Replication and Disaster Recovery Using VMware Cloud Disaster Recovery (VCDR)

VMware DRaaS

Table of contents

Replication and Disaster Recovery Using VMware Cloud Disaster Recovery (VCDR)

Introduction

VMware Cloud Disaster Recovery (VCDR) protects your vSphere virtual machines by replicating them periodically to a VMware Cloud backup site and recovering them as needed to a VMware Cloud on AWS Recovery Software Defined Data Center ("SDDC").

VCDR supports two deployment modes- On-demand and Pilot Light:

- The on-demand deployment (also known as "just in time" deployment) of a cloud DR site provides an attractive alternative to continuously maintaining a warm standby cloud DR site. With on-demand deployment, the recurring costs of a cloud DR site are eliminated in their entirety until a failover occurs and cloud resources are provisioned.
- With a Pilot Light deployment, VMware Cloud Disaster Recovery enables a smaller subset of SDDC hosts to be deployed ahead-of-time for recovering critical applications with lower RTO requirements than an on-demand approach. The Pilot Light deployment mode assists organizations to reduce the total cost of cloud infrastructure by maintaining a scaled-down version of a fully functional environment always running in warm-standby while ensuring that core applications are readily available when a disaster occurs.

VCDR supports two different sites which can be configured as protected sites:

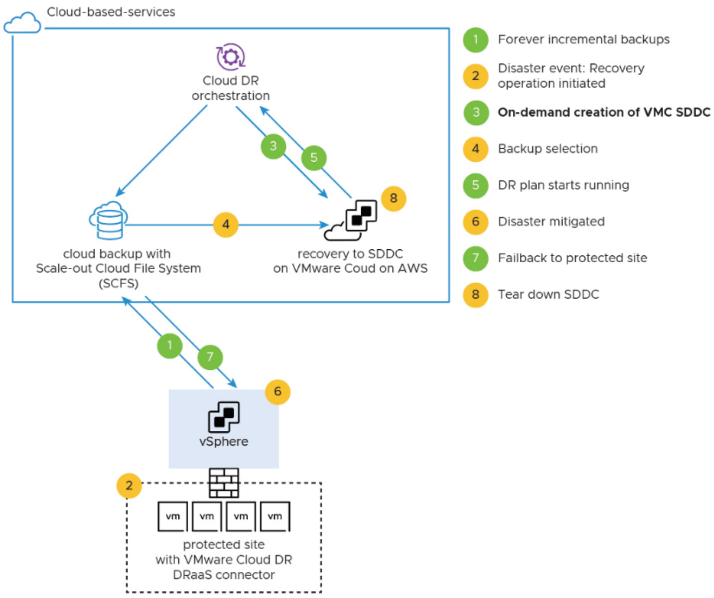
- On-prem vCenter
- VMware Cloud on AWS SDDC

The following figure demonstrates communication between VCDR components

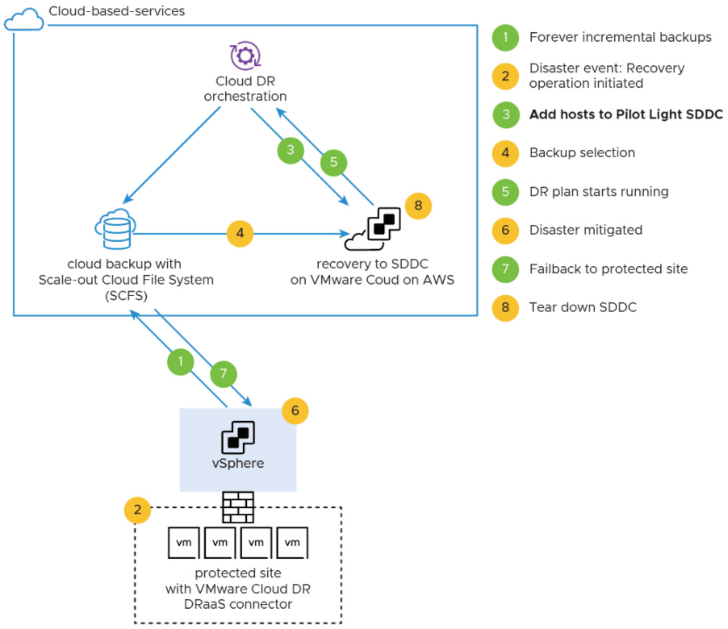
Use Cases	
Pre-requisites	
General Considerations/Recommendations	
Cost Implications	link
Performance Considerations	While the minimum RTO of 4 hours is configurable, also add recovery SDDC creation time when designing for On-demand use case.
Documentation Reference	VMware VCDR user guide

