

Provide DR monitoring, displaying DR status of all sites and protected VM groups with detailed alarms for fast troubleshooting

4. Retrieve files

Able to directly retrieve files from local backup data (Windows) without recovering a whole VM

5. VM recovery

Able to recover a whole VM directly from local backup data

6. Failover to DR site

Failover VMs to DR site for fast business recovery in the event of disaster or planned maintenance

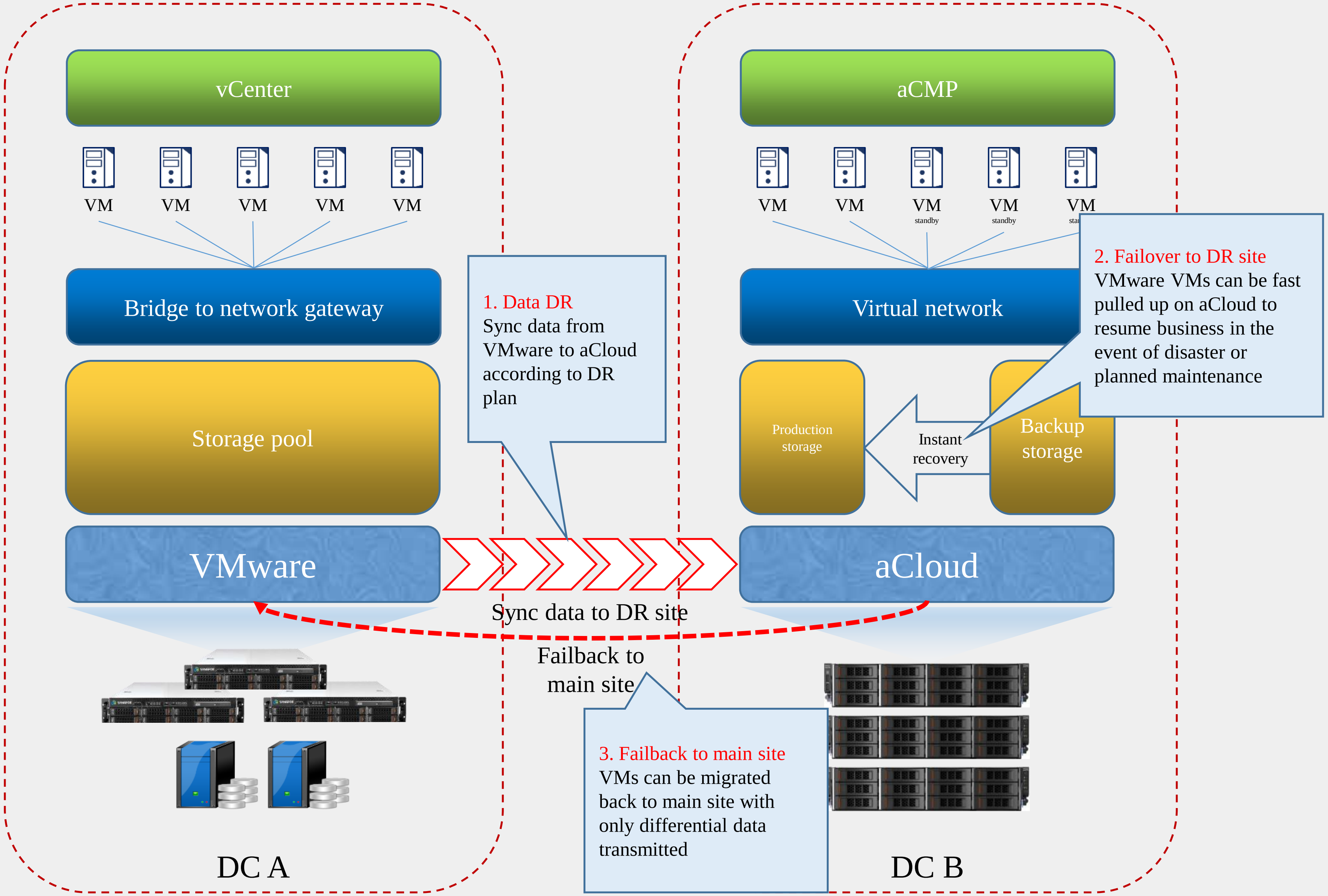
7. Failback to production site

Failback VMs back to production site with only differential data transmitted

Solution highlights:

