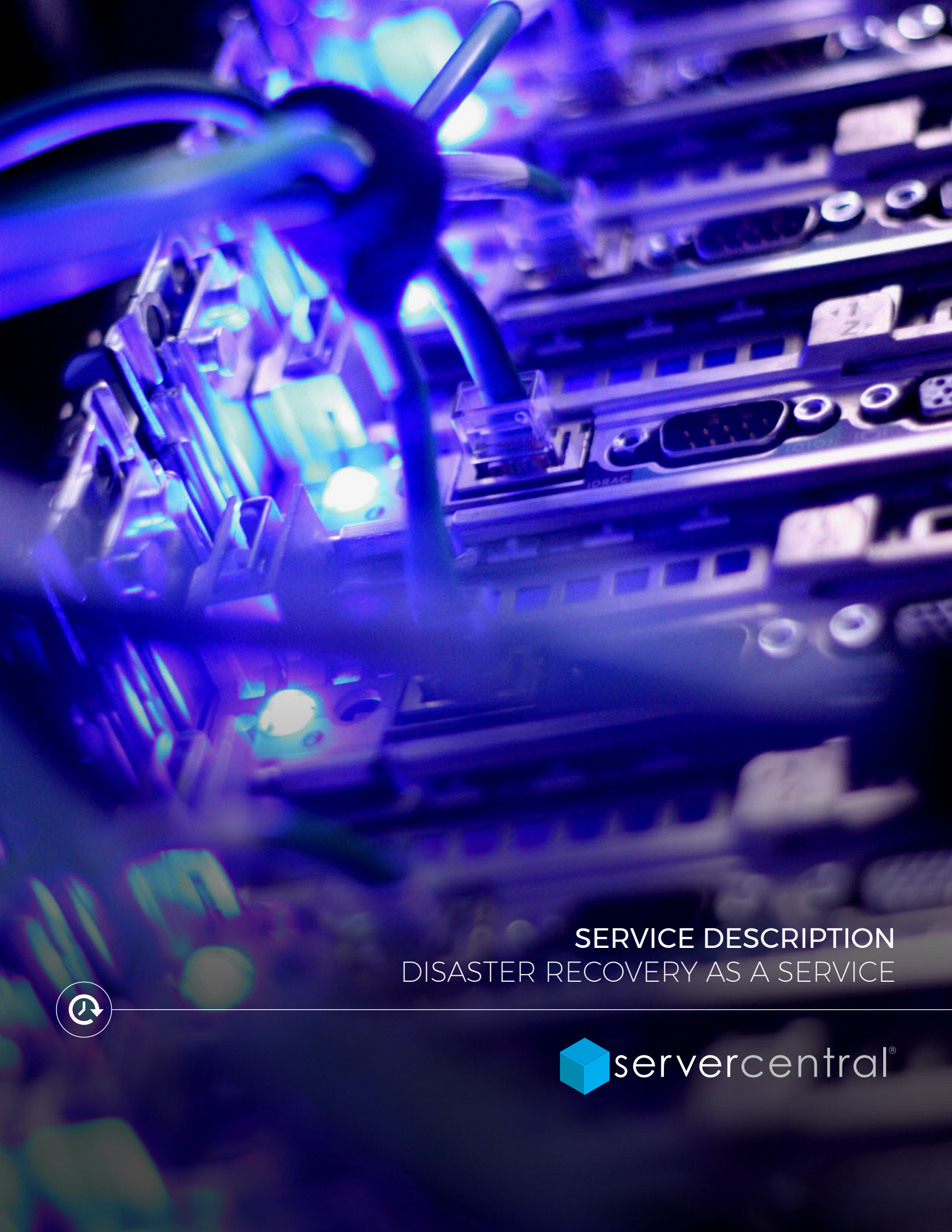


SERVICE DESCRIPTION
DISASTER RECOVERY AS A SERVICE

servercentral®

Contents

Service Overview

ServerCentral's Disaster Recovery as a Service (DRaaS) is a combination of automated protection of virtual machines, a managed service to coordinate the ongoing real-time replication of data between two sites, managed failover testing on a regular basis, and managed failover & failback in the event of a declared disaster. ServerCentral's DRaaS provides the ability to failover a virtualized environment to a ServerCentral data center in response to a declared disaster. Upon declaration of a Disaster Event, ServerCentral and the Customer will perform the pre-defined set of activities set forth in a mutually agreed-upon Runbook. DRaaS includes regular testing of failover and failback, with the option to run additional tests.