Enabling Replication Using VCDR

The following figure shows the replication and failback workflow in an on-demand SDDC Scenario.


Cloud-based-services
Cloud DR orchestration
cloud backup with Scale-out Cloud File System (SCFS)
recovery to SDDC on VMware Coud on AWS
vSphere
vm
vm
vm
vm
protected site with VMware Cloud DR DRaaS connector
1 Forever incremental backups
2 Disaster event: Recovery operation initiated
3 On-demand creation of VMC SDDC
4 Backup selection
5 DR plan starts running
6 Disaster mitigated
7 Failback to protected site
8 Tear down SDDC

The following figure shows the replication and failback workflow in a Pilot Light Scenario.


Cloud-based-services
Cloud DR orchestration
cloud backup with Scale-out Cloud File System (SCFS)
recovery to SDDC on VMware Coud on AWS
vSphere
vm
vm
vm
vm
protected site with VMware Cloud DR DRaaS connector
1 Forever incremental backups
2 Disaster event: Recovery operation initiated
3 Add hosts to Pilot Light SDDC
4 Backup selection
5 DR plan starts running
6 Disaster mitigated
7 Failback to protected site
8 Tear down SDDC

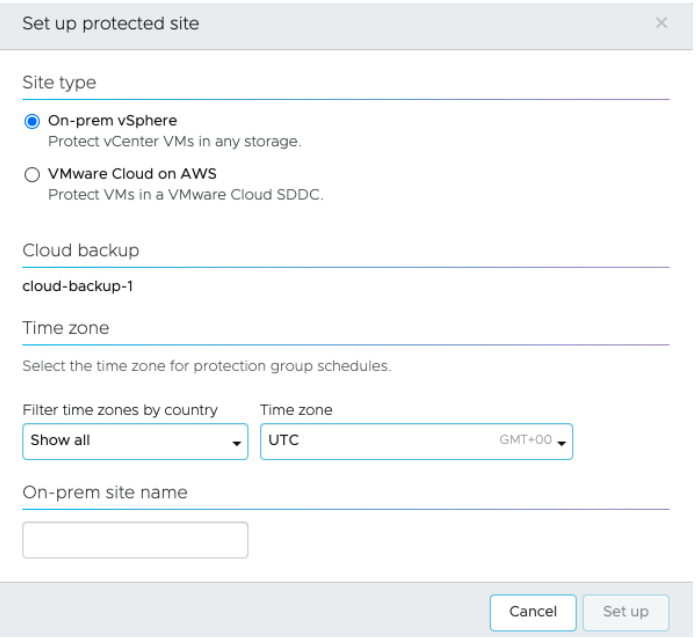
Setup a Protected Site

VCDR supports two types of protected sites for both On-Demand and Pilot Light SDDC deployment – on-prem vSphere and VMware Cloud on AWS SDDC.

On-Prem vSphere

Before configuring the on-prem environment, note the network requirements for the DRaaS connector and also configuring API token in the Intro to DR document. Procedure:

1. In the VMware Cloud Disaster Recovery UI, click Sites > Protected sites.
2. Click the Set up protected site button in the upper right corner.
3. In the Setup protected site dialog box, under Site types select On-prem vSphere.
4. Enter a name for the protected site.
5. Select a time zone from the drop-down menu, and then click the button on the right to set the time zone for the protected site.
6. Click Setup.



