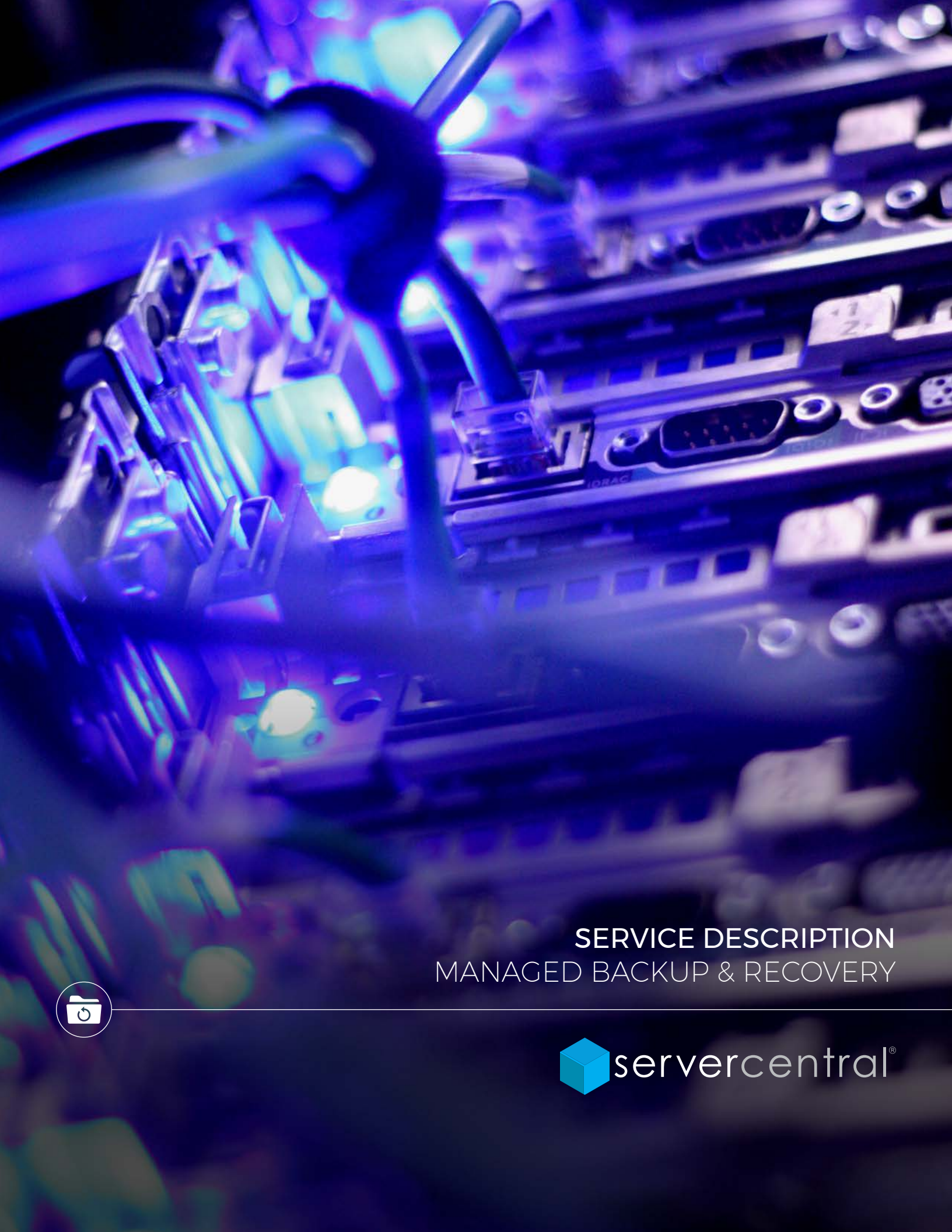


SERVICE DESCRIPTION
MANAGED BACKUP & RECOVERY

servercentral®

Contents

Service Overview

ServerCentral's Managed Backup & Recovery Service provides data protection for applications, files, and virtual or physical servers. Backups are performed, stored, and maintained in one of ServerCentral's data centers. Managed Backup & Recovery is a fully managed solution that is configured, administered, monitored, and supported by the ServerCentral Managed Services team. Restores can be performed on-demand, via service requests by the Customer, with options for restore into ServerCentral cloud services or Amazon Web Services.