The Customer will define a Source site and a Target site for recovery. The Source site can be at a Customer-operated premise, a colocation environment in one of ServerCentral's secure, resilient data centers, or in a ServerCentral Enterprise Cloud or Private Cloud Service. The Target site will be in a ServerCentral Enterprise Cloud or Private Cloud Service.

ServerCentral begins by working with the Customer to assess their needs, examining the virtual environment, the physical infrastructure, and the network connectivity options. ServerCentral will verify the Customer's desired Recovery Point Objective (RPO) and Recovery Time Objective (RTO). Assessment includes an inventory of the applications used in the environment, with an eye toward understanding application dependencies, data flow, and level of importance. This information is used to map applications into priority groups and tiers to ensure that applications failover in the correct order and priority. The Source location and Target destination for replication will be defined. All of this information is documented in a Runbook, maintained by ServerCentral and accessible for the Customer.

ServerCentral will then implement the hardware and software necessary to support the Customer's DRaaS requirements. Secure network connectivity will be provisioned and maintained for the term of the service. During normal operations, ServerCentral will monitor the replication processes and confirm the expected replication Service Level Agreements (SLAs) are met. ServerCentral will also keep the configurations of ServerCentral-operated physical assets used with the Service in sync, including firewalls, switches, routers, clusters, hypervisors, SANs, and network transit.

An initial failover and failback test will be performed for all VMs and applications protected by the Service. A separate, annual, full test of failover and failback procedures is also included with the Service. Customers can elect to have ServerCentral run additional testing through the term of the Service, with options for a sandbox or full tests. A sandbox test includes booting up replicated VMs in the Target site with Customer verification of data integrity and application functionality, but does not include full network testing or failback of VMs. A full test includes all failover and failback procedures documented in the Runbook.

In the event of disaster, failover and failback of applications will follow a collaboratively planned method and an organized plan for recovery. ServerCentral and the Customer will pre-define the disaster criteria and business rules that would lead to a disaster event. The Customer will define the person(s) who can declare a disaster and request failover. The Customer will also designate a different person(s) who will verify the declaration and approve the request. These steps reduce the likelihood of an error state in one part of the Customer's infrastructure leading to an unintentional disaster being declared.

After verification, ServerCentral begins executing the plan documented in the Runbook, activating the VMs based on groups and tiers. ServerCentral will verify the operational state of the VMs in the Target location, including successful guest OS boot and IP addresses. After this, the Customer will verify the operational state of applications and related software tools operated by the Customer.

The Customer will have the option to continue to run the VMs at the Target site as long as needed (additional fees may apply). Once the timeframe for failback to the Source site is determined, ServerCentral will follow the plan for failback documented in the Runbook. Again, ServerCentral will verify the operational state of the VMs in the Source location and the Customer will verify the operational state of applications and related software tools operated by the Customer.

Customers can also get information, request changes, view the Runbook, and review service ticket history about the DRaaS service in general through ServerCentral's Customer Portal.

Key Features

- Based on proven, best-in-class hardware and software
- Highly-available, resilient, and secure design
- Automated protection of virtual machines in near real-time
- Managed failover and failback of VMs
- Collaborative planning and assessment of Customer needs
- Based on Customer-defined RPO, RTO, and business needs
- Includes synchronization of physical devices used with the Service
- Service documented in ServerCentral-maintained Runbook
- Initial + Annual full failover & failback test, with option for additional tests
- Complete infrastructure configuration & administration by ServerCentral
- 24x7 continuous monitoring, alerting, and support of the infrastructure
- Secure Customer Portal for documentation & service requests

