Synoptek { Private Cloud

Table of Contents

1 Introduction

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Cloud Assessment and Planning (the "Service"). The service definitions found herein reflect Companies standards at the time the Service Order(s) was issued. Company reserves the right to change any particular standard herein to reflect the current company's best practices or industry standards at its sole discretion with or without notice.

2 Service Offerings

Synoptek owned Private Cloud Hosting Services are designed to maximize the value of running workloads on a secure private cloud platform, hosted and managed by Synoptek, consisting of specific units of x86 processing, power, storage, memory capacity and comprehensive network services. This enables customers to access cloud computing capabilities without having to build and maintain their own datacenter. Many organizations wanting to host sensitive data or high performance applications with a cloud provider require architectural options that are not available from standard, public, multi-tenant cloud services. Synoptek owned Private Cloud Hosting Service offers more flexibility than public cloud

Synoptek owned Private Cloud Hosting Services (herein called the "Service Offering" (s)) allows for the hosting of virtual machines (here in called VMs) and applications on two different core platforms allowing IT organizations to extend their cloud infrastructure and software deployments beyond their datacenters.

- VMware® Powered
  - Virtualization: based on VMware® vSphere®. VMware vCenter is provided and to be used for management and automation.
  - **Region:** Rochester, NY / Dallas, TX / Santa Clara, CA, Las Vegas, NV
- Microsoft® Powered
  - Virtualization: based on Microsoft Windows Server Hyper – V technology. Optional; Microsoft System Center components are used for management and automation.
  - **Region:** Rochester, NY / Dallas, TX / Santa Clara, CA, Las Vegas, NV

All Service Offerings offer selections for compute, storage, networking and public IP address resources that can be expanded as your needs grow. Additionally, added features such as Data Protection, Managed Services and a growing list of ancillary data and application services are offered with Synoptek owned Private Clouds.

All services include built-in infrastructure redundancy, high availability, higher disk I/O and 10Mbps Bandwidth at no additional charge.

Having Service Offerings available in multiple regions enables you to manage region specific resources. You can run workloads closer to your business specific customers or comply with various regulations and other legal requirements. You can also choose to leverage multiple regions to enable redundancy of your data or workloads. Redundant configuration can play a role in your business continuity and disaster recovery strategy, which can include failing over to a second data center, protecting data by deploying to a second data center, or recovering operations in a second data center in the event of a disaster

There are three available starter packs for both Service Offerings called Basic, Standard and Plus.

Basic	1 Usable Blade (+1 Spare), 32Ghz Usable, 256GB RAM Usable, 12 Cores
Standard	2 Usable Blade (+1 Spare), 64Ghz Usable, 512GB RAM Usable, 24 Cores
Plus	3 Usable Blade (+1 Spare), 128Ghz Usable, 1024GB RAM Usable, 48 Cores

Customer can add additional resources where needed. *(Note: Plus cannot be upgraded)*

CPU Upgrade - BASIC	Add 4 Cores / 12Ghz
RAM Upgrade - BASIC	Add 128GB RAM
CPU Upgrade - STANDARD	Add 8 Cores / 24Ghz
RAM Upgrade - STANDARD	Add 256GB RAM

2.1 Access to Platform Management Console

Access to a management console (the "Console") will be made available once services have been enabled. This will serve as the primary means of interfacing with the Service Offering which will allow for access, consumption, and management of cloud resources on that dedicated platform as well as virtual datacenter management, configuration of network services, and VM instance lifecycle management.

- vSphere Client is typically used to connect to vCenter, this access is provided for VMware.
- Hyper-V Manager; a Microsoft Management Console (MMC) snap-in is used to manage the Hyper-V role and the virtual machines configurations

Application Programming Interface Access

Customer will have full access to any hypervisor specific APIs for programmatic resource management, hybrid management or workload migration.

2.2 Technical Documentation and Orientation

Onboarding will provide the necessary URLs and verify the customer can successfully connect to the Service Offering and provide a 30-minute familiarity session to the platform. It is assumed that the customer has enough third party training and should be familiar with the hypervisor of choice.