- Integrated in the platform, no need for additional software, 1 click to enable VM-level DR solution
- Adopted "local backup – offsite DR"DR solution, instant recovery from local CDP with seconds-level continuous protection. A variety of RPOs (1s, 10s, 10mins, 30mins, 1h, 2h, 4h, 8h, 12h, 1d, 2d, weekly) for offsite DR based on aCloud
- Save bandwidth consumption by features like continuous backup from breakpoint and compressed replication
- Provide 1-click failover to DR site, network can be preconfigured to minimize RTO to 10 mins
- Provide 1-click failback to production site from DR site
- Provide main aCMP and standby aCMP for eliminate single point failure of aCMP
- Provide visualized DR monitoring with detailed running status and alarms
- Easy to use, no learning curve

VMware to aCloud DR: Solution introduction



1. Data DR
Sync data from VMware to aCloud according to DR plan

2. Failover to DR site
VMware VMs can be fast pulled up on aCloud to resume business in the event of disaster or planned maintenance

3. Failback to main site
VMs can be migrated back to main site with only differential data transmitted

Solution highlights

- Integrated in the platform, no need for additional software, 1 click to enable VMware VM-level DR
- Integrated with standard API provided by VMware, keep track of CBT data by snapshot and offer various DR intervals (10mins, 20mins, 30mins, hours and days). Only incremental data is copied.
- Provide 1-click failover, network can be preconfigured, RTO can be as minimum as 10mins
- Provide 1-click failback to main site, only differential data is transmitted
- Provide aCMP to not only configure VMware DR, but also do lifecycle management for VMware VMs
- Provide visualized DR monitoring with detailed running status and alarms
- Easy to use, no learning curve

Restrictions

- If NFS and Windows shared folder are used as backup repository, VMware VMs can only be recovered to VMware because aCloud doesn’t support to run VMs on NFS or Windows shared folder.

3. Disaster tolerance function configuration guide

SANGFOR
深信服科技

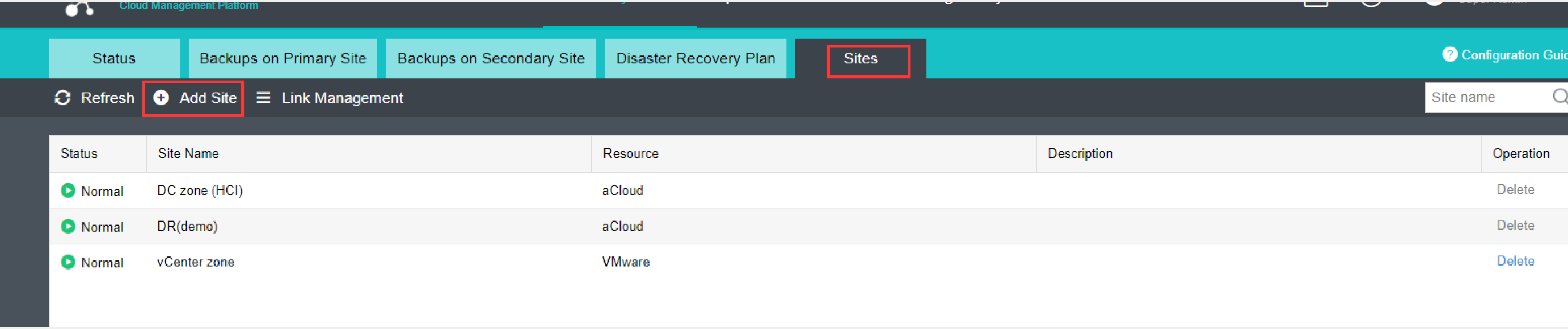
Disaster recovery configuration requirements

The DR function requires us to master the configuration points of the following configuration items:

- Site and site link configuration
- Local recovery virtual machine configuration
- Disaster recovery plan configuration
- Disaster recovery configuration
- Host service emoves back to the primary data center configuration.

