January 2025

Managing Your Recovery SDDC Deployment

Considerations for the VMware Cloud on AWS Recovery SDDC for VMware Live Cyber Recovery

vmware®
by Broadcom

Table of contents

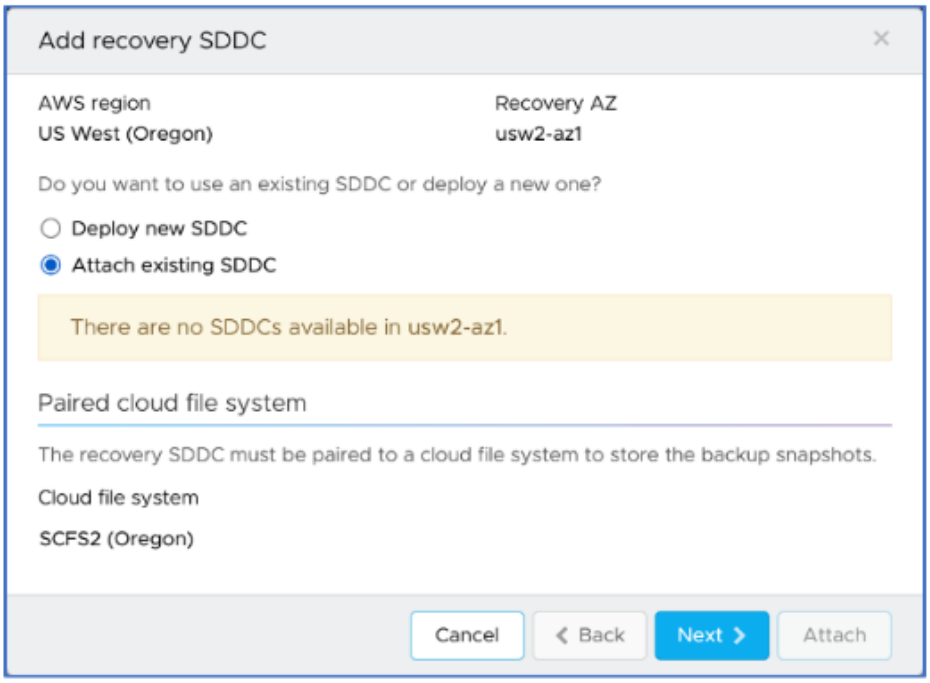
Introduction

VMware Live Recovery provides an easy to use and cost-efficient ransomware recovery solution for your production data center cyber recovery needs by leveraging the VMware Cloud on AWS infrastructure as your recovery site. With this recovery solution, it is possible to protect on-prem vCenter environments as well as other VMware Cloud on AWS SDDCs to a Recovery SDDC in another VMware Cloud on AWS supported Region / AZ. There are some things to understand and consider when setting up and managing the Recovery SDDC. This article will review several of the key topics. The implementation of this capability is provided through the VMware Live Cyber Recovery products in the VMware Live Recovery solution.

Deploying or Connecting the Recovery SDDC

The VMware Live Cyber Recovery Orchestrator UI provides one possible method to deploy a new Recovery SDDC or attach an existing SDDC. It is important to note that there is a 1-1 mapping of the Cloud File System (SCFS) used to hold the protected VM snapshot recovery point data and the associated Recovery SDDC. To understand the rules and limitations of AWS Region and AZ dependencies, please consult the product documentation details.

Working within the deployment location constraints, it is a simple task of creating a new Recovery SDDC or attaching an existing (previously constructed) SDDC instance. These options are shown in the screenshot below where we see that there is not an existing SDDC in the same Region/AZ as the SCFS:



Just in Time vs Persistent Deployments

For organizations just getting started with VMware Cloud on AWS, it is possible to manage the Recovery SDDC in a Just-in-Time approach and deploy the cloud-based Recovery SDDC site only when needed for testing purposes or to support an active ransomware recovery event. With the Just-in-Time approach, the Recovery SDDC is manually created by the Recovery SDDC administrator. Note that this step can take a couple of hours to complete from task initiation to final configuration and should be factored into the overall RTO planning for Just-in-Time scenarios. Once the testing has been completed, or the ransomware recovery incident resolved, and services returned to the original Protected site, decommissioning (deleting) of a Just-in-Time Recovery SDDC is also a manual task of the Recovery SDDC administrator. A Just-in-Time SDDC will need to be manually created, configured, and destroyed each time it is needed.

The alternative is to have a persistent Recovery SDDC deployed. In this case the Recovery SDDC is created once and configured for use and then stays online 24/7, it's always there. Note that in either a Just-in-Time or persistent mode the Recovery SDDC can be a minimal configuration of just 2 hosts or scaled up with cloud elasticity to the desired capacity to support recovery testing or actions. In addition to faster recovery times because the Recovery SDDC already exists and does not have to be deployed, configuring the Recovery SDDC for proper Recovery operations can also be set up and tested ahead of time with a persistent deployment configuration.

In either case, it is important to have the appropriate cloud host subscriptions in place to support the use of the Recovery SDDC.