Set up protected site

Site type

● On-prem vSphere
Protect vCenter VMs in any storage.

○ VMware Cloud on AWS
Protect VMs in a VMware Cloud SDDC.

Cloud backup

cloud-backup-1

Time zone

Select the time zone for protection group schedules.

Filter time zones by country: Show all

Time zone: UTC GMT+00

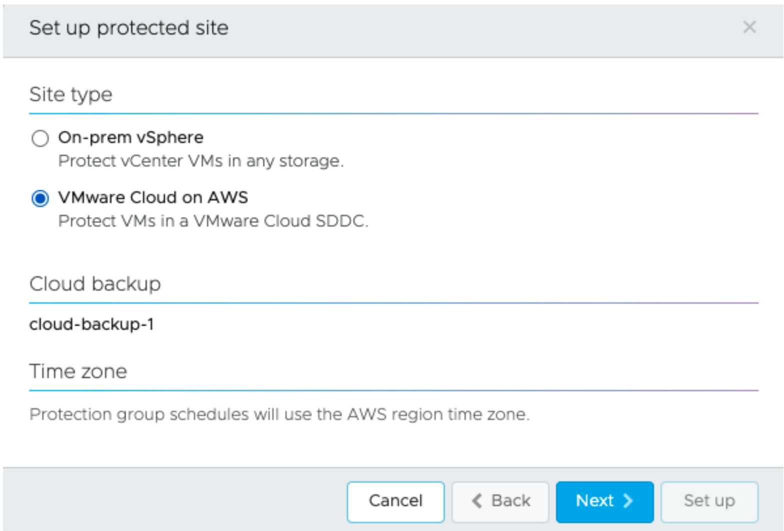
On-prem site name

VMware Cloud on AWS SDDC

Before you set up a protected site for an SDDC, you must deploy an SDDC and have a network segment already configured for it.

When the protected site is a VMware Cloud on AWS SDDC, the time zone schedule followed for snapshot/replication is dependent on the region of the source SDDC deployment. The time zone cannot be modified and you must adjust the schedule of replication accordingly. Note: the SDDC which is being protected should belong to the same account.

1. In the VMware Cloud Disaster Recovery UI, click Sites > Protected sites.
2. Click Set up protected site in the upper right corner.
3. In the Setup protected site dialog box, under Site types select VMware Cloud on AWS.
4. Under Cloud backup, if there is more than one Cloud backup site deployed in your environment, you can select the backup site. The backup site you select cannot be in the same AWS region where your Recovery SDDC is running.
5. Under Time Zone, you see that the time zone is set to the same time zone as your recovery SDDC. After the protected site is created, you can change this time zone for the site.



Set up protected site

Site type

○ On-prem vSphere
Protect vCenter VMs in any storage.

● VMware Cloud on AWS
Protect VMs in a VMware Cloud SDDC.

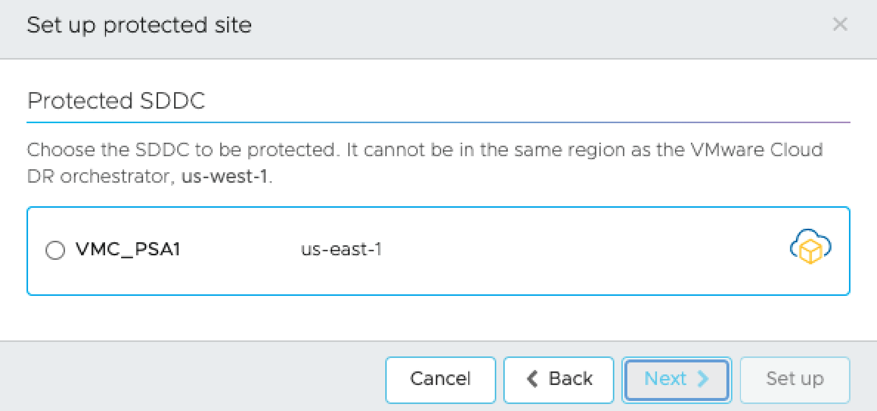
Cloud backup

cloud-backup-1

Time zone

Protection group schedules will use the AWS region time zone.

