TECHNICAL ARTICLE
November 2024

Disaster Recovery vs Ransomware Recovery

Use Case Comparison

vmware®
by Broadcom

Table of contents

Introduction

Data Center Disaster Recovery has been a challenge for IT operations since the first business dependencies existed on the data center for continued business operations. However, that DR landscape has been changing over the past decades and now presents some very new and challenging problems for IT operations to work into their current practices

Traditionally, a DR solution addressed getting the business back into service as quickly as possible after a data center level disaster. These disasters were usually physical problems with the production environment that could not be mitigated with better infrastructure at the production site – for example: loss of power, loss of site (natural disasters), or unplanned catastrophic human error or negligence.

Although complex, the framework and procedures for recovering from these data center disasters were straightforward and well understood. We will get into those in a bit more detail in this article.

A new type of disaster has emerged that threatens IT operations – ransomware! IT organizations still have the same operational objective at hand – get back into service as quickly as possible. However, the path and processes for this type of recovery from infection are much different.

Let's look at several key areas of recovery solutions and examine the differences between data center recovery and ransomware recovery when it comes to planning and processes for either of these scenarios. The key areas to consider are:

- Recovery Site
- Backups
- Networking
- Recovery Workflow
- Operations Team Actions

Recovery Site

For either type of disaster, you will need a recovery site to help with getting operations restored. The recovery site need is often temporary and dedicating permanent physical resources can be a costly and complex measure. In this case, emerging, cloud-based, as a service, recovery sites make a lot of sense.

- With a data center disaster, there is usually something "failed" at the original production site preventing normal operations and the DR site is used to run the business applications while the original site is repaired or replaced.
- With a ransomware attack, your production site is usually still intact and can be used to run applications, but the applications have been compromised and unable to run. In this case, your DR site is used as an IRE (Isolated Recovery Environment), to provide a place to safely repair (or

clean) the application VMs so they can resume safe operations back in their original location. We will go into a little more detail on this through this discussion.

Backups

Protecting business application data with backups makes logical sense in either case. This has been going on for a very long time. We won't get into the specifics of the backup methods, but the location of the data is important as it can be costly and time consuming to move the data to the recovery site when needed. The backup data should reside in the recovery site region. Also, the restoration of the data – think recovery points or point in time copies – should also be expedient as you do not want to wait for lengthy data restore cycles even if the backups are at the recovery location. There is another key distinction when contrasting these two types of disasters – which recovery point in time is best?

- For data center disasters, there is typically a single recovery point of interest – the latest, greatest usable backup copy. In this case, RPO SLAs are important and the shorter or more recent the better. For example, 30 minutes ago might be just fine. Bringing these recent copies online quickly in the DR site and getting the applications up and running is the primary objective.
- For ransomware situations, your data has been infected by malware at some point and you are potentially dealing with a prolonged and unknown dwell time on the application systems involved. The latest copy of protected data may also be compromised. You will want a deeper inventory of backups to choose from as your team will likely be iterating over the copies looking for the ideal base copy to begin the recovery. Having other recovery points of the same application system to draw files and folders from to help minimize overall data loss during the necessary remediation tasks is a great feature.

Networking

Connecting application systems to each other and to their users – internal or external – is critical to any recovery operation. We won't go into specific networking practices here but instead let's examine the networking management needs.

- For data center disasters, the networks at the production and DR sites are typically similar and easily mapped in the plans and ready to run and access the applications as soon as they are recovered. The networks may already be connected as the two sites – production and DR – may still need to communicate during recovery.
- For ransomware situations, the recovery networking is more fluid, yet controlled, keeping applications isolated and turning network access on or off to prevent reinfection while at the same time ensuring some undesirable behavioral actions – such as unwanted lateral movement – can be discovered and remediated. Being able to move in/out of specific network configurations with ease during the recovery tasks is crucial.

Recovery Workflows

The orderly following of a well-defined and tested set of task steps is critical to getting business services back into operation while dealing with the unexpected "disaster".

- Data center disaster workflows tend to be fairly linear, grouped, and programmatic, following a well-defined run book based on the scope of the disaster at hand and the systems affected.
- Ransomware recovery workflows tend to be more iterative and singular in nature as the recovery team begins to hunt for the intruder malware, spread of the problem, and determine the best recovery point(s) – as well as apply changes – more of that later. This iteration needs to be able to be conducted in a controlled environment and as quickly as possible from the available backups.

Operations Team Actions

In any of these disaster recovery situations, the operations team needs to be focused on getting the business services back up and running.

- For data center disasters, this falls primarily onto the shoulders of the infrastructure and applications team. Infrastructure – is the application available at the DR site? Applications – is it running as expected after restarting? Both need to agree on the "good to go" outcome.
- With ransomware situations, the operations team must expand to include the cybersecurity team as well as the broader networking (security) team. The infrastructure team is bringing candidate application recovery points online – in the IRE – and applying the appropriate malware tools and network controls to make sure the selected version is "healthy and clean". At the same time, they must work with the networking team to make sure it is not getting compromised or compromising other systems. Once these tasks are done, then the applications team can get involved to determine the operational state of the application.

