

CenturyLink Service Guide

CenturyLink Private Cloud on VMware Cloud Foundation

(Formerly Dedicated Cloud Compute Foundation (“DCC-F”))

This Service Guide (“SG”) sets forth a description of the CenturyLink Private Cloud on VMware Cloud Foundation Services offered by CenturyLink (or the “Services”), including technical details and additional requirements or terms. This SG is subject to and incorporated into the Agreement, CenturyLink TS Service Exhibit and Hosting Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedule, or Service Orders to SSG, shall mean SG.

Version	Previous	Section Modified	Date
CLO-20190513-SG- Private Cloud on VMware Cloud Foundation	CLO-20180824- SG- Private Cloud on VMware Cloud Foundation	Page 4	May 13, 2019

Table of Contents

CenturyLink Service Guide	1
CenturyLink Private Cloud on VMware Cloud Foundation	1
Service Description	3
CenturyLink Private Cloud on VMware Cloud Foundation Nodes	3
Single CenturyLink Private Cloud on VMware Cloud Foundation Nodes	4
Storage for CenturyLink Private Cloud on VMware Cloud Foundation Nodes	4
Adding RAM for CenturyLink Private Cloud on VMware Cloud Foundation Nodes	5
CenturyLink Private Cloud on VMware Cloud Foundation Guest Operating Systems and Virtual Appliances.....	5
VMware software and connectivity to the CenturyLink Private Cloud on VMware Cloud Foundation Nodes as listed in Table 1 below.....	5
TABLE 1 - CenturyLink Private Cloud on VMware Cloud Foundation Node - VMware	5
vCloud Director 9.0	5
Software and Security Patch Deployment	7
Definitions.....	9

CenturyLink Private Cloud on VMware Cloud Foundation

Service Description

CenturyLink Private Cloud on VMware Cloud Foundation is a hosted private cloud service that provides a managed infrastructure for Customer's use. The infrastructure includes use of the physical servers, space and power for the servers, virtualization Software system licenses, network connectivity to layer 2 switches, use of integrated storage services, management and monitoring of the servers and underlying infrastructure hardware virtualization Software packages system, and use of VMware's vCloud Director interface for automated instance provisioning. CenturyLink Private Cloud on VMware Cloud Foundation is based on CenturyLink's Hybrid Cloud management strategy. For clarity, CenturyLink Private Cloud on VMware Cloud Foundation uses VMware's Cloud Foundation Architecture, including Software Defined Networking and VSAN Storage for a completely integrated Hyper-converged Cloud Infrastructure.

VMware vCloud Director allows the Customer to configure the environment enabled by CenturyLink Private Cloud on VMware Cloud Foundation.

The primary capabilities of CenturyLink Private Cloud on VMware Cloud Foundation are:

- Hyper-converged Infrastructure – Integrated VSAN Storage with Solid State Drives for High IOPS performance capable of greater than 100,000 IOPS.
- Software Defined Networking – Provide Software Defined - Firewalls, Server Load Balancer, VPNs, Routing and VLAN creation.
- Scalable – A minimum 4 Node stack that can be expanded to multiple 64 Node stacks. Capability to increment one Node at a time. Allows for meeting a broad range of a Customer's private cloud requirements. A more detailed description of CenturyLink Private Cloud on VMware Cloud Foundation Node is set forth below.
- Allows the Customer to bring their own IP Addresses, Public or Private.

Optional Add-on Services:

- Integration with CenturyLink Cloud Application Manager Services. Cloud Application Manager must be purchased and contracted for separately, and if purchased allows Customer to utilize the Application Lifecycle Management and multi-cloud management options for Managed OS and Managed Applications with CenturyLink Anywhere Services.
- CenturyLink Services Management for building out your environment and configuring moves adds and changes as requested by the Customer must be purchased separately.

Note: The Service Level Agreement ("SLA") applicable to this Service is the "Managed Hosting Services" SLA Attachment.

CenturyLink Private Cloud on VMware Cloud Foundation Nodes

A CenturyLink Private Cloud on VMware Cloud Foundation Node is a dedicated, physical server as well as licensing, monitoring and management of the VMware Cloud Foundation Software Bundle, including vSphere Enterprise Plus, Software Defined Data Center Manager, NSX Enterprise, VSAN Advanced and VCenter. CenturyLink Private Cloud on VMware Cloud Foundation Nodes are built upon the HP ProLiant rack mount servers. Traditional server Nodes are available in various configurations.