3 Support

Synoptek will provide support for problems that the Customer reports to assist with adoption of and related to the Service Offerings 24x7x365. See Appendix A for more support matrix

- Customer may assign up to 3 named contacts to contact the service desk on behalf of the Customer. The Service Desk is a central point of contact for handling the following Customer issues:
    - Incident ownership, initial troubleshooting and escalation of incidents within the defined Service Level Agreement (SLA);
    - Respond to "how to" questions such as how to provision or remove cloud instances and migrate data.
    - Respond to access issues and requests;
    - The service desk can be contacted at:
        - Toll-Free number TBD; region based.
        - Email at support@synoptek.com
        - https://www.autotask.net/clientportal/

The Client Advisor (CA) will serve as the single point of accountability in delivering the Service, providing the following support:

- Establish and manage relationship with identified Customer contacts.
- Work with the operations team proactively to identify opportunities and continually improve.
- Customer experience with respect to the services outline here.

- Define key measures and periodically review them with Customer.
- Pro-actively explain any high severity incidents, root causes, and resolution efforts.
- Coordinate with other business units as agreed, to ensure a unified Synoptek solution.
- Develop and review cloud consumption with Customer including forecast and growth projections.
- Public Cloud Best Practices
- Support Ticket Review
- Overall Cost Review

3.1 Service Provisioning

Synoptek will provide the following provisioning services:

- Implementation of platform components (physical servers, physical storage, and physical network devices) needed to support contracted Service Offering when applicable.
- VMWare
    - Installation of VMWare vCenter Server Software created and configured as a VM.
    - Installation of VMWare ESXi Server in single datacenter location across necessary hosts.
    - Configure and Present initial storage volume(s)
    - Configure Host Clustering
- Microsoft
    - Installation of Windows Server
    - Installation of Hyper-V Role
    - Configure and Present initial storage volume(s)
    - Configure Host Clustering
- Providing initial network resources including default public IP addresses when applicable.
- Creating the initial administrative user account in the Console using default administrator privileges and system preferences.

Customer will be responsible for the following provisioning services:

- Establishing the necessary bandwidth to take advantage of services being provided.
- Establish the necessary VPN connectivity (if needed).
- Creating additional user accounts in the Console, and changing default system preferences as needed.
- Creating and configuring applicable VMs, networks, network security settings and requirements.
- Installing and configuring custom or third-party applications and operating systems on deployed VMs.

3.2 Data Recovery

Synoptek will provide the following services with respect to data recovery of the Service Offering Platform ONLY:

- Data protection, such as routine backups, for the Service Offering infrastructure, including top-layer management and user-management interfaces owned and operated by us.
- Data and infrastructure restoration for the Service Offering infrastructure, including top-layer management and user-management interfaces owned and operated by us.

Customer will be responsible for the following services with respect to data recovery within the Service Offering:

- Data protection, such as routine backups, for the data and content accessed or stored on Customer VMs or storage devices, configuration settings, etc.
- Data, content, VM, and configuration restorations for assets accessed or stored on the customers Console.
- Managing their business continuity plan.
- See Data Protection Service 4.3 **(Optional Service – Additional charges apply)**
- See Disaster Recovery 4.4 **(Optional Service – Additional charges apply)**

3.3 Monitoring

Synoptek will provide the following services with respect to monitoring:

- Monitoring the infrastructure, infrastructure networks, top-layer management and user-management interfaces, and computing, storage, and network hardware for availability, capacity, and performance.
- Perform regular Capacity checks on cluster utilization and storage utilization and will communicate to Customer when the Capacity reaches 75% utilization
- See Appendix C for Infrastructure Monitoring Parameters

Customer is responsible for the following services with respect to monitoring:

- Monitoring the assets deployed or managed within the account, including but not limited to VMs, operating systems, applications, specific network configurations, operating system or application vulnerabilities, etc.
- Monitoring capacity utilization of resources allocated to Customers virtual environment.
- Review Synoptek provided capacity updates and request additional resources from Synoptek when capacity utilization limits are reached.
- See Managed Services 4.5 **(Optional Service – Additional charges apply)**

3.4 Incident and Problem Management

Synoptek will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which Synoptek has direct administrative and/or physical access and control, such as Synoptek provided Private Cloud Hosting servers, storage, and network devices.

