

CLOUD RECOVERY SUCCESS: A TECHNICAL DRaaS GUIDE

How does DRaaS work?

Drill into the process for testing your cloud recovery capabilities with EVault Senior Manager Jamie Evans as a guide.



Testing full recoveries of IT environments requires a proven methodology. Establishing and meeting RTOs, configuring a cloud recovery system, and tracking your changing environment are all critical components of a successful cloud recovery operation. In this expert Technical Guide, learn how Jamie Evans, Senior Manager of Disaster Recovery as a Service (DRaaS) for EVault, helps clients complete a full recovery of their systems.



Jamie Evans

Senior Manager of Disaster Recovery as a Service (DRaaS)

EVault[®]
from Carbonite

THIS IS THE CHALLENGE AND OPPORTUNITY THAT I FACE EVERY DAY IN MY ROLE: TO DELIVER SUCCESSFUL CLOUD RECOVERY FOR MY CLIENTS NO MATTER WHAT

No one ever wants a recovery to go south—whether it's your first or 50th time completing a data recovery operation. But your organization will experience a bit more anxiety when it goes to perform its first recovery using a new solution. If the phrase “successful recovery”, in your experience, has applied to only a few applications or a limited set of files, it's understandable that you may be anxious the first time you test a recovery of your entire environment. Know this: you can successfully conduct a full recovery of your environment the first time as well as every time thereafter.

This is the challenge and opportunity that I face every day in my role: to deliver successful cloud recovery for my clients no matter what. While we never guarantee that a recovery will occur without some hiccups during the process, I can point to the fact that every cloud recovery that I have overseen has met our agreed upon service levels

whether that guarantee is for a 1-hour recovery, a 24-hour recovery, a 48-hour recovery, or some combination of all three.

EVault Cloud Disaster Recovery Options

Recovery Time Objective	Implementation
1 Hour	Live Site-to-Site Replication
24 Hour	Recover from Cloud Backup
48 Hour	Recover from Cloud Backup

Our best practices are ones we have developed internally over the years—and we follow them strictly to ensure we can recover any of our clients' environments based upon our contractual obligations. Furthermore, these steps are applicable and transferable to any environment to enable a successful recovery in the cloud.



CLOUD DISASTER RECOVERY BEST PRACTICES



After a client inks a cloud recovery deal with us, we engage our internal fulfillment team to verify that we can recover their environment. To do so, we configure our environment to match their environment by following our internal cloud disaster recovery (CDR) best practices guide. These best practices help us define your existing environment, see the jobs it's handling, and the order in which these jobs need to be recovered.

Configure Your Environment



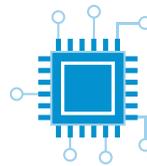
Companies that have already done the prep work of documenting their environment can greatly accelerate our information-gathering process and shorten the time it takes our fulfillment team to certify that our environment is ready to recover your environment. Once our environment is properly configured, my team performs the actual cloud recovery.

Compare Environments



At this stage, we have a design call with the client. Our objective is to mimic the client's site in our cloud as closely as possible. We do this so that when the customer accesses its account during an actual disaster, a declaration of disaster, or in any time of need, its experience feels the same as if it accessed its own environment.

Collect Vital Information



During the design call we go beyond the hardware requirements previously gathered by our fulfillment team. We work to collect specific information about the servers we are recovering, the operating systems, their patch levels, the subnets in use, and the network architecture they are on.

