# ServerCentral Business Continuity & Disaster Recovery Services

# SERVERCENTRAL BUSINESS CONTINUITY & DISASTER RECOVERY SERVICES

SERVICE & PROCESS INTRODUCTION

At ServerCentral, Business Continuity and Disaster Recovery (BC/DR) refers to a continuum that begins with backups and ends with turnkey disaster recovery services. The reason we view it in this way is that all applications (and all businesses) have very different needs. Successful business continuity isn't one answer to one question. It's multiple answers to multiple questions, all aligned specifically in support of your unique business requirements.

Is this the only way to view business continuity? No. We don't expect it to be. However, we do have a tremendous amount of experience working with companies like yours on a daily basis to develop the best possible solutions that meet unique needs, and we recognize that the solutions to these requirements consistently fall along one or more steps of this continuum.

## BUSINESS CONTINUITY & DISASTER RECOVERY SERVICES

ServerCentral's Business Continuity & Disaster Recovery Services are comprised of five solution sets that can be applied to applications individually or collectively to meet your specific requirements.

### BACKUP

Backup is a simple way to copy and later retrieve applications, files, and data from a location outside of your production environments.

### ARCHIVE

Archival is simply the cold storage of backups and other data that don't need to be recovered to maintain production. Archival is typically used for data with long-term security, legal, or compliance retention requirements.

### REPLICATION

Replication is the frequent (or near real-time) copying of applications and data from one location to another so that all systems share the same level of information.

### DISASTER RECOVERY (DR)

Disaster Recovery is, at its core, an area of IT security planning. DR focuses on protecting an organization from negative impacts associated with an unplanned event, such as a natural disasters, equipment failures, etc. The objective of DR is a formal DR Plan (DRP) that can be followed in an emergency to restore applications and services. This plan is a collection of policies, procedures, and actions that are clearly understood throughout an organization, tested regularly, and quickly executed in the event of a disaster – whether it's a natural or human-induced disaster. This last part, human-induced disaster, is an important point to note.

### DISASTER RECOVERY AS A SERVICE (DRAAS)

Disaster Recovery as a Service takes DR one step further by offloading failover testing and execution of event mitigation onto ServerCentral. In a DRaaS environment, the replication of your virtual or physical infrastructure takes place in our data centers. The DRP policies, procedures, and actions are clearly defined by your team and ours. Our team conducts regular testing of failovers scenarios and, in the event of an actual emergency, we perform your failover as well. The entire DRaaS service is wrapped in a predefined Service Level Agreement (SLA) specifically written to achieve your operating objectives.

# SERVERCENTRAL'S BC/DR PHASES

We begin all Business Continuity/Disaster Recovery (BC/DR) relationships with a very clearly defined process. The first step in this process is Discovery.

## DISCOVERY

- Identify the current status of your DR strategy
- Set RTOs/RPOs for each application
- Set recovery prioritizations for each application (the order in which each application will be brought back online)
- Identify your compute, memory, storage, and network footprints for each application
- Define the minimum viable infrastructure for recovery for each application (in many cases, you won't need 100% coverage for a non-critical application in a disaster state)
- Map exactly how end users connect to these applications
- Verify security and compliance requirements should a disaster event occur
- Define what specifically needs to happen in order for an event to be declared and a failover action to be executed

Within your infrastructure an important distinction to make is which applications have which RTOs/RPOs. How critical are these applications, really?

We uncover this information during discovery at this granular level because applications and processes are likely to have significantly different requirements than one another. Some applications will need to be up and running instantaneously should an event occur. Other applications may not be required for days (or even weeks).

Once each application in question has been assigned RTO/RPO values within the discovery process, we can really begin to identify the key requirements for meeting your business continuity objectives.

Why do we put so much emphasis on this part of the process? It's simple, really. Some applications are very easy to prepare for and manage in the case of a disaster. Anything virtualized/clustered/software with support for failure scenarios—applications like email, for example—are easy to prepare for. These types of applications require far less resources and planning to provide continued service.

However, other applications are far more difficult to prepare for and manage. Old, end-of-life software and legacy apps not coded for redundancy are prime examples. Physical servers with older OSs which may have certain BIOS requirements, RAM requirements, specific drivers for older hard drive interfaces (ATA or SCSI) may not be easily or readily available.

The point of discussing this in detail isn't to create fear, uncertainty, and doubt. We simply want to be 100% clear about all of the steps in order to deliver you a business continuity solution that meets your needs.

## PLANNING

After Discovery is complete, we begin Planning. Planning is a ServerCentral-focused step in the process. During this step, our solution architects, network engineers, virtualization experts, storage experts, data center operations managers, provisioning team, and professional services managers work together to develop a solution that meets the requirements identified during Discovery.

When the Planning is complete and we have what we believe to be a sound solution to your requirements, we meet with you and your stakeholders to present the proposed solution and discuss project timelines.

## VALIDATION

The Validation step in the process is where the most give-and-take occurs. This is where the scope and answers to questions identified in Discovery will change. This is by far the most fluid part of the process—but it's also the most important. At this point you will see, firsthand, how we've taken your requirements, applied our experience and technology, and arrived at what we believe is the best possible answer for you.