One other thing to consider when setting up your Recovery SDDC, is that once VMware Live Cyber Recovery has connected to the Cloud File System (SCFS) and it is mounted to that Recovery SDDC for VM recovery operations, you will need to detach the Recovery SDDC if you plan to keep the SDDC for other purposes. Otherwise, the Cloud File System connection will go away once the Recovery SDDC is deleted.

Configuring the Recovery SDDC for Ransomware Recovery

The Recovery SDDC can be created directly from the Orchestrator UI following the rules for deploying the Recovery SDDC into the appropriate AZ and the appropriate region. Once the Recovery SDDC is deployed it will still need to be configured. Some of these configuration updates will have to be done directly in the VMware Cloud on AWS console or in the Recovery SDDC itself.

To access the Recovery SDDC, you will need to update the firewall rules to enable access to the administrator to log into the vCenter and any other peripheral networks that are not directly part of VMware Live Cyber Recovery.

Once the Recovery SDDC is deployed you'll need to configure access to that Recovery SDDC on the external networks that you want to use for your recovery site. Setting up those application access networks is outside the scope of this discussion.

Configuring the Recovery SDDC state for proper testing or ransomware recovery use requires a couple of post deployment steps to be completed. Other things that need to be configured in the recovery site for proper Recovery plan mapping include:

- considerations for resource groups if you are building out clusters or want to partition the recovery site in any way, those resource groups will need to be created and configured so that they can be included in the Recovery plan mappings
- folder structure and virtual networks of the Recovery SDDC that will be part of the mappings
- necessary vCenter tags that you are using in your Protected Site inventory Protection Groups will need to also be registered into the Recovery SDDC for proper compliance checks

Each of these configuration settings will need to be set up in the Recovery SDDC prior to the plans being compliant and fully ready to run for a successful ransomware recovery operation with VMware Live Cyber Recovery. These are tasks that you need to do inside the vCenter operations of the Recovery SDDC.

For the situation where the SDDC may get deployed and deleted on a regular basis, there is a VMware Fling that might be useful in this scenario here: SDDC Import/Export for VMware Cloud on AWS

With the Just-in-Time approach, anytime the Recovery SDDC is deleted those four things (resources, networks, folders, tags) also go away and will need to be reconfigured manually in the next Just-in-Time deployment. Avoiding these manual reconfiguration processes is one of the other advantages of working with a persistent Recovery SDDC.

In addition to having the Recovery plan mappings in place and being monitored by automated compliance checks run every 30 minutes by the Orchestrator, you can have additional services already up and running in that small persistent Recovery SDDC footprint. These other services might include stretched networks from the Protected site to the Recovery SDDC, VPN access points, even DNS / AD services that you might be using between your Protected site and your Recovery SDDC.

These additional services can be configured upfront and running and operational, while consuming limited resources. The persistent Recovery SDDC approach also lowers the recovery time (RTO) as the Recovery site is ready to go into service at any time.

Creating / Checking Recovery Plans

To construct a Recovery plan, the Recovery SDDC needs to be present so that the Orchestrator can include all the mappings that we just talked about. As you can see there are several things that a persistent Recovery SDDC can provide to the overall solution and make the ransomware recovery administration, setup and recovery processes easier to manage and more expedient.

Even with a Just-in-Time approach, you could:

- create the Recovery SDDC,
- configure it as desired,
- construct the Recovery plans,
- run through all the necessary testing,
- deactivate the Recovery plan,
- then decommission/delete the SDDC.

If a Recovery plan is completely configured and then deactivated and the Recovery SDDC deleted, then when the Recovery SDDC is redeployed Just-in-Time, the Recovery plan can be reactivated, and the compliance checks can be used to guide what changes need to be made to the Recovery SDDC to match the Recovery plans.

Scaling the SDDC Up or Down

In either case, for the Just-in-Time or the persistent Recovery SDDC, when testing or during an actual ransomware recovery event the Recovery SDDC can be scaled up with more hosts and clusters as needed to support the actual workloads that are being tested or remediated. The Recovery SDDC scaling can be semi-automated using elastic DRS capabilities or it can be manually configured by the Recovery SDDC administrator. In addition to the additional costs with larger Recovery SDDCs, there will be some provisioning time and cloud compute resource availability associated with periodically scaling a Recovery SDDC. In some cases, it is advised to have the Recovery SDDC sized to the minimum configuration to support the most critical ransomware recovery workload needs.

Another consideration when scaling up the Recovery SDDC for testing or for actual ransomware recovery actions, is to consider what you want the desired Recovery SDDC size to be after the testing is complete or the workload has been failed back to the protected site. A Recovery SDDC can be as small as 2-host cluster. Another consideration is to consider leaving the initial Recovery SDDC alone and adding additional SDDC clusters and hosts to that Recovery SDDC. The additional clusters can be scaled up with additional hosts and you can have multiple clusters in a single Recovery SDDC configuration. The scale back task, which again is a manual operation by the Recovery SDDC administrator, can remove the additional clusters leaving just the original Recovery SDDC.

