



Data Center Virtual Server Hosting OLA

Office of Information Technology
Data Center Infrastructure
March 23, 2022



Virtual Server Hosting Operational Level Agreement (OLA)

Created by Kenneth Cooper

Table of Contents

General Overview	2
Service Description	2
2.1 Service Scope	2
2.2 Equipment and Software	2
2.3 OIT Data Center.....	3
2.4 Operational Support	3
2.5 Optional: Systems Administration	3
2.6 Optional: Network Firewalls and Scanning.....	3
2.7 Optional: OIT Data Backup and Recovery Service	3
2.8 Optional: Off-site Copy of Virtual Server Data	4
Roles and Responsibilities.....	4
3.1 Service Recipient Responsibilities and Requirements.....	4
3.2 Service Provider Responsibilities and Requirements	5
3.3 Parties	5
Service Management	6
4.1 Service Uptime	6
4.2 Hours of Support.....	6
4.3 Service Requests	6
4.3.1 Normal Incident Handling.....	6
4.3.2 Major Incident Handling	6
4.4 Service Management	7
4.5 Charges.....	7
OLA Review & Update.....	7
Appendix A - Explanations for Customer Responsibilities.....	7

General Overview

The Office of Information Technology (OIT) provides a Virtual Server Hosting service to the UCI campus. Unlike “colocation” or other physical server hosting services, virtual server hosting is a service where a virtual server is leased and the customer is not required to make an initial investment in buying server and storage hardware. [Additional information about the service](#) can be found on the OIT website. This is an Operational Service Level Agreement (OLA) between OIT and Virtual Server Hosting customers (which includes internal OIT units). The scope of this document includes:

- Services provided by OIT to Virtual Server Hosting customers.
- Levels of response time, availability and support associated with these services.
- Responsibilities of the OIT service provider and the customer.
- Processes for requesting services and getting help.

This OLA is reviewed annually, or as otherwise needed. It remains valid until revised or terminated. Any changes to the OLA will be reflected here and announced through OIT’s virtual server users mailing list.

Service Description

2.1 Service Scope

Technologies supporting virtual servers (guests) include physical server compute and memory resources on a server cluster and virtual server operating system disk space on redundant storage infrastructure. The Virtual Server Hosting platform resides in the OIT Data Center. Included in this service are the provisioning of a new virtual server, operational support, consultation on sizing and appropriate use, redundant network connectivity. Optional services include: systems administration of the hosted virtual server, network firewalls and scanning, backups, and off-site copying of virtual server data.

2.2 Equipment and Software

The service is hosted on an HPE server cluster; each server is configured with 10g or 25g Ethernet network controllers, and the maximum possible RAM. Storage is provisioned via OIT's enterprise storage from Tintri using IP-based NAS. In addition to the redundant and high availability features in the hardware components, the VMWare virtual environment allows for dynamic movement of virtual servers between hosts, as well as High Availability (automatic restart) for virtual servers. The service uses VMWare's vSphere product to administer the

virtual server environment. vSphere allows users to manage their virtual servers via a web browser-based client or Windows-based desktop client.

2.3 OIT Data Center

The equipment is located the OIT Data Center, utilizing the same infrastructure as OIT's other enterprise services: earthquake protection tables; large-scale uninterrupted power supply (UPS); data center chilled water cooling; on-site emergency cooling; generator-backup power. Physical security includes door locks, video surveillance, and security alarms that trigger UCI Police response [Additional information on Data Backups](#) can be found on the OIT website.

2.4 Operational Support

OIT provides assistance and consulting to the virtual machine owners. This includes recommendations for virtual machine sizing and configuration, use of OIT tools for virtual server monitoring and performance management, and cloning and modifying existing virtual servers.

2.5 Optional: Systems Administration

The owner of the virtual machine is responsible for identifying a capable system administrator for their virtual machine. OIT will provide the initial setup of the virtual server but will not provide on-going system administration unless specifically contracted to do so. [Information for OIT contracted system administration](#) is available on the OIT website.