6. Click Next.
7. Select an SDDC to protect. This SDDC cannot be in the same AWS region where your Recovery SDDC is deployed.
8. Click Next.



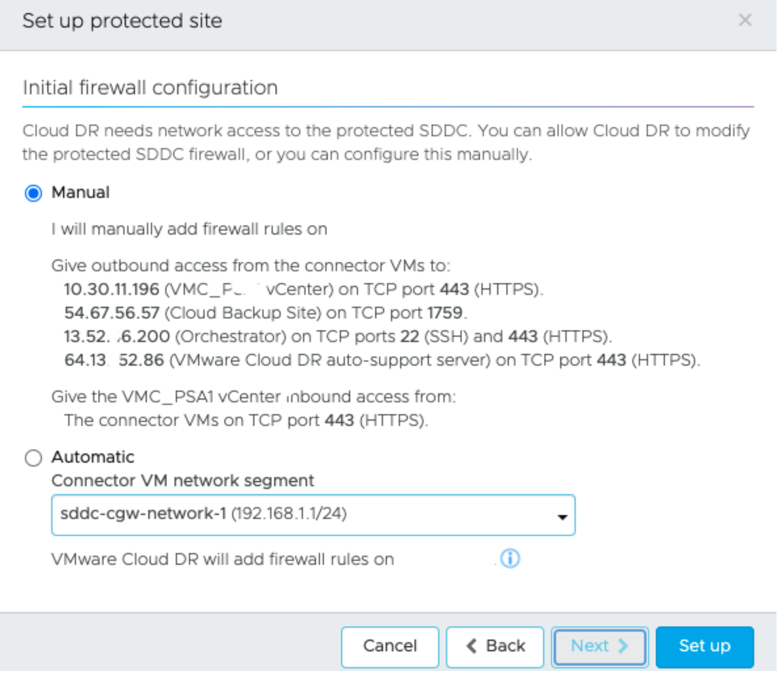
Set up protected site

Protected SDDC

Choose the SDDC to be protected. It cannot be in the same region as the VMware Cloud DR orchestrator, **us-west-1**.

○ VMC_PSA1 us-east-1

9. Create firewall rules. You have a choice when creating the firewall rules. You can allow the system to create firewall rules for the DRaaS Connector (recommended). Or you can manually create those firewall rules from the VMware Cloud Disaster Recovery UI. If you are not sure which to select, see Network Considerations for a Protected SDDC for more information.



Set up protected site

Initial firewall configuration

Cloud DR needs network access to the protected SDDC. You can allow Cloud DR to modify the protected SDDC firewall, or you can configure this manually.

● Manual

I will manually add firewall rules on

Give outbound access from the connector VMs to:
10.30.11.196 (VMC_P... vCenter) on TCP port **443** (HTTPS).
54.67.56.57 (Cloud Backup Site) on TCP port **1759**.
13.52. .6.200 (Orchestrator) on TCP ports **22** (SSH) and **443** (HTTPS).
64.13 52.86 (VMware Cloud DR auto-support server) on TCP port **443** (HTTPS).

Give the VMC_PSA1 vCenter ınbound access from:
The connector VMs on TCP port **443** (HTTPS).

○ Automatic
Connector VM network segment
sddc-cgw-network-1 (192.168.1.1/24)

VMware Cloud DR will add firewall rules on

10. Click Setup. When the site is set up, it is displayed as a protected site.