Add Site

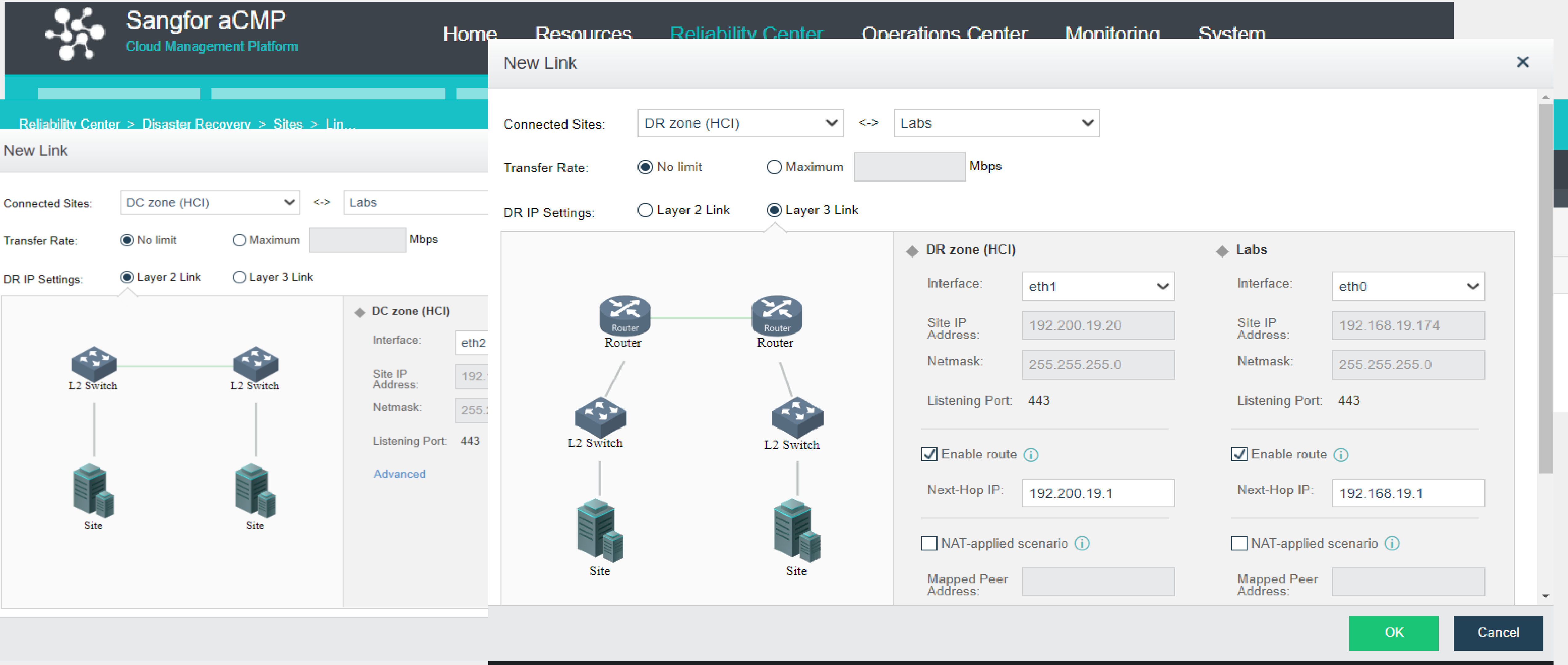
Before doing the DR plan, it needs to configure the site according to the Availability Zone. Once the site is defined, the primary site and the backup site are defined from the configured site when the disaster recovery plan is created.