Customer is responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- User-deployed and user-configured assets such as VMs, virtual networking, custom developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.
- Operating system administration including the operating system itself or any features or components contained within it.
- Performance of user-deployed VMs, custom or third-party applications, customer databases, operating systems imported or customized by customer, or other assets deployed and administered by customer that are unrelated to the Console or the Service Offering platform.

3.5 Change Management

Synoptek will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the Console, the network services console, or the Service Offering platform.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Console, the network services console, or the Service Offering platform.

Customer is responsible for:

- Management of changes to their VMs, operating systems, custom or third-party applications, databases, and administration of general network changes within the Customers control.
- Administration of self-service features provided through the Console, up to the highest permission levels granted to the customer, including but not limited to VM and network functions, backup administration, user configuration and role management, general account management, etc.

3.6 Security

Responsibility for the end-to-end security of the Service Offering is shared between Synoptek and the Customer. Synoptek will provide security for the aspects of the Service Offerings over which Synoptek has sole physical, logical, and administrative level control. The Customer is responsible for the aspects of the Service Offerings over which the customer has administrative level access or control. The primary areas of responsibility as between Synoptek and the customer are set forth below.

Synoptek will use commercially reasonable efforts to provide:

- **Physical Security:** The Service Offering is housed in state of the art data center facilities. The following controls are in place at the physical layer in the data centers:
    - Equipment Location: The Service Offering operates in the United States. A site selection team determines each data center site. The site selection process includes a rigorous assessment, ensuring that each site has appropriate measures and countermeasures in place such as man traps, locking cages, staffed personnel and cameras.
    - Data Centers: Synoptek use well-established data center providers to host workloads. Each data center is certified. The providers are reviewed by independent third party auditors to meet the physical security requirements for, SOC 1 Type 2/SSAE 16 and SOC 2 Type 2. SOC2 reports outlining these specifications are available, upon request, subject to execution of an appropriate confidentiality and nondisclosure agreement.
- **Information Security:** Synoptek will protect the information systems used to deliver the Service Offerings for which Synoptek have sole administrative level control.
- **Network Security:** Synoptek will protect the networks containing our information systems up to the point where the Customer haves some control, permission, or access to modify the networks.
- **Security Monitoring:** Synoptek will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offerings over which Synoptek has sole administrative level control. This responsibility stops at any point where the customers has some control, permission, or access to modify an aspect of the Service Offerings.
- **Patching and Vulnerability Management:** Synoptek will maintain the systems Synoptek use to deliver the Service Offerings, including the application of patches Synoptek deem critical for the target systems. Synoptek will perform routine vulnerability scans on a quarterly basis to surface critical risk areas for the systems Synoptek use to deliver the Service Offerings. Critical vulnerabilities will be addressed in a timely manner.

Customer is responsible for the following:

- **Information Security:** Customer is responsible for ensuring adequate protection of the information systems, data, content, or applications that customer deploys and/or access on the Service Offerings. This includes but is not limited to any level of patching, security fixes, data encryption, access controls, roles, and permissions granted to the Customers internal, external, or third party users, etc. Customer must also meet their own regulator controls.
- **Network Security:** Customer is responsible for the security of the networks over which the Customer has administrative level control. This includes but is not limited to maintaining effective firewall rules, exposing only communication ports that are necessary to conduct business, locking down promiscuous access, etc.
- **Security Monitoring:** Customer is responsible for the detection, classification, and remediation of all security events that are isolated within the Customers virtual instance(s), associated with VMs, operating systems, applications, data or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which the Customer is required to participate and which are not serviced under another Synoptek provided security program.

3.7 Storage

The Service Offering includes persistent block storage as a part of the subscription. There is one storage option available; Blended Storage. The storage options allow for growth without downtime. The Service Offering does not include any storage and must be acquired at the time of purchase. The customer can specify additional storage which can be included with the Service Offering. After the time of purchase, the customer can purchase additional storage by submitting a ticket through the service desk. See Appendix B in this Service Description for additional information.