2.6 Optional: Network Firewalls and Scanning

The owner of the virtual machine is responsible for the security of their virtual server. OIT provides additional services to assist owners with maintaining the integrity of their servers.

- Information about Network Firewalls
- Information about Security Scanning

2.7 Optional: OIT Data Backup and Recovery Service

The owner of the virtual machine is responsible for protecting the data on their virtual machine against unintentional loss. OIT provides fee-based services for Data Backup and Recovery. Information about OIT's Data Backup and Recover Service is available on the OIT website.

2.8 Optional: Off-site Copy of Virtual Server Data

OIT has the ability to replicate data in the virtual server environment to off-site storage maintained and controlled by OIT. Please contact OIT via the Help Desk to discuss this option in more detail.

Roles and Responsibilities

3.1 Service Recipient Responsibilities and Requirements

Virtual servers offer campus subscribers tremendous flexibility to address UCI's computing needs and have become a critical resource for the UCI community. Virtual servers themselves are fairly well contained and limit the impact that one virtual server can have on another. However, owners of the virtual servers are given certain privileges in the virtual server environment to facilitate the management of their server; if misused, these privileges can negatively impact the running of the overall virtual server environment decreasing the value of the service for all users. To reduce risks to the virtual server environment, owners are required to abide by the following policies (refer to Appendix A for explanations):

- vSphere snapshots will not be kept longer than 2 days.
- vSphere snapshots will only be used when critical changes are being made to the guest; only 2 snapshots are permitted per virtual server at any given time.
- vSphere snapshots will be deleted outside of normal business hours which are 8am to 5pm weekdays.
- Guest file systems will be aligned to the underlying storage device.
- Balance monitoring tools will be enabled for all virtual systems.
- Owners will maintain the Annotations/Notes field for each virtual server.
- Owners will use the Critical/Production/Development folders to organize their virtual servers.
- VMware Tools will be installed on all virtual servers.
- Owners will assign a capable system administrator to each virtual machine they own.
- Owners will comply with all campus and UC security policies.
- Disk defragmentation tools should not be run on virtual servers.

The guest OS System Administrator is the primary troubleshooter for any issues within the guest virtual machine. The guest OS System Administrator will escalate an issue to OIT for additional support if the issue is possibly related to physical hardware resources. At least one representative for the virtual server owner should be subscribed to the OIT virtual server user mailing list.

3.2 Service Provider Responsibilities and Requirements

OIT's responsibilities and requirements in support of this Agreement include:

- Maintenance of the physical hardware of the Virtual Server Hosting service including server and storage administration.
- Maintenance of the software environment of the Virtual Service Hosting service including applying patches and upgrades for the virtual environment.
- Consistent resource monitoring and subsequent tuning and advisement as it pertains to virtual guest performance.
- Provisioning assistance in regards to access and integration into the campus network topology.
- Identification of performance bottlenecks on the hypervisor and storage layers.
- Architecture of the hardware and software resources of the virtual environment infrastructure.
- Ensuring compliance to campus and UC policy and associated security requirements for the virtual environment infrastructure.
- Performing system tuning as needed to the physical server and storage environment.
- Managing permissions and security groups that control access to the virtual server environment.
- Coordinating with vendors for any licensing, maintenance and support requests related to the virtual environment infrastructure.
- Capacity planning for physical resources (physical servers, disk storage).

OIT has the right to halt any guest system to protect the integrity of the campus computing environment. This includes systems that are being poorly managed, have been compromised, are negatively impacting the service environment, or do not fulfill the Service Recipient Responsibilities. OIT will notify the registered Service Recipient in advance unless urgent action is required. If and when resource contention occurs, due to a server host failure or resource over-allocation, systems in the Critical folder will have priority in resource allocation over systems in the Production folder, which will have priority over systems in the Development folder. The Virtual Server Hosting service has been designed to avoid resource contention; however, the potential resource contention exists. OIT will subscribe the initial virtual server requester to the OIT virtual server user mailing list which will be used to convey information relevant to the Virtual Server Hosting service.