Status	Site Name	Resource	Description	Operation
Normal	DC zone (HCI)	aCloud		Delete
Normal	DR(demo)	aCloud		Delete
Normal	vCenter zone	VMware		Delete

Site-Site link configuration

After configuring the site, it needs to configure the inter-site link to define the link between the data synchronization between the sites.



Sangfor aCMP
Cloud Management Platform
Home
Resources
Reliability Center
Operations Center
Monitoring
System
Reliability Center > Disaster Recovery > Sites > Lin...

New Link

Connected Sites: DC zone (HCI) <-> Labs

Transfer Rate: ● No limit ○ Maximum Mbps

DR IP Settings: ● Layer 2 Link ○ Layer 3 Link

DC zone (HCI)

Interface: eth2

Site IP Address: 192.

Netmask: 255.

Listening Port: 443

New Link

Connected Sites: DR zone (HCI) <-> Labs

Transfer Rate: ● No limit ○ Maximum Mbps

DR IP Settings: ○ Layer 2 Link ● Layer 3 Link

DR zone (HCI)

Interface: eth1

Site IP Address: 192.200.19.20

Netmask: 255.255.255.0

Listening Port: 443

☑ Enable route

Next-Hop IP: 192.200.19.1

□ NAT-applied scenario

Mapped Peer Address:

Labs

Interface: eth0

Site IP Address: 192.168.19.174

Netmask: 255.255.255.0

Listening Port: 443

☑ Enable route

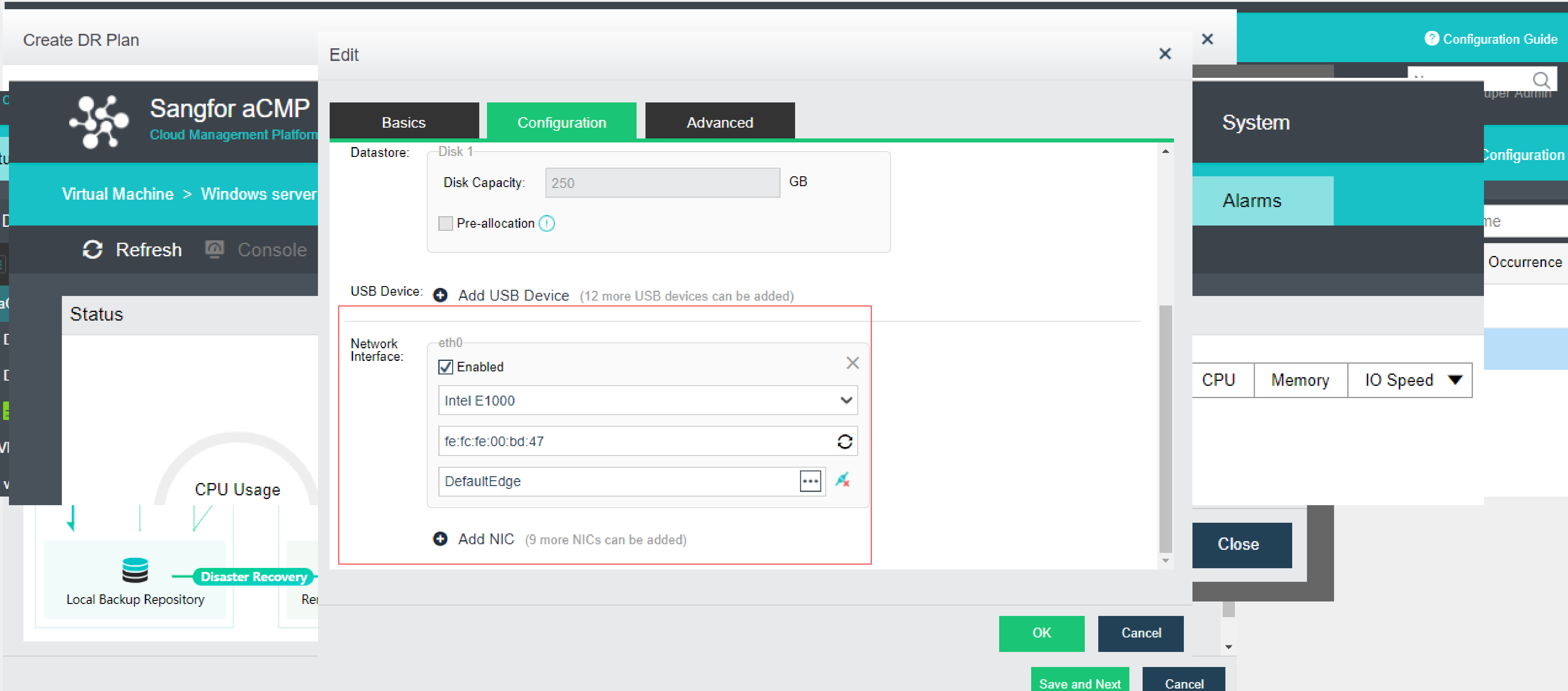
Next-Hop IP: 192.168.19.1

□ NAT-applied scenario

Mapped Peer Address:

Disaster recovery plan configuration

Click〖Reliability Center〗→〖Disaster Recovery〗; Select〖Disaster Recovery Plan〗, click **Create DR Plan** button



Edit

Basics | Configuration | Advanced

Datastore: Disk 1

Disk Capacity: 250 GB

□ Pre-allocation

USB Device: Add USB Device (12 more USB devices can be added)