3.8 Networking Services

The Service Offerings include the following network services as a part of the Service Offering:

- Network Address Translation (NAT): Separate controls for source and destination IP addresses, as well as port translation.
- Dynamic Host Configuration Protocol (DHCP): Configuration of IP pools, gateways, DNS servers, and search domains.
- Load Balancing: Simple and dynamically configurable virtual IP addresses and server groups.
- Static Routing: Static routes for destination subnets or hosts.
- No vDom or Virtual Firewall is included.

ENHANCED LOAD BALANCING: SSL offloading and Application level load balancer. **(Optional Service – Additional charges apply)**

3.9 Self-Directed Migration

Customer have the option of migrating VMs or data over the public network using native VMware tools and hybrid connectors built into the version of vSphere running on the customers provisioned Service Offering.

PROFESSIONAL MIGRATION SERVICES: are not included but are available for the conversion of existing physical or virtual services. These capabilities support onboarding to Synoptek and export from Synoptek. **(Optional Service – Additional charges apply)**

3.10 Exclusions

- Virtualization design.
- Evaluation of Customer's IT operations and organization.
- Migration of any existing physical servers into a virtualized server environment.
- Virtualization platform software licenses in Customer's data center.
- Application profiling, which includes identification of applications compatible with virtualization and analysis of server/application interdependencies.
- Managed Services above the hypervisor in management of Customer's virtual environment.
- Any services, tasks or activities other than those specifically noted in this Service Description.
- The development of any intellectual property created solely and specifically for the Customer.
- Synoptek will not be responsible for defects or malfunctions in third party software not managed by Synoptek Managed Services.
- Synoptek will not be responsible for end-points not managed by Synoptek Managed Services.

4 OPTIONAL SERVICES

The following services are presented to enhance the Private Cloud Service Offering.

4.1 Firewall Services (Optional Service – Additional charges apply)

Firewall Services is an optional service that delivers a vDom firewall that resides on Synoptek infrastructure and provides the following:

- Firewall: Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for all protocols.
- Site-to-Site Virtual Private Network (VPN): Uses standardized IPsec protocol settings to interoperate with all major VPN vendors.
- Web Filtering: Designed to restrict or control the content a reader is authorized to access, delivered over the Internet via the Web browser. It may be used to improve security, prevent objectionable activities, and increase productive within an organization.
- Intrusion Prevention System: Will to monitor for known attack signatures, either alerting or blocking matching traffic as per vendor recommendations and best practices.
- Application Control: Detects and take action against network traffic depending on the application generating the traffic.
- Gateway Level Antivirus: Enable protection on HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP sessions.
- Active Directory Integration.
- See Appendix B for Additional Firewall Details.

SSL VPN: SSL VPN enables remote users to connect securely to private networks behind the firewall. **(Optional Service – Additional charges apply)**

4.2 Seed Loading Service (Optional Service – Additional charges apply)

Seed Loading Service is an optional data copy service for the purpose of transferring large numbers of VMs or templates from your local environments to your Synoptek environment.
As part of this service, Synoptek will:

- Ship a physical storage device, permitting the customer to load VMs or templates onto the device and ship it back to Synoptek using the customers preferred carrier. The content that the customer load onto the device will be encrypted thereby ensuring security of your content during transfer.
- Transfer the data from the device into your instance.

Customer will be responsible for:

- Following the instructional documentation accompanying the storage device.
- Returning the storage device to us within 45 calendar days from date of shipment. If the storage device is not returned within the 45-day period, you will pay us a replacement fee for the storage device plus any shipping and handling charges, as assessed by us.
- Backing up any data, applications, or VMs transmitted via the service; Synoptek will not be responsible for any data loss that may occur as a result your use of this service. This optional service may be subject to additional fees.