3.3 Parties

OIT Help Desk, oit@uci.edu, (949) 824-2222 Fields all support requests, creates trouble tickets, and engages OIT staff to resolve. Data Center Infrastructure (DCI) staff members Kazuto Okayasu and Mitchell Stratford are OIT's primary supporters of the Virtual Hosting Service.

They are responsible for overall management and monitoring of the service including the underlying servers and storage. Ken Cooper is the Document owner.

Service Management

4.1 Service Uptime

The Virtual Server Hosting service is designed for 24/7 uptime with service maintenance windows as defined in this agreement.

4.2 Hours of Support

OIT provides 24x7 support and monitoring of the overall service environment. Support for individual virtual machines is normally provided during normal business hours of 8am to 5pm on weekdays (excluding University designated holidays). Support outside of these hours is provided on an emergency basis or if scheduled in advance with DCI staff.

4.3 Service Requests

New Virtual Server Hosting requests are submitted via the [Server Design Request Form](#) (UCInetID login required). All other support requests must be initiated by contacting the OIT Help Desk via phone or e-mail. The OIT Help Desk will create a support ticket for tracking purposes and contact OIT support staff as needed.

4.3.1 Normal Incident Handling

Requests for new Virtual Servers will be completed within 5 to 7 business days, if all information is accurately provided. If the request cannot be completed within this timeframe, the requestor will be contacted via phone or e-mail with an explanation for the delay. Please note that registering hosts via DNS is a separate service with a different response time. Non-urgent support requests will receive a response by the next business day.

4.3.2 Major Incident Handling

Urgent support problems will be responded to within 2 hours during business hours and within 4 hours outside of business hours. OIT will determine the urgency of each request using the following criteria:

- Significant number of people affected.

- Academic and Administrative deadlines.
- Significant impact on the delivery of instruction.
- Significant or lasting impact on student academic performance.
- Significant risk to law, rule, or policy compliance.
- Significant harm or financial loss to the university.

Urgent requests must be submitted by phone to the OIT Help Desk.

4.4 Service Management

OIT will use the OIT Change Notification and oit-changes mailing list to announce all significant changes to the Virtual Server Hosting service. The OIT virtual server user mailing list will be used to keep virtual server owners informed of information relevant to them. All changes will be announced in advance. Changes that cause a service interruption will be scheduled at least 7 days in advance. Changes that are not expected to cause a service interruption may be announced the day of the change. Exceptions may occur in response to emergencies.

4.5 Charges

Customers will be billed monthly via campus recharge unless other arrangements are made at the time of the service request. [See pricing for Virtual Server Hosting.](#)

OLA Review & Update

Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The document owner is responsible for facilitating regular reviews of this document. The document owner will incorporate all subsequent revisions and obtain mutual agreements and approvals as required. Review Date: March 2022.

Appendix A - Explanations for Customer Responsibilities

vSphere Snapshots will not be kept longer than 2 days.

vSphere snapshots represent a significant commitment of resources to create and delete; to limit the performance impact on the virtual server environment, snapshots will not be kept more than 2 days. Owners are responsible for policing any snapshots they create. OIT may delete any older snapshot without notice to the owner. When creating a snapshot, the owner should put date information (either creation date or expiration date) in the name or

description. OIT should be notified in advance if any snapshot must be kept more than 2 days via a service request. In addition, the snapshot description should contain information about how long it is being retained.

vSphere snapshots will only be used when critical changes are being made to the guest OS.

Use of snapshots is restricted to situations when a critical change is being made within the guest OS that cannot be easily reversed by traditional means, e.g. when applying large, complex patches or performing extensive application upgrades. Snapshots should not be used in lieu of traditional backups or to preserve a virtual server against external events.

vSphere snapshots will be deleted outside of normal business hours.

When a snapshot is created, the VMWare environment freezes all changes to the virtual server. It does not create a copy of the virtual server (creating a copy is referred to as cloning); it continues to use the frozen copy as a base to track all block changes that would have been written to the file system. Each and every change is saved until the snapshot is deleted; this is similar in concept to a database transaction log. The longer a snapshot is kept, the more data is saved and more disk resources are consumed. When a snapshot is deleted, the VMWare environment then applies all of the saved changes chronologically to the frozen snapshot consolidating all the past activity into the VMDK. This is very IO intensive and should be done after 5pm or before 8am any day.