Network Interface: eth0

☑ Enabled

Intel E1000

fe:fc:fe:00:bd:47

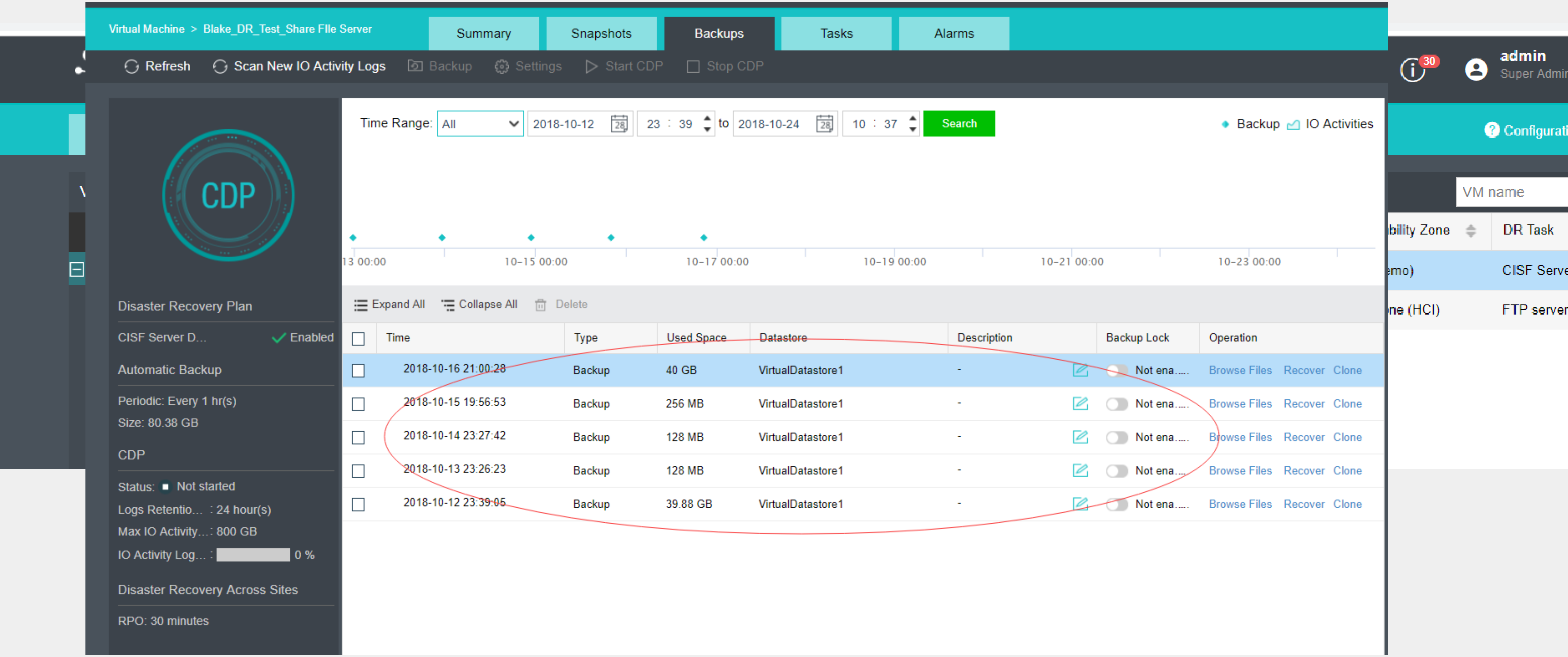
DefaultEdge

Add NIC (9 more NICs can be added)

OK | Cancel

Local recovery virtual machine

Click Edit Virtual Machine at the primary site to go to the virtual machine configuration interface and restore from the Backup configuration.