CenturyLink Private Cloud on VMware Cloud Foundation Host options are the HPE DL-Gen10 or the Dell PowerEdge R640 with the Intel Scalable Xeon Platinum/Gold/Silver Series CPU Configuration Options. Note that a Minimum of 4 Nodes is required per Stack

Standard Options

Small Configuration	Medium Configuration	Large Configuration
<ul style="list-style-type: none"> • 20 cores • 128 GB RAM • 5 TB usable storage (SSD) per node 	<ul style="list-style-type: none"> • 28 cores • 256 GB RAM • 10 TB usable storage (SSD) per node 	<ul style="list-style-type: none"> • 36 cores • 512 GB RAM • 15 TB usable storage (SSD) per node

Custom Options

Custom Configuration
<ul style="list-style-type: none"> • 16 - 44 cores • 128 GB to 1.5 TB RAM • 5 TB to 17.5 TB usable storage (SSD) per node

Please note: RAM can be configured in 128 GB Increments. Usable storage can be configured in 2.5 TB increments with a 5 TB minimum.

Each Node is connected to dual homed 10 GigE switches with 4 10 GigE Ports. Two 10 GigE Ports are for VSAN traffic only and two 10 GigE Ports are for Customer traffic and VMware management. There is also a single GigE port connected for Integrated Lights Out (ILO) remote management. CenturyLink and its vendors do not have access to any information or traffic transmitted via the Service.

Storage for CenturyLink Private Cloud on VMware Cloud Foundation Nodes

All storage provided with CenturyLink Private Cloud on VMware Cloud Foundation is SSD Local Disks that are configured with VMware VSAN as part of the standard service offering. The default VSAN configuration is RAID-5. Additional VSAN Storage can be added to a CenturyLink Private Cloud on VMware Cloud Foundation Node through a change order process, which means a Service Order signed by the Customer. Additional storage must adhere to vendor requirements, including that all VSAN storage has to be symmetrical across all Nodes. For example, if Customer wants to add 2.5 TB of useable

storage to one Node, CenturyLink will require that Customer also purchases the same amount of storage to all Nodes in the stack.

Adding RAM for CenturyLink Private Cloud on VMware Cloud Foundation Nodes

Adding RAM to CenturyLink Private Cloud on VMware Cloud Foundation Nodes can be done through change order process requiring a new Service Order to be signed. Consistent with storage requirements above, and per vendor requirements, the additional RAM ordered and installed needs to be same amount for each of the Nodes in the Stack. For example, if Customer wants to increase a Node by 128 GB of RAM, CenturyLink will require that Customer increase the RAM on all Nodes in the stack.

CenturyLink Private Cloud on VMware Cloud Foundation Guest Operating Systems and Virtual Appliances

Customer has the ability to install any type of Guest Operating Systems (OS) or Virtual Appliance as long as it supports being installed on a VMware Hypervisor Platform and the version of Vsphere implemented. Customer is solely responsible for ensuring that any Guest OS or virtual appliance is and remains compatible with the CenturyLink Private Cloud on VMware Cloud Foundation infrastructure provided and maintained by CenturyLink.

Guest OS licenses may be provided by the Customer or CenturyLink can provide licenses for Window Server or RHEL for a fee. Additional third party software terms will apply.

Service Description

CenturyLink is responsible for maintaining and supporting all standard installed VMware software and connectivity to the CenturyLink Private Cloud on VMware Cloud Foundation Nodes as listed in Table 1 below.

TABLE 1 - CenturyLink Private Cloud on VMware Cloud Foundation Node - VMware Software Included as per CPU Socket Licensing

VMware® Software Package	Version
VSphere Enterprise Plus	ESXi 6.7 U1
VCenter Standard	6.7 U1
Software Defined Data Center	3.5
NSX Enterprise	6.4.4
VSAN Advanced	6.7
vCloud Director	9.5
vCloud Director Extender	1.1

vCloud Director 9.5

VMware vCloud Director (vCD) is the interface presented to the Customer. From the vCD login it is Customer’s responsibility to build out their networks, routers and security devices such as Server Load Balancers, Firewalls and VPNs. In addition the vCD environment is where a Customer will create Catalog of images, Templates, import open virtual formats (OVFs) and manage Snapshots. All communications