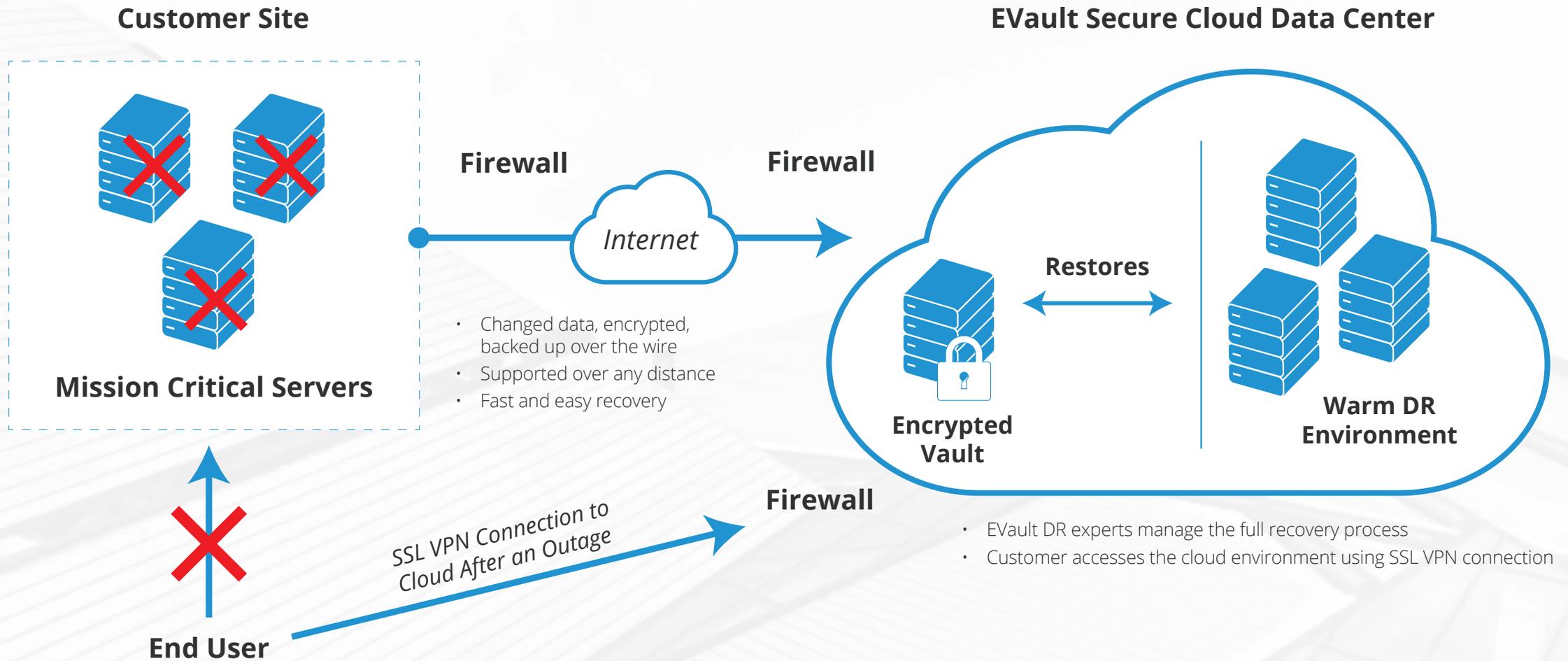
Create and Connect VLAN



Now we have a design document. We send that to our network operations team and they create a VLAN for us. We connect to that VLAN from inside our VMware vCenter implementation made accessible through our private cloud. This configuration gives both us and our clients the ability to remotely log in and connect via either an SSL VPN link or an IPSec tunnel once we have recovered their servers.



HOW IT WORKS



SHOULD YOU EVER NEED TO CALL ON US TO PERFORM AN ACTUAL RECOVERY, YOU CAN HAVE CONFIDENCE THAT IT WORKS



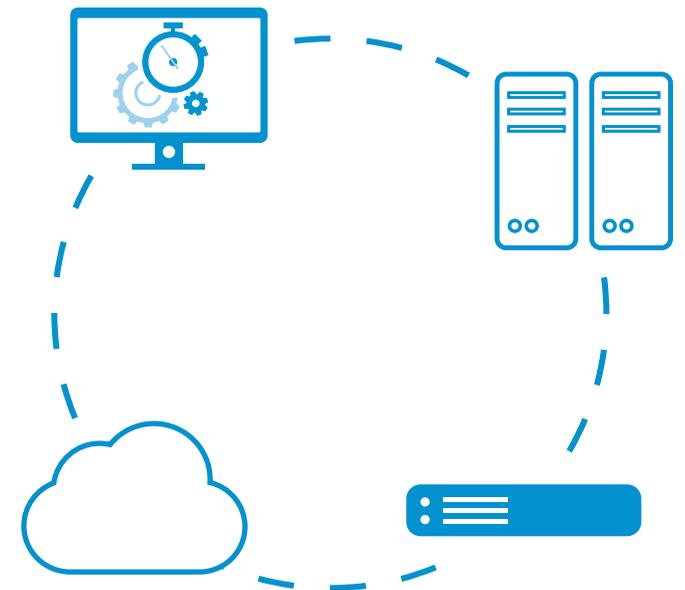
A TESTED, TIMED RECOVERY

Once your environment is documented and we have mimicked your environment at our site, we do a tested, timed recovery. This test positions us to say that we know we can meet your RTOs because we have completed and demonstrated a successful recovery at our site. That way, should you ever need to call on us to perform an actual recovery, you can have confidence that it works.