4.3 Data Protection Service (Optional Service - Additional charges apply)

Data Protection Service is an optional service that provides secure, backup and recovery capabilities that enable the customer to protect important VM data and content hosted in their Service Offering environment.
Data Protection Service may be ordered and is subject to additional fees based on the amount of VMs being backed up and retention required. For more information, see *Service Description for Data Protection Service*

4.4 Disaster Recovery (Optional Service - Additional charges apply)

Disaster Recovery is an optional service that provides secure recovery capabilities and resources into a different datacenter for full site recovery. For more information, see *Service Description for Disaster Recovery*

4.5 Managed Services (Optional Service - Additional charges apply)

ITAAS SERVER - Synoptek will provide enhanced management of customer managed virtual servers including 24x7 monitoring, OS patch management, backup management, Anti-Virus, and OS troubleshooting within the Service Offering. Synoptek will also provide monthly reports documenting critical alerts, scans, and event resolutions. Should a problem be discovered through our remote monitoring, Synoptek shall make every attempt to rectify the condition in conformance with the Service Level Agreement. For more information, see *Service Description for ITaaS*

ITAAS SITE **-** Synoptek will provide enhanced management of customer managed virtual router, virtual switch and virtual firewall systems within the Service Offering. Synoptek will also provide monthly reports documenting critical alerts, scans, and event resolutions. Should a problem be discovered through our remote monitoring, Synoptek shall make every attempt to rectify the condition in conformance with the Service Level Agreement. For more information, see *Service Description for ITaaS*

4.6 Microsoft SPLA licensing and Setup (Optional Service- Additional charges apply)

Synoptek must provide Microsoft specific licensing's under the Microsoft SPLA rules and guidelines. All licensing must run within the walls of Synoptek datacenters. Synoptek can assist with the installation of Synoptek provided SPLA licensing though it's Move, Add, Change and Delete, Service Request process and/or Professional Services.

5 Appendix A - Supported Services

Synoptek 24x7x365 Service desk will work with your team to provide consulted and informed support around the self-serve functions at a minimum as it relates to the Service Offering platform once transitioned to support. Additional Managed, Application and Professional Services are available optionally as stated in the Service Description.

6 Appendix B - Features

Hosts:

- Designed to have no single point of failure
- Fault Tolerant capable of suffering host fails
- Fully automated VM and Storage movement and redundant N+1 compute and storage capacity. Architected for resiliency and high availability. (Does not include disaster recovery capability)
- Hypervisor will boot from SAN

Network:

- Multiple, redundant connections to Synoptek core network

Storage:

- Designed to have no single point of failure
- 1Gbps iSCSI SAN fabric
- Blended Storage consisting of SSD and Standard Disk

vDom Firewall:

- 24 x 7 stateful packet filtering
- 90 days of log retention
- Device monitoring (excluding security event monitoring)
- Firmware and signature updates as determined by Synoptek
- Standard reporting depending on the selected configuration
- Maximum of two (2) configured security zones
- Up to two (2) VLANs
- Unlimited standard configuration changes as reasonably requested at no additional charge
- Problem resolution on firewall issues
- Antivirus and intrusion detection and prevention
- 10 Mbps of Internet bandwidth
- URL and category-based filtering (including subcategories)
- Active Directory integration for user- or group-based security policies
- Multiple web content filtering profiles (requires optional AD integration)
- Site-to-site VPN (up to ten)

7 Appendix C - Monitoring

Synoptek monitors our data center environments using SNMP, syslog and other API based technologies. Comprehensive monitoring templates ensure that all aspects of the environment are monitored for performance, availability, and capacity. The following metrics are monitored:

VMWare & Hyper-V

Category	Datapoint
UCS hardware status monitoring	✓ Chassis ✓ Power Supplies ✓ IO Modules ✓ Blades Servers ✓ Fabric Interconnect ✓ Operational status ✓ Fault condition ✓ Physical Switch I/O operational and administrative status ✓ UCS chassis Management controller statistics ✓ CPU Statistics
UCS environmental status monitoring	✓ Power status ✓ UCS cooling fan type and condition ✓ Temperature statistics on all components ✓ Voltage status for each component
Storage Monitoring	✓ Disk, Memory Modules, Chassis Temperature ✓ Inventory – Storage Processors, Front end (FC, Gb) Ports, Back End (FC,SAS) Ports, Disk Drives ✓ Configuration Details – LUN details, Raid Groups, Host-Port Mappings ✓ Availability – SP Status, SP Port Status, FC/Gb/SAS Ports Status, Disk Drive Status, LUN Status and Raid Group Status ✓ Performance – Array, Device Drive, LUN, Storage Pool and Storage Volume Statistics
Virtual environment monitoring	✓ Server availability ✓ Server performance (**CPU**: Clock Speed, CPU utilization **Memory**: Free, Total and Used Memory **Disk**: Free, Used, Total and Virtual Allocation) ✓ Network Interface – Total Bytes/sec ✓ Network Interface – packets Outbound errors ✓ VMware & Hyper-V Hypervisor Host Storage: Storage Type, Availability Storage size, used size and free size