ServerCentral will work with Customers to understand their data protection needs and configure the service parameters to support their unique business, financial, and technological requirements. Customers can adjust the frequency of backups, retention policy, encryption methods, and data locations to fit these requirements. Backup data can be replicated to a second ServerCentral-operated data center to provide physical redundancy. The Managed Backup & Recovery Service can protect data on virtual or physical servers.

As a fully managed service, ServerCentral's engineers support the underlying hardware & software tools used to deliver the Service, as well as administer and monitor the backup, replication, and recovery processes put in place. Customers receive a weekly Managed Backup & Recovery Service Report detailing the status of backup jobs, completion of jobs, and any other information about the jobs. Customers open support requests to create or alter backup jobs, change data retention policies, or get any additional information about the service.

In the default configuration, the Service will provide one (1) weekly full backup and daily incremental backups, with the data for all backups retained for 14 days in a ServerCentral data center. Customers can choose to have more or less frequent backups, shorter or longer retention timeframes, or replication to a specific data center. Replication to a second or third ServerCentral-operated data center is available as an option, for an additional fee.

The Managed Backup & Recivery Service enables encryption of data by default. The Service will generate the encryption keys necessary to protect the data. Data is encrypted as it is written to the Backup Server, and the resulting encrypted data blocks are stored to any backup files. The Service includes encryption-at-rest so data remains encrypted while stored in any ServerCentral-operated data center.

Restores for backup data are performed upon request. Data is generally restored to the primary system where the data originated. Managed Backup & Recovery does support the option for virtual machines or data to be recovered manually to a different target system. Target systems can include a new virtual machine created in ServerCentral's Enterprise Cloud or Managed Private Cloud service or an environment within Amazon Web Services. Manual recoveries are performed on a best-effort basis and will include additional charges for use of storage and/or cloud services.

This Service is available to all ServerCentral customers using services in a ServerCentral-operated data center, including Colocation, Enterprise Cloud, Managed Private Cloud, Managed Amazon Web Services or Dedicated Servers. Customers using ServerCentral's network connectivity services are also eligible to use the service.

Key Features

- Complete configuration & administration by ServerCentral's backup experts
- Backup job monitoring, with regular reporting
- Backup, retention, and replication schedule designed around Customer requirements
- Option for restore into ServerCentral cloud services
- 24x7 Service infrastructure health monitoring, performance metrics, and alerting
- Operated by trained & experienced backup and storage management engineers
- Firmware updates and vendor feature analysis
- Periodic tuning to adjust performance and effectiveness of the service
- Secure customer portal for ticketing and other deliverables