The test serves other purposes as well. It gives us the ability to appropriately size our environment to match our client's actual recovery requirements. For example, many of our clients allocate extra memory, processing, and/or storage on their production systems so they can easily and affordably tap into those resources as they grow over time or so these systems can dynamically handle peak loads.

During a recovery, our clients do not necessarily need access to that excess capacity and performance. In that case, we allocate only the resources they need to recover (with a margin of overhead). This reduces the resources and costs associated with staging a recovery.

Once the environment is built at our site, we present it to our client for testing. This is a tightly managed process. We schedule timed tests with our clients. If they have 1-hour, 24-hour, and/or 48-hour recovery time objectives, that is the amount of time to test. Those are the RTOs we need to meet to prove to them the recovery works.



A TESTED, TIMED RECOVERY *(cont.)*

TO DATE, WE HAVE RESPONDED TO MORE THAN 50 DECLARATIONS AND WE HAVE MET THE SLAs ASSOCIATED WITH EACH OF THEM

Adhering to this schedule, we have never missed a recovery service level agreement (SLA) when an actual disaster is declared. To date, we have responded to more than 50 declarations and we have met the SLAs associated with each of them.

We have had customers who did not subscribe to our cloud disaster recovery (CDR) service but because they used our

cloud backup service, they asked us to spin them up in our cloud. Even in those cases, we recovered their applications and brought them up at our site without having had the ability to test it beforehand. While I would never recommend that approach, that gives you some indication about how well our backup and recovery process works and the capabilities of our team who handles these recoveries.



DOCUMENTATION CHEAT SHEET

Once the test is done and the client signs off that the recovery works as planned, we tear it down. However, we also document the results of our testing and hand that off to our clients. In many cases, our clients find this documentation as beneficial as proving that the recovery worked.

These technical details, as well as any other insights we gather during the recovery, are included in the final document. We do not provide our clients with our internal disaster recovery plan—EVault treats that as a professional service engagement—but our clients do receive the documentation they need to develop a framework so they can conduct a recovery on their own.

The other benefit of having this documentation with the test results is that it may satisfy either internal or external compliance requirements. This documentation often goes to their board of directors and potentially may even be shared with their customers. These test results make their customers feel safe and secure knowing that the company is recoverable and test results prove it.

The documentation we provide includes:

- The site where the recovery took place
- The number of servers recovered
- The name of each server recovered
- The IP address of each server recovered
- The fully qualified domain name
- The subnet mask
- The length of time it took to recover each server
- The length of time it took to recover the entire environment
- Issues that delayed the anticipated recovery time
- Any servers that had to be rebooted and/or repaired
- Any requirements to recreate the master boot record



IN FACT, 20 PERCENT OR MORE OF YOUR ENVIRONMENT MAY CHANGE OVER THE COURSE OF A YEAR

YOUR ENVIRONMENT—IT IS A CHANGIN’

Once you have successfully completed a recovery, you cannot rest on your laurels. A lot of people do not think about change in their environment but every environment experiences change. If you know anything about technology, or if you have been a system or network administrator, you know change is going to occur. There are patch level changes, changes that result from hardware failures, driver changes, and more.

In fact, 20 percent or more of your environment may change over the course of a year. The percentage of change between tested recoveries requires that you take one of two steps to ensure successful recoveries going forward.

A. Document changes as they occur and update your disaster recovery plan accordingly.

B. Start over.

The difficulty of maintaining a successful disaster recovery plan largely depends on the number of changes in your environment and how effective your internal change control processes are. If you have a nominal amount of change and tight control over your environment, you can feel confident about successful recoveries—if you document every change and continually update your disaster

recovery plan. Conversely, if you are unable to tightly monitor and control your environment, it may be easier and faster to start over each time you do a disaster recovery.

We believe tracking the changes in your environment as they occur is the more prudent option. It’s true you may miss some changes that occur, but these gaps can usually be identified and fixed during your annual, or semi-annual, DR test.



Jamie Evans

Senior Manager of Disaster Recovery as a Service (DRaaS)

EVault[®]
from Carbonite

Jamie Evans has worked in IT since 1998, starting on the Sony laptop/desktop assembly line in Rancho Bernardo, CA. He has experience ranging from system and network administration to data center operations and consulting. For the last seven years, Jamie has been focused on the disaster recovery space. He helped build the EVault Cloud Disaster Recovery business when it started with less than 20 customers. Today his team protects more than 5,000 servers.