Implementation

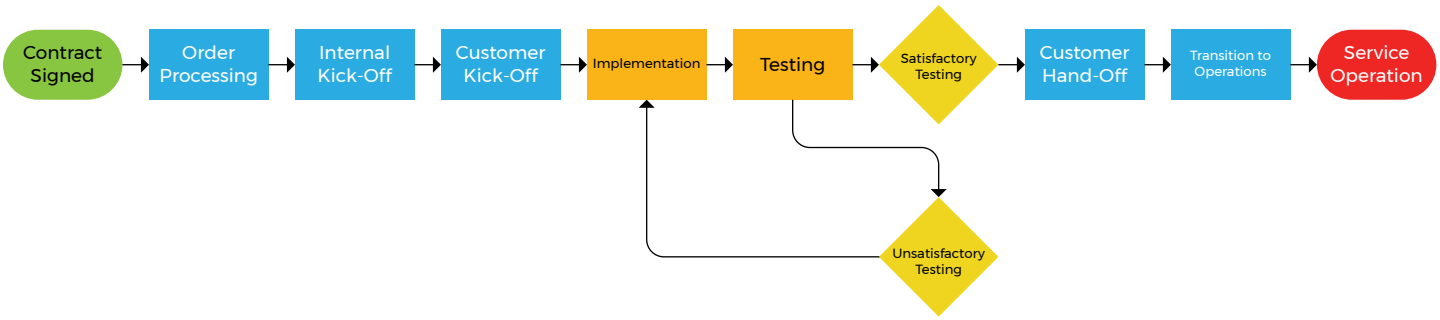
Validation

The Validation process begins with a comprehensive review of the information collected by Sales or Professional Services during the Discovery phase. The ServerCentral Provisioning and Managed Services teams will coordinate with you to gather all details necessary to configure any hardware and software required for the DRaaS service. This includes establishing required secure network connectivity and bandwidth between the Source site and the Target site, establishing a list of Disaster Recovery Administrators, and installing any replication software or hypervisor drivers. Other client-specific requirements, such as traffic forwarding policies, procedures, or third-party requirements, will also be reviewed. This information is documented and stored in the Technical Design Workbook. The Technical Design Workbook is used to create a Customer Workbook that is shared with the Customer after Implementation.

The Technical Design Workbook provides all necessary information to ServerCentral engineers to ensure that information-gathering is complete and the Service will be able to address the Customer's needs. This may include network diagrams, configuration details and requirements, special security considerations, and more. The Technical Design Workbook will serve as a basis for configuration detail and will be utilized in the long-term planning and execution of the Service.

Implementation Process

All provisioning activities at ServerCentral follow our Implementation Process summarized in the Graphic below:



Internal Kick-Off

After the customer's order for the Service is processed, ServerCentral holds an Internal Kick-Off meeting to assign the ServerCentral resources necessary to provision the service. Sales attends this meeting to provide information from the pre-sales process. A Project Manager or Project Lead will be assigned to coordinate and own the remainder of the Implementation Process from this point forward and act as the main point of contact with the Customer.

Customer Kick-Off

The Customer Kick-Off Call includes an overview of the provisioning process, a review of the information collected to date, and validation of the Customer's desired outcomes for the Service. The projected time line of the deployment will be established and the customer will be informed of any information they must provide for ServerCentral to complete the build. Generally, the Project Manager will also create a schedule for regular updates during the implementation process. The Customer should be prepared to designate at least one technical Contact for ServerCentral to work with during the process.

Provisioning & Testing

Implementation includes the activities necessary to provision the service. ServerCentral engineers will configure, deploy, and test the various hardware and software tools used to deliver the service. ServerCentral records all of the configurations used to implement the Service in a Customer Workbook, which is provided to the Customer after Implementation.

ServerCentral technical teams will perform testing on the ServerCentral-operated infrastructure that supports the Service. This usually includes, but is not limited to validating software configuration, system redundancy verification, verifying network connectivity, monitoring and alerting configurations, including verification of data replication, and activation of the Service in the Customer Portal. Any deficiencies found will be corrected and re-tested until the system functionality is verified. Requests for customer-specific test criteria will be reviewed by ServerCentral and evaluated on a case-by-case basis.

Billing

After a successful Test phase, Implementation will be considered complete and the Service Delivery phase begins. In general, billing for the service begins immediately after Customer data is being replicated.

Service Delivery

Customer Hand-Off

The Project Manager or Provisioning staff will schedule a Customer Hand-Off Meeting with a member of the Managed Services team, either in person or via conference bridge. The Meeting is designed to advise the Customer of the state of the service, the current configuration, and answer any general questions about the Service.

Training is also provided on the ServerCentral Customer Portal, including providing any access credentials to the Customer, walking the Customer through support engagement procedures, and general interaction with the Portal.