Implementation

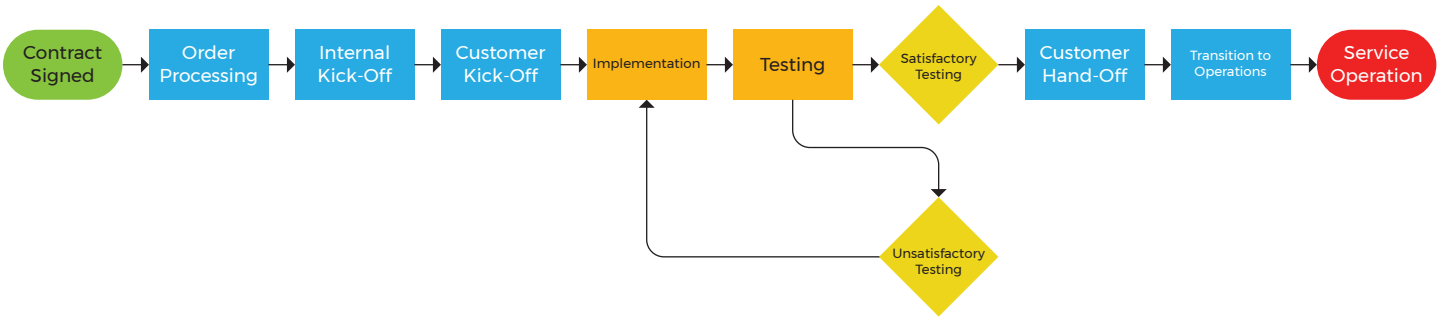
Validation

The Validation process begins with a comprehensive review of the information collected by Sales or Professional Services during the Assessment phase. The information usually includes a list of the applications & devices designated to be protected with the Service, Recovery Point Objectives (RPO) & Recovery Time Objectives (RTO), number and types of virtual & physical servers, credential exchange, permission for agent installation (if needed), long term retention schedules, and initial configuration details. Other client-specific requirements, such as audit controls, security 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 environment prior to customer hand off. This usually includes, but is not limited to access to source systems, verification of network bandwidth, monitoring and alerting configurations, 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 as soon as the first backup job is complete.

Service Delivery

Customer Hand-Off

The Project Manager or Provisioning staff will schedule a Customer Hand-Off Meeting, 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. The Meeting will usually include training on using 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.

Initial Configuration

During the Service Delivery, the ServerCentral Provisioning and Managed Services teams will review the configuration documents in the Technical Design Workbook and discuss any changes to scope. These changes, if any, will be documented in the Customer Workbook described above.

Many times, the Service will be integrated with additional Services provided by ServerCentral. Some examples include Colocation, Managed Firewall, Managed Storage, Enterprise Cloud 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

Using the baseline information in the Technical Design Workbook, the ServerCentral Engineering team will configure the baseline parameters for initial operation. The Customer can request to have some variables for the Service changed after the initial configuration. The variables include:

- Backup
  - Add/remove backup jobs
  - Add/remove source systems
  - Modify backup schedule
  - Modify retention schedule
- Restore
  - Request restore to source systems
  - Request restore to new target (optional, for-fee service)
- Reporting
  - Request job status reporting
  - Alter report frequency
- Replication
  - Add replication site (optional, for-fee service)

Once the Managed Backup & Recovery Service has been deployed, any configuration changes will be performed by ServerCentral. Information about the initial configuration of the Service will be available in the Customer Workbook or by submitting a service request.

Customers do not have access to the devices or software tools that deliver the Service, which are wholly administered by ServerCentral. Should any ongoing changes be necessary, such as changes in backup schedules, adding backup sources, or any other type of work, 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 associated with your Managed Backup & Recovery Service, please refer to the appropriate Service Description for further information regarding those services.

Service Operations

General Operations

The Managed Backup Service, including all security, environmental, access control, are 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.

In the event of hardware failure, ServerCentral personnel will proactively replace any failed hardware and restore the Service to normal operations. ServerCentral's network team will attempt to coordinate the replacement to fit with the Customer's normal change schedule.

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.

Customers may also view real time and historical graphs of the Service via the ServerCentral Customer Portal located at *https://portal.servercentral.com*.

ACCOUNT MANAGEMENT SERVICES	
Dedicated Client Relationship Manager	Included
IMPLEMENTATION SERVICES	
Hardware & Software Procurement & Assembly	Included
Data Center Provisioning (Generator+UPS-backed Redundant Power, Cooling, Cables, Rack)	Included
Resilient Facility (24x7 Physical Security, Video Surveillance, Fire Suppression, Monitored Access)	Included
Network Provisioning (routing, VLANs, cabling between source systems and Service)	Included
Feature Validation for Backup Tools	Included
Backup Job & Backup Site Configuration	Included
Assistance with setting up optional replication infrastructure	Optional
Assistance with backup agent installation on customer-operated devices (if needed)	Optional
24 X 7 MONITORING SERVICES	
Backup Platform Health Monitors	Included
Backup Platform Availability Monitors	Included
Backup Platform Performance Monitors	Included
Storage Capacity Monitors	Included
Backup Job status	Included
Replication job status	Optional
Custom Runbook coordinated with Customer	Optional