Sometimes our answer is met with a resounding, "Yes! That's it!" Other times, our answer is met with, "This is really awesome, but it's too expensive."

Both answers are fine. The point of validation is to get the solution just right so that everyone is happy, comfortable, and all needs are accounted for.

## DEVELOPMENT

After Validation, we begin Development of the solution's infrastructure. This includes event mitigation processes, network elements, security/compliance requirements, compute/memory/storage resources, and so on. While in Development there will be a lot of back and forth, the interactions are typically more tactical than strategic.

## TESTING & DEPLOYMENT

From Development, we move on to Testing & Deployment. This phase is pretty self-explanatory. Testing encompasses verifying the infrastructure will perform as architected. Deployment encompasses a true test-run via failover testing to be sure the infrastructure is set and all applications perform as intended in a failover state.

## MANAGEMENT

The final step of the process is Management. At this point the solution is deployed and we're providing ongoing management and administration of all core business continuity elements, including network, security, compute, storage, failover testing, and event mitigation.

## FAILOVER TESTING

During standard Failover Testing, ServerCentral performs a manual failover of the infrastructure into a sandbox environment. The standard test procedures allow us to validate:

- VM/VPG failover
- VM/VPG point-in-time failover
- Compete protected site disaster
- VPG failback & move
- IP address reconfiguration
- Testing will be performed
- Interoperability of VMotion
- Interoperability of protected VM storage VMotion
- Recover a shutdown VM
- Alarm system validation

## NON-VIRTUALIZED ENVIRONMENTS

There are a number of options for us to pursue in setting up BC/DR for non-virtualized environments. These solutions are dependent upon some very specific configuration information, including network, compute, memory, and storage usage (similar to virtualized environments, as well as the acceptable timeframe between data snapshots. The replication solutions available for non-virtualized environments are based upon snapshot technologies (either independent apps or in-SAN replication capabilities, so we're talking about completely different RTO and RPO windows when we're talking about non-virtualized environments.

In order to provide a detailed solution for a non-virtualized environment, we'll need to have a conversation that addresses a handful of unique discovery questions so that a disaster event for your application(s is mitigated within your desired timeframe.

The main difference between the DR and DRaaS solutions is that in an virtualized environment, we can work within the I/O stream and do near real-time replication. This foundation permits delivery of the DRaaS solution. In a non-virtualized environment, we're working with snapshot-based solutions that elongate RTO/RPO windows and have a much heavier infrastructure requirement due to the size of the snapshot data on top of production data. Again, this is something that can absolutely be done, it's just part of a larger, more detailed conversation.

## RUNBOOKS

Each ServerCentral customer receives their own unique runbook that details the specific configurations and steps associated with their BC/DR environment. This runbook is a living, breathing document followed by all ServerCentral operations teams.

This is the law, if you will, relative to how we will support and deliver your BC/DR services.

Periodic reviews of the runbook are also scheduled to be sure that the changing elements of your business and infrastructure continue to be met.

## EVENT DECLARATIONS

First and foremost, a disaster event declaration is exactly why we have custom runbooks, as everything that takes place will be in accordance with your specific runbook.

How is an event is declared? An event declaration can take place either automatically or manually. An automatic declarationis triggered by a system alert. This alert can be anything you want and is defined as a critical occurrence that requires your application(s) to fail over. These alerts are defined during Discovery, set up during Development, and noted in your runbook.

A manual declaration is a manual request for failover when conditions exist that you feel meet the need to utilize DR infrastructure. A manual declaration is triggered by a phone call or trouble ticket.

Once the event declaration has occurred, it is time to execute the failover. The failover begins with a spin-up of your DR compute resources. These resources may already be on or they may need to be turned on with the declaration. This is a decision point for you and your organization in terms of the recovery time required for each application and the cost associated with those resources.

This information is also defined in your runbook.

Again, not all applications have to be defined in the same way. The availability of these compute resources can (and should vary on an application-by-application basis.

Once the compute resources are spun-up and verified to be operational, your IP space will be reassigned to the DR infrastructure. This is a critical step because it keeps all of your end users in line with the application.

At this point, your applications are online and your end-users are operational. Should it have been identified and defined in the Discovery and Validation phases, we may be involved in helping you understand the root cause of the event. We may not. This is where your specific needs and requirements are going to play a major part in determining exactly what roles ServerCentral takes. We can be as involved or uninvolved as you like.

The final step in the disaster recovery process is a Return to Production. This is, without a doubt, the most complex part of the entire process. In order to meet your requirements, unique processes will be defined within your runbook. This may include using the "former" production environment for DR now that it has failed over, or it may include an application-by-application reverse migration to the old production equipment. There isn't one answer here, so we will work with you to discuss the benefits, challenges, and risks associated with each potential decision on an application-by-application basis. This is the final element of your runbook.

## CONCLUSION

Every organization has different expectations of, and requirements for, their BC/DR environments. What makes ServerCentral truly unique is that we work with you (yes, real people are there every step of the way 24x7x365) to design, develop, deploy, and manage your BC/DR services. A ServerCentral solution means you can focus on one thing and one thing only: your business.