

SERVICE DESCRIPTION
MANAGED PRIVATE CLOUD



Contents

- Service Overview..... 3
 - Key Features 3
- Implementation 4
 - Validation..... 4
 - Implementation Process..... 4
 - Internal Kick-Off 4
 - Customer Kick-Off 5
 - Provisioning & Testing..... 5
 - Billing..... 5
- Service Delivery 6
 - Customer Hand-Off..... 6
 - Initial Configuration..... 6
 - Additional Modifications..... 7
- Service Operations..... 8
 - General Operations 8
 - Responsibilities 10
 - Additional Services..... 11
 - Access Management..... 12
 - Service Level Agreements..... 12
 - Service Interaction..... 13

Service Overview

ServerCentral's Managed Private Cloud Service is a flexible, scalable, and secure Infrastructure as a Service (IaaS) offering, deploying private infrastructure to meet a Customer's specific needs. Managed Private Cloud is delivered on an enterprise-class stack, including redundant servers, multi-gigabit networking, high performance storage, and an enterprise-class virtualization platform, all architected for the Customer's application requirements.

The Managed Private Cloud infrastructure is built with best-in-class technologies from market leading vendors to insure performance, stability, and resilience. The infrastructure can be configured in multiple ways, and is generally designed to be fully redundant and configured for automatic failover for compute and networking. The Service can include complete management of the underlying hardware and software tools used to deliver the Service, including virtualization platform management, hypervisor patching and updates, on-site hardware sparing, and full maintenance & support, all monitored 24 x 7 by ServerCentral's Network Operations Center (NOC).

Customers are allocated resource pools on dedicated hypervisors with Managed Private Cloud. Each resource pool includes a flexible configuration of network, compute, memory, storage, and security services, as well as the software

and access methods required to utilize the cloud resources. Customers create and manage virtual machines (VM) in each resource pool, with complete control over VM provisioning, VM size, and the guest operating system. Resource pools are deployed on dedicated infrastructure, allowing ServerCentral to optimize the performance and scalability of the service.

Managed Private Cloud is delivered from ServerCentral data centers in multiple geographies, giving Customers the option to deploy resources in different availability zones. The Service is also connected to ServerCentral's scalable, redundant data center network and core routing infrastructure, offering access to low-latency, high-performance internet transit. Managed Private Cloud provides an option for connectivity to Customer-operated infrastructure, as well as other third-party public cloud platforms.

VMs can be administered two ways. Customers can administer the VMs in Managed Private Cloud using the Private Cloud Portal. Or, ServerCentral can abstract the day-to-day VM management activities and include those as part of the service. Customers can also get information, request changes, and review service ticket history about the Managed Private Cloud service in general through ServerCentral's Customer Portal.

Key Features

- Based on proven, best-in-class hardware and software
- Dedicated infrastructure, fully customized for a single tenant
- Resource pool architecture, consisting of vCPU, vMemory, and SAN storage
- Flexibility to modify resource pools without VM downtime
- Dynamic scalability of resources to meet evolving requirements
- Generally configured for high availability and dynamic resource allocation
- 24x7 continuous monitoring, alerting, and support of the infrastructure
- Private Cloud Portal for control of VMs in each resource pool
- Option for complete VM configuration & administration by ServerCentral
- Secure customer portal for monitoring, documentation, ticketing, and other deliverables
- Option for integration with Customer-operated infrastructure
- Ability to connect to other third party public clouds

Implementation

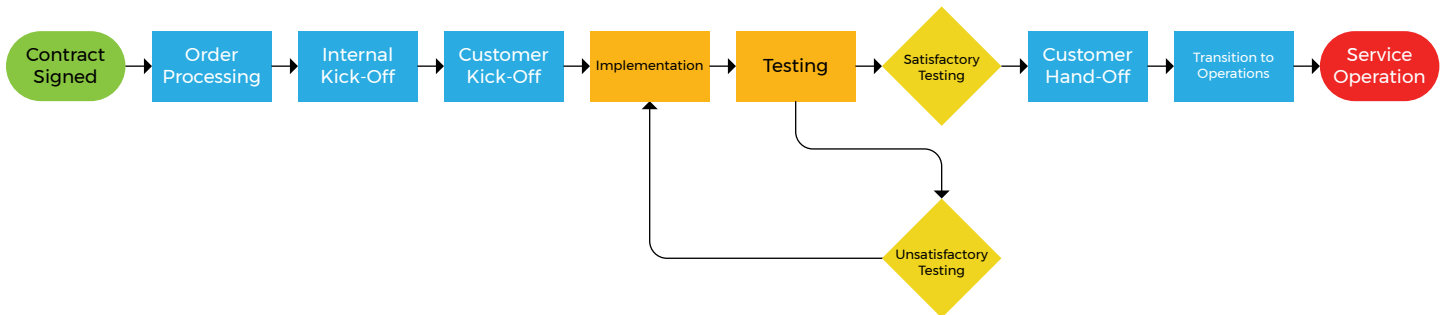
Validation

The Validation process begins with a comprehensive review of the information collected by Sales or Professional Services during the Discovery phase. The information usually includes the applications to be used with the Service, computing resources necessary to support the applications, performance requirements, design considerations for remote access, customer-operated hardware or software that will be integrated with the Service, expected growth, and compliance or regulatory controls. 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 Managed Private Cloud environment prior to customer hand off. This usually includes, but is not limited to cable pull testing, system redundancy verification, verifying network connectivity, 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 immediately after the resource pool is available and the Customer has the ability to create VMs.

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 Customer will receive training on using the Private Cloud Portal. A member of the Managed Service team will provide a demonstration of Private Cloud Portal functionality, including VM creation, IP assignment, firewall rules, and answer any general questions the Customer may have regarding the use of the Enterprise Cloud Portal.