Disaster Recovery Plan

CISF Server D... ✓ Enabled

Automatic Backup

Periodic: Every 1 hr(s)

Size: 80.38 GB

CDP

Status: ■ Not started

Logs Retentio... : 24 hour(s)

Max IO Activity...: 800 GB

IO Activity Log... : 0 %

Disaster Recovery Across Sites

RPO: 30 minutes

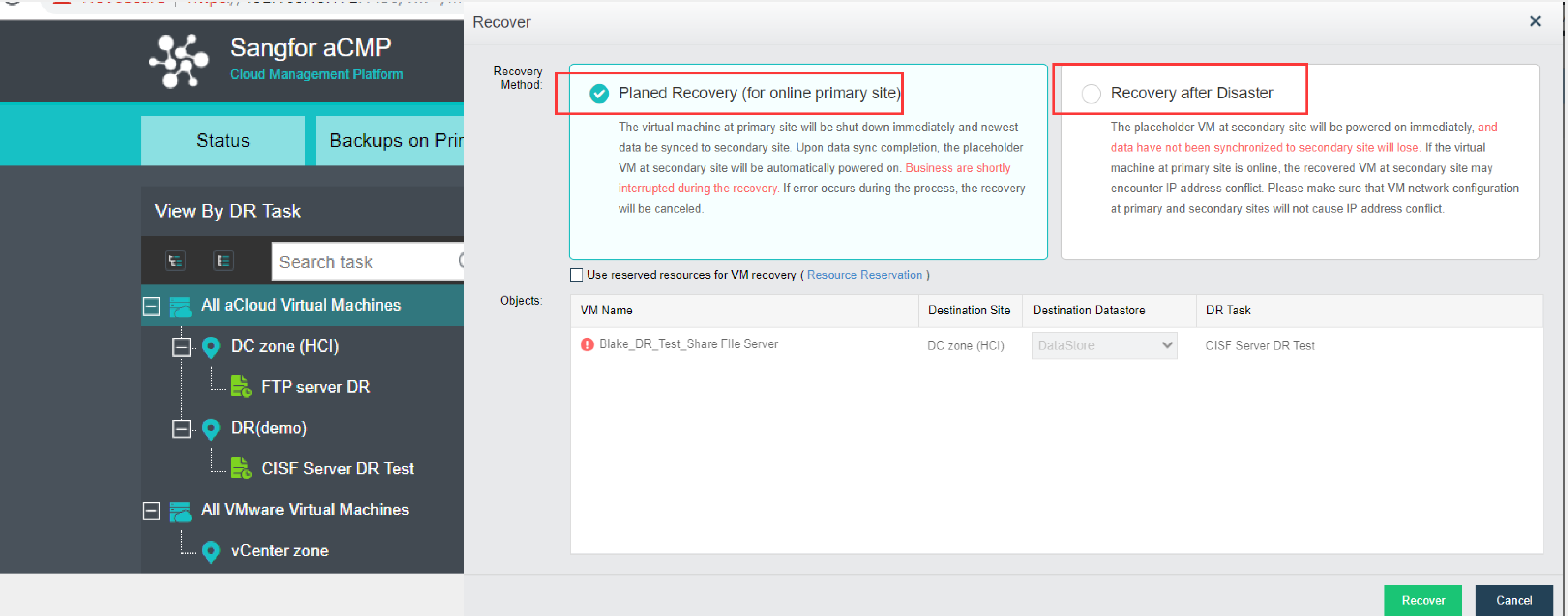
Time Range: All 2018-10-12 23 : 39 to 2018-10-24 10 : 37