Guest file systems will be aligned to the underlying storage device.

Guest file systems hosted on the NetApp storage device must be aligned to the underlying NetApp file system. If they are not aligned, this decreases IO performance for the entire virtual server environment since each data request from the storage to the guest OS is twice the size it would be compared to a guest file system that was properly aligned. Since the NetApp uses a Write Anywhere File Layout (WAFL), data is not laid out sequentially; grabbing two blocks of data instead of one also increase the disk seek time. Thinking of this as reading two randomly placed data blocks on a disk instead of reading one randomly placed data block. A guest OS installed by OIT has already been aligned. If a virtual server owner chooses to perform a bare-metal installation or chooses to reinstall the OS that OIT has provided, the owner assumes responsibility for aligning the guest file system to the underlying storage. Owners who install the OS on their virtual server should contact OIT via a service request for assistance with guest file system alignment.

Balance monitoring tools will be enabled for all virtual systems.

OIT uses a tool that provides end-to-end monitoring from the underlying NetApp storage through the vSphere infrastructure to the guest OS; this tool can also monitor some applications running within the guest OS. The software tool is currently called OnCommand

Balance. OIT requires each virtual server owner to allow Balance access to monitor activity. Guests monitored by Balance are automatically checked for the alignment issue highlighted above. A guest OS cannot be used in the OIT Virtual Server Hosting environment if it is not supported by the monitoring tools.

Owners will maintain the Annotations/Notes field for each virtual server.

Each guest has an annotation/notes field located on the summary page via the vSphere client. These notes are a critical resource for OIT staff. Each guest should include information on who to contact when there is an issue. Other recommended information would include any special instructions on what the service does and how OIT should treat the server if problems occur.

Owners will use the Critical/Production/Development folders to organize their virtual servers.

Owners will categorize their virtual servers using the Critical/Production/Development folder structure OIT has created. This structure is used by OIT to set server restart priority during any service maintenance. Virtual servers in the Critical folder will be started first by OIT, followed by virtual servers in the Production folder. Virtual servers in the Development folder will be left for the owners to manually power on after the service has returned to normal operation. This folder structure quickly communicates to OIT staff how important a specific virtual server may be to its owner and should be maintained in conjunction with the annotation/notes field.

VMware Tools will be installed on all virtual servers.

Every guest will have VMware Tools installed. OIT provides the virtual server to the owner with these tools already installed. These tools allow the guest to run more efficiently and allow OIT to initiate a clean shutdown of the guest OS if necessary. Without VMware Tools installed OIT can only remove power from the virtual server if a server restart is needed; removing power in this manner could result in corruption of the guest OS. VMware Tools are updated by the vendor. Virtual server owners should maintain the most current version for their servers. A guest OS cannot be used in the OIT Virtual Server Hosting environment if it is not supported by the VMWare Tools.

Owners will assign a capable system administrator to each virtual machine they own. Poorly managed servers put all other servers in the environment at risk, including all servers and desktops on the UCI network. OIT provides many options to assist owners with maintaining and patching servers, including the contracting of system administration. OIT should be notified if any virtual server cannot be kept patched and updated so that appropriate safeguards can be established.

Owners will comply with all campus and UC security policies.

OIT requires that the security of every computing system or device connected to the network be established and maintained in order to protect the campus network. Owners are responsible for knowing and complying with appropriate policies.

Disk defragmentation tools will not be run on virtual servers.

Users will not run defragmentation tools and will not check virtual disks for fragmentation. Fragmentation is not an issue at the guest level in a vSphere environment. Checking for fragmentation is waste of resources and will also "poison the cache" causing slow performance by filling the cache with read-once data blocks. De-fragmenting is worse in that moving blocks around impacts performance and is seen as changed blocks by the underlying storage layer; changed blocks get retained in snapshots reducing the overall storage capacity.