8 Appendix D - Reporting

Reports	Description	vSphere	Hyper -V	Pre-generated	Upon Request
VM Inventory Reports	Device details Report	X	X		X
	Disk space Report	X	X		X
	Virtual Hardware Report	X	X		X
	Software Report	X	X		X
	Virtualization Performance Report	X	X		X
Network Reports	Interface errors and discards	X	X		X
	Interface utilization and traffic	X	X		X
Firewall	Bandwidth Report	X			X
	Basic Security Report	X			X
	Detailed Application Usage Report	X			X
	Threat Report	X			X
	User Report	X			X
	Web Usage Report	X			X
Security Reports	Hypervisor based Anti-Malware status report	X			X
	Hypervisor based Anti-Virus status report	X			X
	Log Inspection Report (HIPAA Only- Agent)	X			X
	Log Inspection Detailed Report (HIPAA Only - Agent)	X			X

9 Appendix E – HIPAA Considerations

(R)= Implementation is required. (A)= Implementation is addressable.

- The safeguard must be assessed to whether or not it is a reasonable and appropriate safeguard in your environment. If the safeguard is not implemented, then it is required to document the reason why and also implement an equivalent alternative safeguard if reasonable and appropriate.
- Where there is a shared responsibility with Customer and Synoptek, each is responsible uniquely for the service they retain administrative control over.
- (OPT) = Optional Service
- Adding Optional Managed Services (ITaaS) will require a reevaluation of the HIPAA standards below.

Standards	Implementation Specifications	Customer	Synoptek
Administrative Safeguards			
Security management process	Risk analysis (R)		X
	Risk management (R)	X	X
	Sanction policy (R)	X	X
	Information system activity review (R)		X
Assigned security responsibility	Assigned security responsibility (R)	X	X
Workforce security	Workforce authorization and/or supervision (A)	X	X
	Workforce clearance procedures (A)	X	X
	Workforce termination procedures (A)	X	X
Information access management	Isolating heath care clearinghouse function (R)	N/A	N/A
	Access authorization (A)	X	X
	Access establishment and modification (A)	X	X
Security awareness and training	Security reminders (A)	X	X
	Protection from malicious software (A)	X	X
	Log-in monitoring (A)	X	X
	Password management (A)	X	X
Security incident procedures	Response and reporting (R)	X	X
Contingency plan	Data backup plan (R)	X	X
	Disaster recovery plan (R)	X	X
	Emergency mode operation plan (R)	X	X

	Testing and revision procedure (A)	X	X
	Applications and data criticality analysis (A)		X
Evaluation	Security evaluation (R)		X
Business associate contracts and other arrangements	Written contract or other arrangements (R)	X	
Physical Safeguards			
Facility access controls	Contingency operations (A)		X
	Facility security plan (A)		X
	Access control and validation procedures (A)	X	X
	Maintenance records (A)		X
Workstation use	Workstation use (R)	X	X
Workstation security	Workstation security (R)	X	X
Device and media controls	Media disposal (R)		X
	Media re-use (R)		X
	Accountability (A)		X
	Data backup and storage (A)	X	X
Technical Safeguards			
Access control	Unique user identification (R)	X	X
	Emergency access procedure (R)	X	X
	Automatic logoff (A)	X	X
	Encryption and decryption (A)	X	
Integrity	Mechanism to authenticate ePHI (A)	X	
Person or entity authentication	Person or entity authentication (R)	X	
Transmission security	Integrity controls (A)	X	
	Encryption (A)	X	