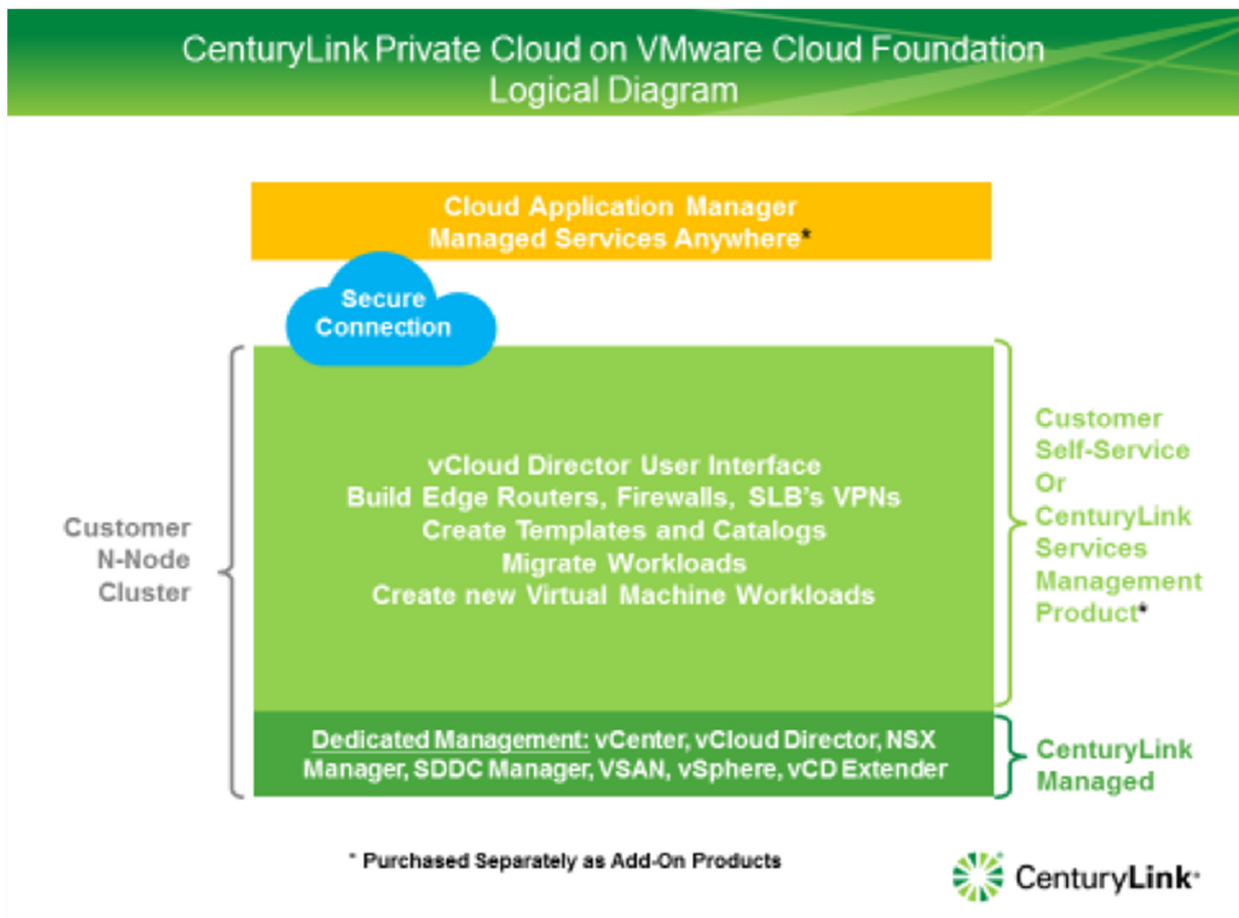
to the backend vCenter, NSX, VSAN, Vsphere and vCD Extender software applications are done through the vCD interface and not directly with the individual VMware software packages.

Monitoring of the Infrastructure

CenturyLink maintains and monitors all components of the CenturyLink Private Cloud on VMware Cloud Foundation Foundation Service - physical servers, including the repair and replacement of defective or failed hardware and the installation of firmware updates, as needed. Hardware upgrades, such as increasing RAM or increasing Storage, can be performed by CenturyLink for an additional fee. CenturyLink may subcontract any hardware support to the manufacturer or equivalent vendor in order to expedite repairs.

CenturyLink also monitors and maintains all of the VMware Software that is installed as part of the standard Service.

The following diagram identifies the Services and the optional Add-On Services that are available.