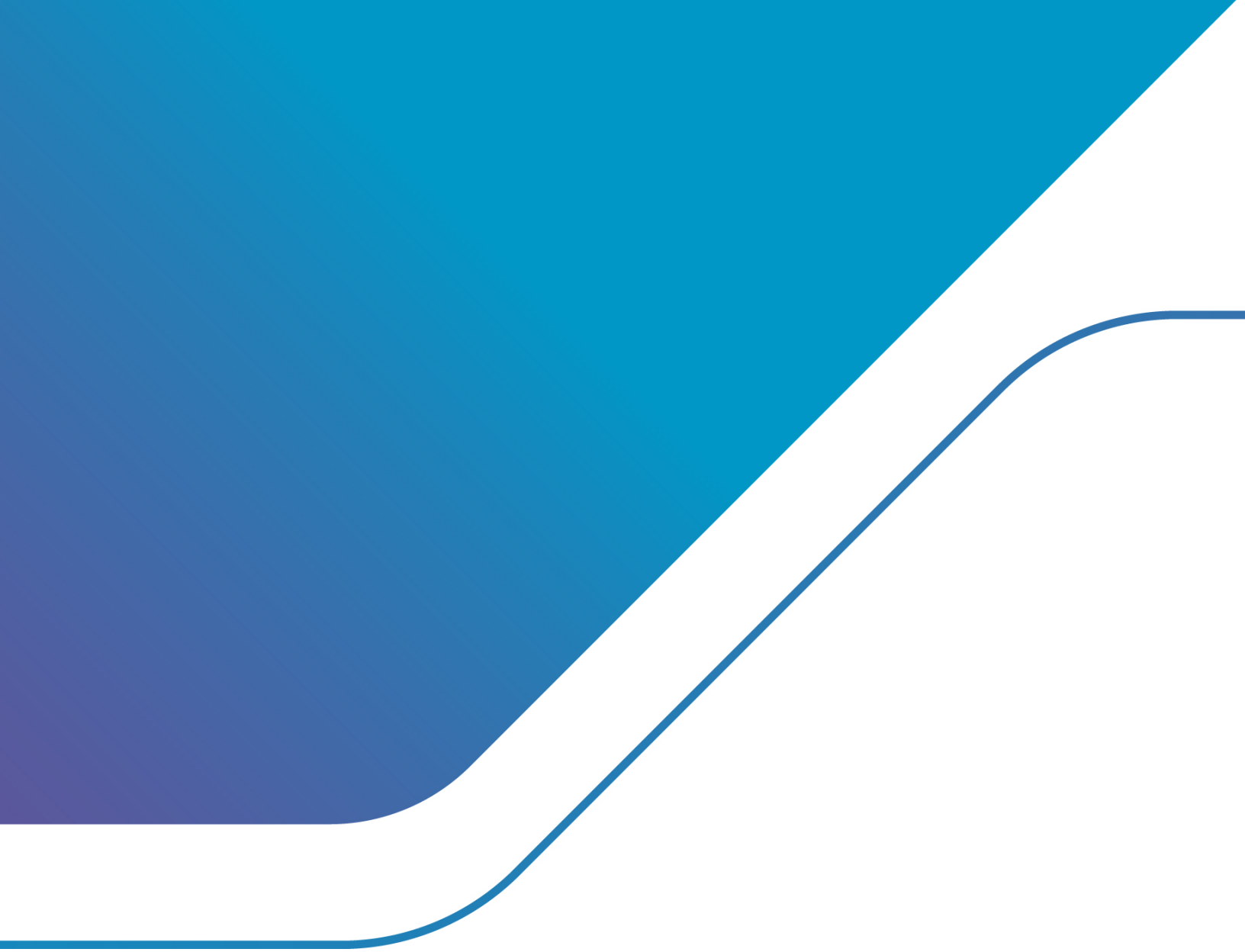
Removing the SDDC

Removing the Recovery SDDC is a manual task even for Just-in-Time deployment instances. When you remove the Recovery SDDC, you will also be removing the connection to the Cloud File System (SCFS). Note that active Recovery plans that have this Recovery SDDC in their configuration will begin to have compliance check alerts as the Recovery site no longer exists. It is suggested to deactivate such plans before removing the Recovery SDDC to avoid these warnings until a Recovery SDDC is deployed again.

Summary

With VMware Live Cyber Recovery, you can create your Recovery SDDC Just-in-Time if desired or use an always-on persistent approach. In either case, the Recovery SDDC is easily provisioned and configured. You can deploy the Recovery SDDC from the Orchestrator UI or through the VMware Cloud on AWS Services console or bring your own SDDC from an appropriate, existing VMware Cloud on AWS configuration. Once connected to the Cloud File System, that Recovery SDDC can service your testing or running of the ransomware recovery plans.

Whether you follow a Just-in-Time or persistent approach, the scalability up and down of the Recovery SDDC, although it's a manual process, is also very simple and straightforward with VMware Live Cyber Recovery. This ransomware recovery solution provides a very effective way of leveraging VMware Cloud on an AWS for ransomware recovery with and easier to manage and cost-effective architecture.



vmware®
by Broadcom