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 ServerCentral Customer Portal is used with all ServerCentral services.

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, Enterprise Cloud, Disaster Recovery as a Service, 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

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

- Private Cloud Resources
 - Private Cloud location (data center)
 - Number of vCPUs
 - Amount of Memory (GB)
 - Amount of Storage (TB)
- Network Information
 - Public addresses whether provided by ServerCentral or the Customer
 - Public IP subnet mask
- Public IP descriptions (i.e. Gateway, VRRP switch, Server NAT, etc.)
- Private (RFC1918) addresses
- Private IP subnet mask, gateway, and DNS settings
- Per-customer IP tracking
- Firewall/VPN
 - Firewall configuration
- Load Balancer
 - Load Balancer configuration

Once the Managed Private Cloud has been deployed, any configuration changes to the resource pools will be performed by ServerCentral. Information about resource pool configurations will be available in the Customer Workbook or by submitting a service request.

The Managed Private Cloud service is configured to have ServerCentral perform management of the underlying hardware and virtualization infrastructure. Customers do not have access to the hardware and virtualization infrastructure used to deliver Managed Private Cloud, which is administered by ServerCentral. Should any changes to a resource pool or infrastructure 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.

Generally, Customers do retain control over VM creation. As noted above, Customers will receive access to the Private Cloud Portal, which is the primary tool used to interact with the service. As noted above, Managed Private Cloud can be configured to have ServerCentral perform VM Administration.

Customers are responsible for the operation of the VM, including the VMs operating system, the applications installed on the VM, monitoring the VM, and the support of any installed software on the VM.

Customers can request to have ServerCentral engineers assist with making changes to the Managed Private Cloud Service on their behalf. This assistance, as well as additional support, is available as a billable service on a time & materials basis. Please contact sales@servercentral.com for more information.

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

Service Operations

General Operations

The Managed Private Cloud service, including all ServerCentral-operated hardware and software, is monitored by ServerCentral’s Network Operations Center. Should any issues or anomalies be detected with the Service, 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. If the Managed Private Cloud is configured for high availability, ServerCentral’s Managed Services team will attempt to coordinate any service-impacting maintenance to fit with the Customer’s normal change schedule.

Based on the Managed Private Cloud configuration, 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 Procurement & Assembly	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, Physical Cabling)	Included
Feature Validation for hardware firmware & virtualization software	Included
Infrastructure Configuration	Included
24 X 7 MONITORING SERVICES	
Network Traffic Analysis & Volumetric DDoS monitoring on IP Transit Service	Included
Hardware Health Monitors	Included
Hardware Availability Monitors	Included
Hardware Performance Monitors	Included
Capacity Monitors	Optional
Custom Runbook coordinated with Customer	Optional
Complex Custom Monitor Development	SOW Based



INFRASTRUCTURE ADMINISTRATION (PROACTIVE SERVICES)	
Hypervisor Administration	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	Included
Firmware Patching & Updates	Included
Full creation management and administration of VMs	Optional
24 X 7 SUPPORT (RETURN TO SERVICE & VENDOR ESCALATION)	
Onsite sparring 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 maintain all software and hardware that provides the compute, network, and storage infrastructure for the Managed Private Cloud.
ServerCentral will monitor the Managed Private Cloud for uptime and availability. This includes any network switches, general Internet connectivity, storage devices, and any other equipment necessary to provide the Managed Private Cloud service. This does not include customer virtual machine monitoring.
ServerCentral will retain exclusive administrative access to the hardware and virtualization infrastructure of the Managed Private Cloud for the duration of the agreement.
ServerCentral will be responsible for hardware and virtualization infrastructure support, including return-to-service and vendor escalation.
ServerCentral will perform periodic software and security updates, install additional capacity, 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
ServerCentral will perform periodic software and security updates, install additional capacity, 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
CUSTOMER RESPONSIBILITIES
Customer is responsible for creating, maintaining, and managing any virtual machines, virtual machine templates, ISO or image catalogs, and IP address tracking of assigned IP pool. Customer is also responsible for managing and securing the underlying guest operating system including any script, application, or operating system updates.
Customer is responsible for managing and securing the underlying guest operating system including any script, application, or operating system updates.
Customer is fully responsible for the installation and operation of any and all scripts and applications installed on any customer managed servers or virtual machines.
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. If a Customer needs support regarding a specific script or application, please contact the software vendors support resources.
Customer is responsible for monitoring the guest operating system of the VM. ServerCentral offers in-guest VM monitoring as a service. Please contact sales@servercentral.com for additional information.
Customer is responsible for installing, configuring, and maintaining all Customer-operated infrastructure and applications connected to the Service
Customer is responsible for maintaining current backups of customer-owned data. ServerCentral offers a fully managed backup service for physical and virtual servers, including VMs the Managed Private 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 Private Cloud Portal. Customer is also responsible for maintaining any user accounts created for the Managed Private Cloud. ServerCentral is not responsible for any unauthorized access to the Managed Private Cloud due to out of date access list information
Customer will provide IP addresses for Customer-owned equipment attached to the Managed Private Cloud. If additional IP addresses are needed, please contact sales@servercentral.com .
Customer will designate and maintain a Technical Contact who can be made available to ServerCentral for troubleshooting or questions
Customer will designate and maintain a Technical Contact who can be made available to ServerCentral for troubleshooting or questions

Requests that are out of ServerCentral's support scope 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 VMs in a Managed Private Cloud. 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 through the Advanced Monitoring Service. For details and pricing information, please contact sales@servercentral.com.

Enterprise Cloud: ServerCentral offers a dynamically scalable public Infrastructure as a Service (IaaS) offering that can be used along with Managed Private Cloud to create hybrid cloud solutions. 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 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.