Software and Security Patch Deployment

CenturyLink will update CenturyLink Private Cloud on VMware Cloud Foundation Nodes with all VMware recommended security patches, updates or hot-fixes and will address the overall integrity and performance of servers. Security threats are evaluated, verified and tested before a patch is recommended to customers. Sometimes a reboot is necessary when a patch is distributed and installed, which CenturyLink will conduct during maintenance hours or coordinate with the Customer.

Customers must approve patches or updates prior to them being applied to their environment; however, CenturyLink is not responsible for any failure in the service, including SLAs if a Customer does not approve the installation of necessary patches or updates.

Please note that VMware Software Upgrades are not included as part of the standard Service but can be quoted and implemented for an additional fee.

Customer Responsibilities: Customer acknowledges and agrees that its failure to perform its obligations herein may result in CenturyLink's inability to perform the Services and CenturyLink shall not be liable for any failure to perform, including any SLAs in the event of Customer's failure. CenturyLink shall not be liable for any failure to perform in the event Customer does not fulfill Customer's responsibilities and requirements as detailed herein and in the event of Customer's errors or omissions in setting up the environment. In addition, CenturyLink is not responsible for any loss or corruption of data or information. CenturyLink's obligations related to data are exclusively governed by the Security and Compliance section of the applicable Agreement.

1. Customer acknowledges that all third party components of the Service are subject to the applicable vendor's decision to (i) not continue to provide or renew the Service with CenturyLink and/or (ii) modify or end of life a component(s). If any of the foregoing occurs, CenturyLink will use commercially reasonable efforts to migrate Customer to another comparable CenturyLink service at any time. Such migration will occur without regard to Customer's current term.
2. Licensing and Third Party Terms:

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to be bound by any additional licensing terms and conditions applicable to such third party software and that it will use such third party software strictly in accordance with such terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

For VMware, Customer must agree to the VMware End User Agreement terms located at: https://www.vmware.com/download/eula/universal_eula.html

3. Bandwidth: To avoid degradation of the Service, Customer must not have sustained bandwidth exceeding rated capacity of the device. CenturyLink will provide the device information as part of the installation process.
4. Access and Permissions: Customer shall provide CenturyLink's approved personnel, immediate access to any systems and devices if there is a service outage and at reasonable times in all other situations. Should CenturyLink determine the need for CenturyLink personnel to physically access the system or devices, Customer must allow CenturyLink personnel access to the

Customer site. Customer shall ensure that all permissions of any kind needed for the installation and operation of the Service are in place at all times. If the Customer has an Access Control List (ACL) that interferes with management connections, the Customer must allow CenturyLink access for management and monitoring.

5. Third Party: The Customer will not instruct or permit any other party to take any actions that would reduce the effectiveness of the Service. The Customer shall not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink. Credentialed scans from firewalls are not allowed.
6. Unauthorized Testing: Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink's network without the prior written consent of CenturyLink.
7. Provide Contact: Designate and maintain a Customer Contact during the service term and any applicable renewal term (including current contact information). "Customer Contact" means a technical point of contact with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable systems.
8. Provide Technical Support. Customer agrees to provide technical support during implementation and on-going support. Customer shall ensure environments are provisioned with servers, local incremental and replica storage, network connectivity, CPU and memory resources, and other infrastructure components; and replication is operational.
9. Neither Customer nor its representatives shall attempt in any way to circumvent or otherwise interfere with any security precautions or measures of CenturyLink relating to the Service or any other CenturyLink equipment.
10. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring its software and systems are up to date and supportable.
11. Customer further acknowledges it is solely responsible for ensuring all devices and hardware are upgraded to meet vendor configurations and agrees that CenturyLink's SLA only applies to currently supported configurations (including but not limited to related devices, software, and operating systems) at the time SLA support requests are triggered. If any configuration or version is identified as "unsupported" by a vendor, the Services are subject to all of the following conditions and/or requirements: (i) a service level objective ("SLO") referring to CenturyLink's reasonable effort to provide support will apply in lieu of any other applicable SLA and will automatically apply from the time CenturyLink receives notice from the vendor of such unsupported service; (ii) CenturyLink, in its reasonable discretion may elect to charge the Customer for any support or additional tasks/work incurred by CenturyLink resulting from Customer's continued use of unsupported configuration until Customer purchases the required and supported upgrades or extended support at an additional cost from the vendor. The requirement to purchase upgrades or extended support from vendor shall apply at any time,

regardless of any contract term, term commitments, or renewal periods. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink shall have no liability therefrom.