The Project Manager will also share the final/completed Customer Workbook, which takes the data from the Technical Design Workbook and Implementation process and acts as a the "as-built" documentation of the Service.

Replication Configuration

ServerCentral Managed Services staff will coordinate with the Customer to create the initial replication schedule, create the protection groups, and configure the VMs for replication. At this time, the data retention settings will also be configured.

Once the replication has been configured, the initial synchronization from the Source site to the Target site will begin. After this initial sync has been completed, any new or changed data will continue to be replicated in the background from the Source site to the Target site.

Runbook Creation

As part of the initial implementation, ServerCentral Managed Services will coordinate with the Customer to build a runbook that will contain all of the technical steps to be executed by both the customer and ServerCentral Managed Services staff when a disaster is declared. This assumes that the Customer has performed all of the necessary business continuity/disaster recovery analysis, identified all critical business processes (and what systems map to these processes), and identified the power-on or restoration order for virtual machines. The Customer will also need to establish the Disaster Recovery Administrator (the person(s) who can declare a disaster event) and the Verification Contact (the person(s) who can verify the declaration and approve a failover).

If more in-depth assistance is needed with building the runbook, professional services from ServerCentral are available. Please contact *sales@servercentral.com* for additional information.

Initial Failover & Failback Test

After the initial Disaster Recovery runbook has been created, ServerCentral staff will work with your staff to perform an initial, one-time, full test of the disaster recovery plan. ServerCentral will work with the Customer to identify a mutually agreed-upon time for the test. Also, the Customer will be required to have staff available to participate in the test to perform the data and application verification, as well as coordinate work on Customer-operated infrastructure that may need to be performed during the test.

Ongoing Testing

ServerCentral staff are available to work with the Customer's staff to conduct periodic testing of the Disaster Recovery Plan. The Service includes one (1) full failover & failback test per year. Regularly scheduled tests may also be added as part of your service. To schedule these tests, please open a support case. For information about the fees for additional tests, please contact *sales@servercentral.com* for more information.

Many times, the Service will be integrated with additional Services provided by ServerCentral. Some examples include Enterprise Cloud, Private Transport, and Managed Backup. All services and products necessary to complete the deployment will be completed either in tandem or in a phased approach during this post-implementation configuration period.

Additional Modifications

Over time, the Runbook may need modifications to it to reflect the Customer's changing needs and environment. ServerCentral Managed Services staff will need to be contacted if any modifications are needed for the runbook or runbook procedures. Customers should open a support case with ServerCentral to request these changes.

Using the baseline information in the Technical Design Workbook, the ServerCentral Engineering team will configure the baseline parameters for initial operation. The variables include:

- Change protection groups
- Increase/decrease number of VMs
- Runbook changes (priority changes, application changes)
- Altering priority for VMs

Customers do not have access to the hardware and software infrastructure used to deliver DRaaS, which is administered by ServerCentral. Should any changes to the Service be necessary, Customers can open a support case with ServerCentral to request the work. Requests for non-standard changes will be reviewed by ServerCentral and evaluated on a case-by-case basis.

For any of the other Managed Services used along with the DRaaS service, please refer to the appropriate Service Description for further information regarding those services.

Service Operations

General Operations

The DRaaS service, including all associated hardware and software, is monitored by ServerCentral's Network Operations Center. Should any issues or anomalies be detected with the Services, a member of the ServerCentral NOC or Managed Services team will take corrective action as planned and notify the customer.

From time to time, ServerCentral will perform scheduled maintenance activities on the infrastructure supporting the service. Customers will be notified in advance for all scheduled maintenance. Emergency maintenance may be required and performed without advance notice. Should a service-impacting emergency maintenance be required, ServerCentral will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