BACKUP SERVICE ADMINISTRATION (PROACTIVE SERVICES)	
Platform Administration	Included
Configuration changes per customer requests	Included
Managed Backup Service Configuration backup	Included
Change Management leveraging ServerCentral's change control process	Included
Change Management coordination with Customer	Included
Firmware Patching & Updates	Included
24 X 7 SUPPORT (RETURN TO SERVICE & VENDOR ESCALATION)	
Onsite sparing of identical hardware in US locations	Included
Hardware Troubleshooting	Included
Hardware Replacement	Included
Hardware Maintenance	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, operate, and maintain the Managed Backup & Recovery Service based on accepted industry best practices.
ServerCentral will retain exclusive administrative access to the Managed Backup Service for the duration of the agreement.
ServerCentral will monitor the hardware, software, and virtual systems used to deliver the Managed Backup Server for uptime and availability. In the event of hardware failure, ServerCentral will replace the hardware as soon as possible.
ServerCentral will monitor and maintain the associated operating systems & backup software, including periodically applying patches, software updates, operating system updates, and license keys as necessary.
ServerCentral will be responsible for the Managed Backup Service's system infrastructure support, including return-to-service and vendor escalation.
ServerCentral will perform firmware updates, including security updates, per the manufacturers recommendations and industry best practices. Updates will occur during declared maintenance windows that will be agreed upon in advance with the Customer
ServerCentral will monitor backup jobs for completion and take corrective action if jobs fail to complete. This may include notification to the Customer and may require joint collaboration between the Customer and ServerCentral to resolve potential issues.
ServerCentral will send a weekly summary of the current week's backup jobs. By default, reports are configured for Saturday delivery, but can be delivered more frequently or on different days of the week upon request.
ServerCentral will maintain the backup service configuration, including implementing any requested backup schedules and adding/removing systems.
ServerCentral will execute any on-demand backup or restore requests. All requests must be submitted as a support request using the ServerCentral Customer Portal, by email, or by phone per the instructions in the Service Interaction section of this document.
ServerCentral will perform firmware updates, including security updates, per the manufacturers recommendations and industry best practices. Updates will occur during declared maintenance windows that will be agreed upon in advance with the Customer
CUSTOMER RESPONSIBILITIES
Customer is responsible for installing, configuring, and maintaining all infrastructure and applications connected to the Service.
Customer is responsible for any data integrity testing, which can be enabled by requesting periodic restores of data for data verification purposes. ServerCentral is not responsible for any data corruption present in the source environment that may be backed up to the Managed Backup service during a scheduled backup run.
Customer is responsible for defining the backup schedule and contacting ServerCentral to request any removals, additions, or modifications to the backup schedule. This includes modifying retention times, adding/removing virtual machines or physical servers from the service, and updating IP addresses required to connect to hosts, guest operating systems, or hypervisors. ServerCentral is not responsible for any lost or unprotected data, or missed backup jobs, due to a failure by the Customer to maintain this information or supply it to ServerCentral.
In certain situations, usernames or other credentials may be required in order to complete a backup job. This is most commonly required for application-aware or database backups. If credentials, usernames, account permissions, or other account information is required for a backup job, the Customer will be responsible for maintaining & updating this information with ServerCentral. ServerCentral is not responsible for any lost or unprotected data, or missed backup jobs, due to a failure by the Customer to supply the proper credentials to ServerCentral.
Customer is responsible to ensure that any Customer-operated servers, virtual machines, guest operating systems, backup agents, customer network infrastructure and other necessary resources are online and available to the backup system. This includes, but is not limited to, network connectivity, opening required host/software firewall ports, physical connectivity, and application availability.
ServerCentral will not troubleshoot or provide any support relating to malfunctioning scripts or applications. Customer is responsible for maintaining the latest version of any and all installed scripts and applications, as well as the security of all scripts and applications installed on VMs. ServerCentral does not provide security auditing or disinfection of exploited software or servers.
Customer will designate and maintain a Technical 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

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*.

Managed Storage: Customers who need expanded production storage can connect to ServerCentral's Managed Storage, a SAN-based service available to Managed Backup customers. Please contact *sales@servercentral.com* for more information.

Cloud Services: ServerCentral offers Enterprise Cloud, Managed Private Cloud and Managed Amazon Web Services solutions that allow easy access to flexible and reliable compute resources. 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.
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 support request with, at a minimum, 48-hour advance notice of the requested date and time. Please note that submission of the 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*.