12. CenturyLink is not responsible for the service or the SLA if any changes by Customer affect the infrastructure or monitoring capability of CenturyLink.
13. Customer consents to CenturyLink's and its affiliates or subcontractors' use and transfer to the United States, or other countries, data or information (including Customer Contact information such as names, phone numbers, addresses and/or email addresses) of the Customer for the sole purpose of: (i) fulfilling its obligations under the Agreement; and (ii) providing information to Customer about CenturyLink's products and services. Customer represents that it will ensure that all information provided to CenturyLink is accurate at all times and that any business contact has consented to CenturyLink's processing of such information for the purposes identified herein.
14. Customer consents to CenturyLink collecting and compiling system and security event log data to determine trends and threat intelligence. CenturyLink may associate this security event log data with similar data of other Customers so long as such data is merged in a manner that will not in any way reveal the data as being attributable to any specific Customer.

Definitions

"Bring Your Own IP": Customers use their IP address in a migration

Catalog: A catalog is a container for vApp templates and media files in an organization. Organization administrators and catalog authors can create catalogs in an organization. Catalog contents can be shared with other users in the organization and can also be published to all organizations in the vCloud Director installation.

Client-to-Site VPN: A VPN client on the remote user's computer or mobile device connects to a VPN gateway on the organization's network. The gateway typically requires the device to authenticate its identity.

Cloud Foundation Architecture: VMware Cloud Foundation™ is VMware's new unified Software-Defined Data Center (SDDC) platform for private and public clouds. Cloud Foundation brings together VMware vSphere® (compute), vSAN™ (storage), and NSX® (network) virtualization into a natively integrated stack through automation and lifecycle management capabilities of the new VMware SDDC Manager™.

Data Center means the facility in which the systems are located.

Hybrid Cloud: Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms.

Hyper-convergence: A type of infrastructure system with a software-centric architecture that tightly integrates compute, storage, networking and virtualization resources and other technologies into a single high performance group of physical servers.

Managed Hosting means the set of CenturyLink managed server services that include but are not limited to Intelligent Hosting, Foundation Hosting, and Dedicated Cloud Compute each of which have their own respective Service Guides.

Multiple NAT/Double NAT: NAT (Network Address Translation) is being performed on a router, but additionally on another device connected in front of it resulting in double NAT. The public/private network boundary doesn't exist on the router as it is on the other device(s), which means that both the WAN and LAN sides of the router are private networks. Double NAT is a scenario where multiple routers on network are doing network address translation.

NAT: Network Address Translation.

NODE: The term Node means the physical server where the virtualization software resides and is synonymous in the industry with the term Host.

NSX: A virtual networking and security software product family created from VMware's vCloud Networking and Security (vCNS) and Nicira Network Virtualization Platform (NVP) intellectual property.

Site-to-Site VPN: Site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations.

Snapshot - A snapshot preserves the state and data of a virtual machine at a specific point in time. The state includes the virtual machine's power state (for example, powered-on, powered-off, suspended). The data includes all of the files that make up the virtual machine. This includes disks, memory, and other devices, such as virtual network interface cards.

Software-Defined Data Center (SDDC): A data center facility where the elements of the infrastructure are virtualized and delivered as a service and where the provisioning and operation is abstracted from the hardware and fully implemented through software.

Software-Defined Networking (SDN): Software-defined networking is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

Solid-State Drive (SSD): A solid-state storage device that uses integrated circuit assemblies as memory to store data persistently.

Template: A template (also called a golden image) is a perfect, model copy of a virtual machine (VM) from which an administrator can clone, convert or deploy more virtual machines.

vApp: Stands for Virtual Application and consists of one or more virtual machines that communicate over a network and use resources and services in a deployed environment. A vApp can contain multiple virtual machines.

vCloud Director Extender: VMware Inc.'s vCD Extender runs on vCloud Director is used for self-service migration of virtual workloads.

vCloud Director (vCD): VMware Inc.'s cloud computing management tool. It manages Infrastructure as a Service (IaaS) architectures by monitoring and controlling various cloud-computing components, such as security, virtual machine (VM) provisioning, billing and self-service access.

vLAN: A virtual LAN (vLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2)

VSAN: VMware Inc.'s Virtual Storage Area Network, which is a software-defined storage offering from VMware that enables enterprises to pool their storage capabilities and to instantly and automatically provision virtual machine storage via simple policies that are driven by the virtual machine. CenturyLink is not responsible for unauthorized access if Customer does not take its own steps to maintain security, including encryption.