Service Features

ACCOUNT MANAGEMENT SERVICES	
Dedicated Client Relationship Manager	Included
IMPLEMENTATION SERVICES	
Build or provision the DR resources (Enterprise Cloud or Private Cloud)	Included
Feature Validation for hardware firmware & virtualization software	Included
Data Center Provisioning (Generator-backed Redundant Power, Cooling, Cables, Rack)	Included
Resilient Facility (24x7 Physical Security, Video Surveillance, Fire Suppression, Monitored Access)	Included
Network Provisioning (IP addressing, VLAN Configuration, VPN Tunnels)	Included
Custom Runbook coordinated with Customer	Included
24 X 7 MONITORING SERVICES	
Connectivity between Source and Target locations	Included
Replication services based on agreed-upon timeframes	Included
Hardware Health Monitors (compute, networking, storage)	Included
Hardware Availability Monitors	Included
Hardware Performance Monitors (latency, CPU)	Included
Cluster Capacity	Included
Complex Custom Monitor Development	SOW Based
INFRASTRUCTURE ADMINISTRATION (PROACTIVE SERVICES)	
Hypervisor Administration (ServerCentral-operated equipment)	Included
Firmware Patching & Updates (ServerCentral-operated equipment)	Included
Configuration changes per customer requests	Included
Device configuration backup & monitor for changes	Included
Change Management leveraging the ServerCentral change control process	Included
Change Management coordination with Customer for service-impacting events	Included
24 X 7 SUPPORT (RETURN TO SERVICE & VENDOR ESCALATION)	
Onsite sparing of identical hardware in US locations	Included
Hardware Troubleshooting (ServerCentral-operated equipment)	Included
Hardware Replacement (ServerCentral-operated equipment)	Included
Hardware Maintenance (ServerCentral-operated equipment)	Included
Replication tools & software	Included
Access to 24x7 Network Operations Center (telephone, web, and email)	Included
Access to Customer Portal w/ Customer-defined roles	Included
Ticket Response time - Promised	15 minutes

Responsibilities

The following section outlines the scope and limitation of support that ServerCentral offers for this Service.

SERVERCENTRAL RESPONSIBILITIES
ServerCentral will manage and maintain the ServerCentral-operated hardware that provides the infrastructure for the Disaster Recovery Service. In the event of hardware failure, ServerCentral personnel will proactively replace any failed hardware and restore the Service to normal operations.
ServerCentral will manage and maintain all ServerCentral-operated server or hypervisor software necessary for replication of data to occur between the Source site and the Target site.
ServerCentral will monitor the data replication between the Source and Target sites and take corrective action, if necessary, to ensure RTO/RPO requirements can be met during a disaster.
ServerCentral will work with the Customer to create the initial disaster recovery Runbook. ServerCentral will maintain a copy of the agreed-upon Runbook procedures on the ServerCentral Customer Portal.
During the term of the Service, ServerCentral must be notified of any modifications or changes required by the Customer. ServerCentral will document the changes and update the Runbook for the Customer.
ServerCentral will execute any procedures documented in the Runbook during a declared disaster or fail back event.
ServerCentral will implement and maintain the configurations needed to ensure data is replicating from the Source site to the Target site. This includes implementing any modifications to existing replication jobs, adding or removing hosts from replication, and other activities necessary to maintain the Service.
ServerCentral will coordinate with the Customer for the annual full failover & failback test based on the testing schedule documented in the Runbook.
ServerCentral will monitor the Disaster Recovery Service for uptime and availability. This includes any network connections, general Internet connectivity, storage devices, and any other equipment necessary to provide the Service.
ServerCentral will retain exclusive administrative access to the ServerCentral-operated infrastructure of the Disaster Recovery Service for the duration of the agreement.
ServerCentral will perform periodic software and security updates, and replace any faulty hardware within the underlying infrastructure, per the manufacturers recommendations and industry best practices. Changes will occur during declared maintenance windows that will be agreed upon in advance with the Customer
In general, ServerCentral is not able to make any assumptions regarding your environment, applications, or business processes. All relevant information must be provided by the Customer for this portion of the service.
ServerCentral does not offer business impact analysis consulting services. ServerCentral can work with Customers during the sales process to identify gaps in preparation for a business continuity plan and offer recommendations to third parties that can offer consulting services.
ServerCentral cannot define which systems are critical for your business, computing environment, or critical business processes. This type of data, including Recovery Point (RPO) and Recovery Time Objectives (RTO), must be supplied by the Customer.