Comparison of Recovery Types

Recovery Type	Disaster	Ransomware
Recovery Site Use	Production Failover	Isolated Recovery Environment (IRE)
Recovery Points Used (backups)	One – singular event – very recent RPO from best known state	Multiple – combining data sets, minimize data loss – deeper retention
Networking Setup	Production Access	Isolation Control
DR Plan Workflow	Linear – step-by-step runbooks – bring apps online	Iterative – evaluation of good state – divide and conquer
Special Actions	Application / environment startup – good to go	NGAV – static + live malware (behavioral) analysis

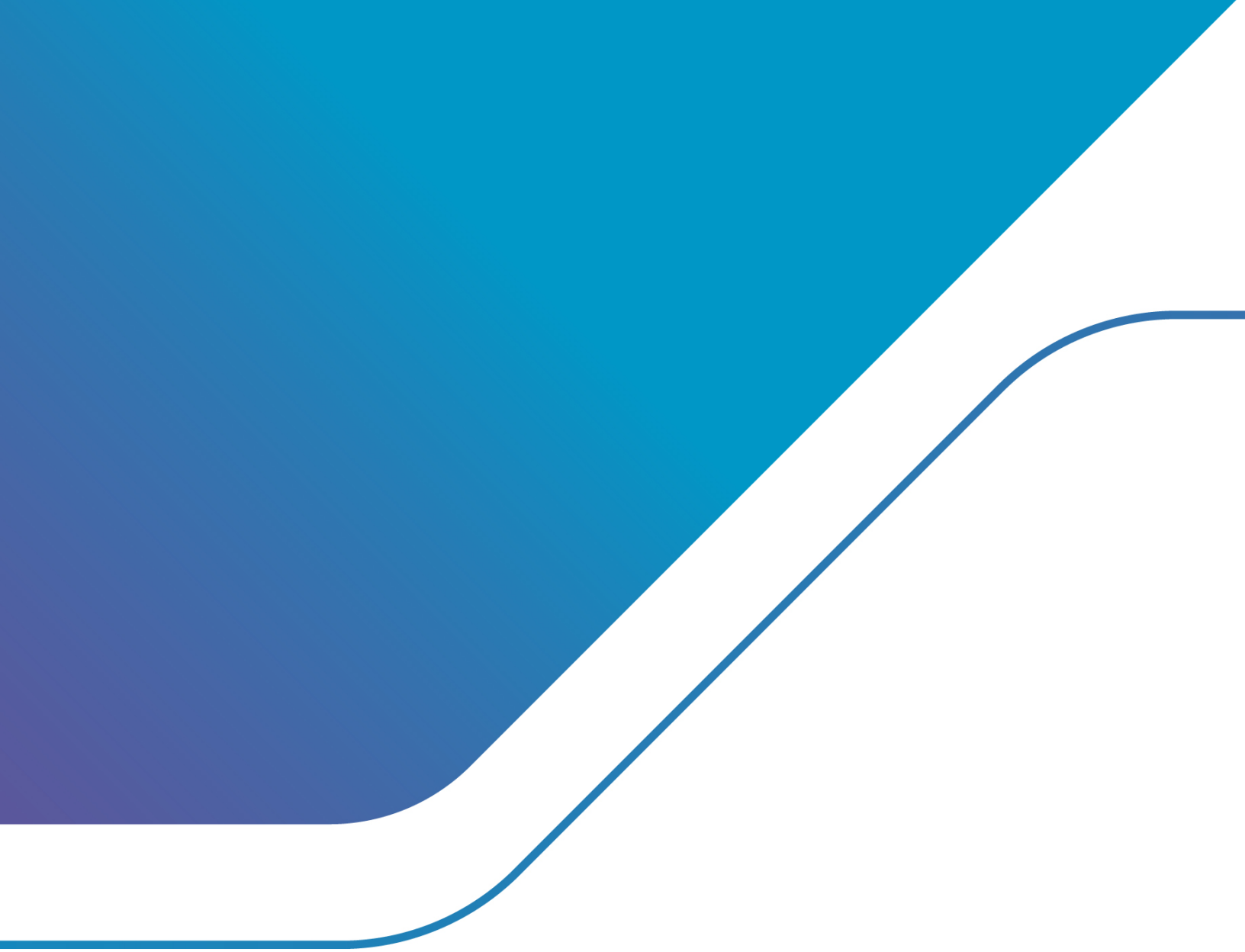
Summary

In this blog, we have covered just a couple of the key differences between data center disaster recovery and ransomware recovery. As you can see, there are some very distinct differences in the approach needed. Your DR solution(s) should be evaluated as to how they are equipped to handle basic data center disaster recovery as well as ransomware recovery. If possible, a common platform that could handle both would help simplify the outcomes and increase the likelihood of success in either case.

The table below summarizes much of the discussion presented above and available in the product documentation. It is followed by links to some additional resources on this topic.

Resources

- VMware Live Recovery
- Resource Center
- Product Documentation
- Blogs



vmware® by Broadcom

Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24