□	Time	Type	Used Space	Datastore	Description	Backup Lock	Operation
□	2018-10-16 21:00:28	Backup	40 GB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
□	2018-10-15 19:56:53	Backup	256 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
□	2018-10-14 23:27:42	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
□	2018-10-13 23:26:23	Backup	128 MB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone
□	2018-10-12 23:39:05	Backup	39.88 GB	VirtualDatastore1	-	Not ena...	Browse Files Recover Clone

Service migration backup site after disaster

Log in to the aCMP DR configuration interface and click Recovery in the backup site to restore the configuration to the backup site.

Recovery type: Planned Recovery and Recovery after Disaster



Recover

Recovery Method:

● Planed Recovery (for online primary site)

The virtual machine at primary site will be shut down immediately and newest data be synced to secondary site. Upon data sync completion, the placeholder VM at secondary site will be automatically powered on. Business are shortly interrupted during the recovery. If error occurs during the process, the recovery will be canceled.

○ Recovery after Disaster

The placeholder VM at secondary site will be powered on immediately, and data have not been synchronized to secondary site will lose. If the virtual machine at primary site is online, the recovered VM at secondary site may encounter IP address conflict. Please make sure that VM network configuration at primary and secondary sites will not cause IP address conflict.

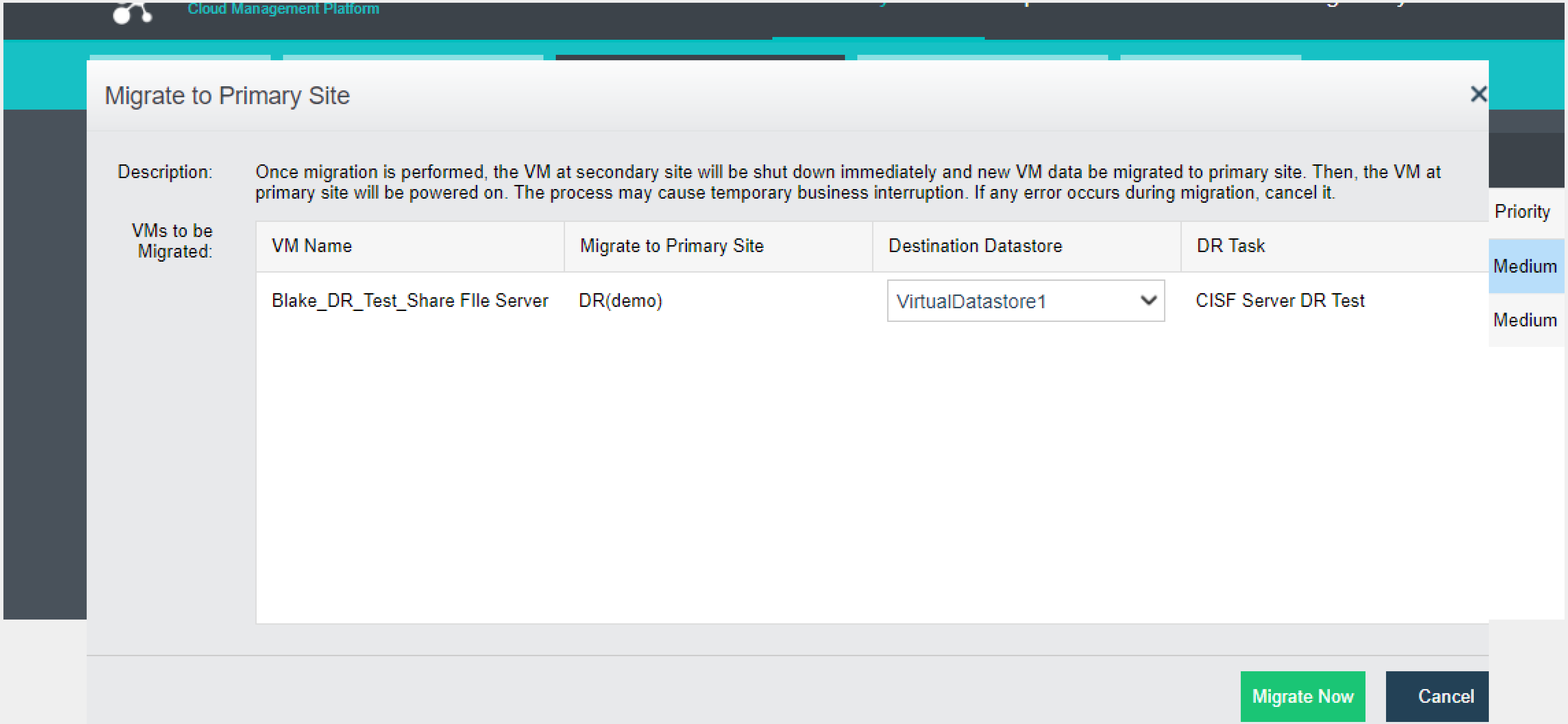
□ Use reserved resources for VM recovery (Resource Reservation)

Objects:

VM Name	Destination Site	Destination Datastore	DR Task
Blake_DR_Test_Share FIle Server	DC zone (HCI)	DataStore	CISF Server DR Test

Service host migrated back to the primary data center

After the primary data center is restored, you can log in to the aCMP and migrate the service host back to the primary data center.



Migrate to Primary Site

Description: Once migration is performed, the VM at secondary site will be shut down immediately and new VM data be migrated to primary site. Then, the VM at primary site will be powered on. The process may cause temporary business interruption. If any error occurs during migration, cancel it.

VMs to be Migrated:

VM Name	Migrate to Primary Site	Destination Datastore	DR Task
Blake_DR_Test_Share FIle Server	DR(demo)	VirtualDatastore1	CISF Server DR Test

4. Disaster tolerance POC

SANGFOR
深信服科技

POC Test Guide

- POC test detailed reference to the following document

SANGFOR_aCloud_v5.8.6_DR POC Test Guide

SANGFOR_aCloud
.6_DR POC Test G

Precautions

- The DR test should ensure that the bandwidth of the primary data center and the backup data center is at least 10Mb. The test environment is recommended to be tested on the 1000Mb link.
- recommended to test with the model configuration of aServer2000 or above
- Both aCMP and HCI must be version 586

SANGFOR
深信服科技

THANK YOU

Thanks for watching

www.sangfor.com