CUSTOMER RESPONSIBILITIES
Customer is responsible for providing all instructions and procedures that ServerCentral will follow during a disaster or fail back event. This includes identifying critical business processes and mapping servers and virtual machines to those processes, as well as the restoration order during a DR event.
Customer must inform ServerCentral of any requested modifications or changes to the Runbook. This includes the removal or addition of any physical servers or virtual machines involved in the Disaster Recovery Service.
Customer is responsible for performing any necessary business impact analysis and to defining critical business processes, as well as mapping these processes to individual systems.
Customer is responsible for the installation and operation of any and all scripts and applications installed on any customer managed servers or virtual machines.
Customer is responsible for the security of all scripts and applications installed on your servers. ServerCentral does not provide security auditing or disinfection of exploited software or servers.
Customer is responsible for maintaining current backups of customer-owned data. ServerCentral offers a fully managed backup service for physical and virtual servers, including the Enterprise Cloud. Please contact sales@servercentral.com for more information.
Customer is responsible for maintaining the list of authorized personnel on the ServerCentral Customer Portal and Enterprise Cloud Portal. Customer is also responsible for maintaining any user accounts created for the Enterprise Cloud. ServerCentral is not responsible for any unauthorized access to the Enterprise Cloud due to out of date access list information
Customer will designate and maintain a Customer Contact who can be made available to ServerCentral for troubleshooting or questions

Requests that are out of ServerCentral's support scope or responsibilities can be performed for a fee or on a time-and-materials basis. Please contact *sales@servercentral.com* for additional pricing information.

Additional Services

Backup: Customers are responsible for maintaining current backups of data on Customer-owned devices. ServerCentral offers a Managed Backup Service for physical or virtual servers, including Private Clouds. Please contact *sales@servercentral.com* for more information.

Monitoring: Customers are responsible for monitoring Customer-owned infrastructure or applications. If desired, ServerCentral can perform that monitoring though the Advanced Monitoring Service. For details and pricing information, please contact *sales@servercentral.com*.

Access Management

Customers are responsible for maintaining the list of authorized personnel in the ServerCentral Customer Portal. The access list can be self-maintained by Customers and can be reached at *https://portal.servercentral.com*. ServerCentral is not responsible for any unauthorized access or modifications to any Service due to out of date access list information.

For ServerCentral Managed Service deployments, Customers will need to designate contacts that can have the following access levels:

ROLE	ACCESS
Administrator	Full access to all account functions, including user management and all other functions listed below
DR Administrator	Able to declare disasters and authorize the execution of fail over and fail back procedures
Manage Users	Access to remove non-Administrator users or add users with permissions at or below the current level
Technical	Able to open support requests
Billing	Able to make billing inquiries related to the Services for the account
Sales	Able to order additional Managed Services via ServerCentral Sales

ServerCentral does not provide forensic analysis of application exploits as part of any managed service. If a Customer suspects that a customer-owned application or device has been compromised or exploited, the Customer is fully responsible for determining the attack vector and any compromise that may exist.

Service Level Agreements

Service Level Agreements (SLAs) are posted for each service at *https://www.servercentral.com/legal-information*. For questions regarding SLAs, please contact your account representative.

Service Interaction

ServerCentral provides customers with an online Customer Portal, allowing access to view and update account information and to open and review tickets. The portal can be accessed at *https://portal.servercentral.com/*.

For any issues, Customers should contact the ServerCentral NOC. Support requests are monitored 24x7x365 by on-site and off-site personnel. There are three ways to contact the NOC:

- Customer Portal: Preferred method for Customers to open tickets, as well as monitor ticket status.
- Email: Customers can email a request for ticket to support@servercentral.com
- Phone: (888) 875-7775 or (312) 829-1111, ext2 or +1 (312) 895-3005

For billing inquiries or to contact Sales, please call +1 (312) 829-1111.

Support requests

Support for all ServerCentral Managed Services is included with each product. However, support requests beyond the scope of the Managed Service or device may result in additional charges. Support staff will indicate if billable time is applicable prior to executing the support request. Additional support can be purchased at a one-time rate or through a pre-reserved set of hours. Please contact your account representative for additional details and pricing.

ServerCentral personnel are generally available to accommodate end user prescheduled maintenance requests. All requests for scheduled maintenance must be submitted as a s support request with, at a minimum, 48-hour advance notice of the requested date and time. Please note that submission of request does not guarantee the requested date and time until ServerCentral personnel confirm availability for the date and time requested. This is necessary to ensure scheduling of all required ServerCentral personnel and to allow sufficient time for ServerCentral Change Review processes to occur.

If you have any questions, comments, or concerns, please notify the Sales team via email to *sales@servercentral.com*.