TOSM VM Shared Server Management

Memorandum of Understanding

DOCUMENT REVISION HISTORY:
6/12/2015 – Replaced Red Hat Linux with Oracle Linux
6/17/2015 – Item 3.8, added “per server” for clarification
1/20/2016 – Added 4.6.1 regarding Bradford network registration requirements for the Customer
7/13/2018 – Added 2.1.10 Datacenter Firewall, updated 3.12 to reflect current email lists, removed outdated info from 5.4/5.5
9/16/2021 – Updated On-call link. Added section 4.9 for disaster recovery options for VMs

---

The department of Technology Operations and Systems Management (TOSM) provides its customers with various IT-related services, including Shared Server Management. This document describes the Shared Server Management service that is available to Texas Tech University (TTU) and Texas Tech University System (TTUS) departments and colleges and serves as a Memorandum of Understanding (MOU) for this service between TOSM and its Customers.

1.0 Overview

This MOU is between TOSM, who is the service provider, and the Customers of this service, the department and colleges of TTU and TTUS. This document outlines the details of the Shared Server Management service provided by TOSM as well as the roles, responsibilities and expectations of both parties while providing a framework for problem resolution and communication.

2.0 VM Shared Server Management service

2.1 Service Description – The TOSM VM Shared Server Management service provides TTU, TTUHSC and TTUS departments and colleges with the ability to lease VMs (virtual servers) that are located within the TOSM data centers but managed entirely by the Customer. Data center features provided to the customer include:

2.1.1 Raised floor space
2.1.2 Network/Internet connectivity
2.1.3 Redundant cooling
2.1.4 Redundant power with maintenance bypass
2.1.5 24x7 monitoring of infrastructure
2.1.6 Diesel Generator with automatic transfer switch that engages during primary power loss
2.1.7 Closed-circuit video surveillance
2.1.8 Biometric readers for data center entry for approved personnel
2.1.9 Network Intrusion Detection System (IDS) managed by TTU Telecommunications
2.1.10 Datacenter Firewall managed by TTU Telecommunications

3.0 TOSM Responsibilities

3.1 TOSM is responsible for the installation, configuration and continued support of all virtualization infrastructure and backup infrastructure necessary to support the leased VMs.

3.2 TOSM will perform the initial VM build and allocate resources according to the Customer's requirements. Supported operating systems include supported versions of Microsoft Windows and current versions of Oracle Linux or CentOS.

3.3 Ample, redundant power will be made available to meet system requirements

3.4 Ample cooling will be made available to maintain proper operating temperature and humidity

3.5 Network access will be provided in coordination with the appropriate network personnel.

3.6 24x7 physical access to the data center for essential personnel

3.7 TOSM will provide monitoring infrastructure for general system availability, but alerts and notifications will be directed to the Customer or their designee.

3.8 TOSM will provide a 1gb shared network connection per server.

3.9 TOSM will provide physical building security.

3.10 TOSM will provide all virtualization hardware and software.

3.11 TOSM will provide VM backups. Please see the VM Backup Services MOU for more information.

3.12 TOSM will be responsible for ensuring that operating system patches are applied in a reasonable amount of time, to be determined by our Server Security team. When possible, operating system patch maintenance will be communicated to the Customer 72-hours in advance via various email communications including distribution lists for IT Project Impacts and NSC Site Coordinators as well as TechAnnounce. The updates will be applied during one of the normal maintenance windows. The windows are Saturday evening from 6:00pm to Sunday 6:00am, and Sunday, 6:00pm to Monday, 12:00am.

3.13 TOSM will be responsible for firewall configurations and anti-virus installation updates to ensure system integrity.

3.14 TOSM is responsible for recommending and implementing resource allocation modifications to provide optimal system performance within the Customer's budget, including reducing allocated resources when they are clearly over-allocated.

4.0 Customer Responsibilities

4.1 Customers are responsible for compliance with all TTU Information Technology Security Policies. The TTU Information Technology Security Policies may be found by visiting http://www.depts.ttu.edu/infotech/security/.

4.2 Customers are responsible for providing TOSM with up-to-date contact information of persons responsible for the server(s), including name, email address and phone number. If contact information changes, the Customer is responsible for notifying TOSM of the change.

4.3 Customer is responsible for completing an MOU Assessment each fiscal year for servers covered under this MOU.

4.4 With the exception of supported Microsoft Windows Server operating systems or Oracle Linux, Customers are responsible for all other associated software licensing and software maintenance.

4.5 The Customer is responsible for application troubleshooting and will remain the primary contact for their end users for application-related issues.

4.6 Since both TOSM and the Customer share administrative access on the system, the Customer is ultimately responsible and accountable for the overall security and integrity of the system. Security issues not related to the operating system must be rectified by the Customer within a reasonable amount of time or the system will be removed from the network until the issues are resolved. If a security breach is suspected on a system the Customer is required, by campus policy, to immediately report the incident to their institution's Information Security Officer (ISO). As a courtesy, we'd also appreciate an email to TOSM at security.tosm@ttu.edu with the details of the incident to help us ensure the integrity of other systems within the data center.

4.6.1 In addition to general security responsibilities, the Customer is also responsible for completing the Bradford network registration process. All systems residing on TTUnet must be registered with the Bradford system in order to be compliant with TTUnet security policies.

4.7 Customer must not disable or uninstall any application or process that has been installed by TOSM according to TOSM best practices. Please see Server Requirements for more information.

4.8 In the event of a disaster where the TOSM data center was rendered incapable of running production workloads, the TOSM VM Backup Service would provide the ability to recover the VM at the offsite facility. Recovery times would vary from a couple of days to potentially weeks.

4.9 Other disaster recovery may be available for an additional charge. If you'd like to discuss disaster recovery options for your VM, please contact us at serversupport.tosm@ttu.edu.

5.0 Server Requirements

5.1 Systems will be configured according to TOSM best practices.

5.2 System firewall must be enabled and configured per TOSM best practices.

5.3 System logs must be sent to the TOSM centralized logging destination.

5.4 All Microsoft Windows servers under this MOU must also comply with the following:

5.4.1 All systems must be configured as member servers on the ttu.edu Active Directory domain and the computer accounts must reside in the TOSM Active Directory Organizational Unit (OU).

5.4.2 System must have anti-virus installed and must be managed by the TOSM anti-virus server.

5.4.3 System will have the Microsoft security updates applied by TOSM during the normal TOSM maintenance windows.

5.4.4 System changes affecting or potentially affecting the operating system configuration and/or underlying hardware configuration must be communicated to TOSM as soon as possible.

5.5 All Oracle Linux systems under this MOU must also comply with the following:

5.5.1 All systems must have a computer account in TOSM Active Directory domain, residing in the TOSM Active Directory Organization Unit (OU).

5.5.2 System must have file integrity checker installed (Aide) as per TOSM best practices.

5.5.3 Systems will have the Oracle Linux security updates applied by TOSM during the normal TOSM maintenance windows.

5.5.4 System changes affecting or potentially affecting the operating system configuration and/or underlying hardware configuration must be communicated to TOSM as soon as possible.

6.0 Problem reporting and issue resolution

6.1 TOSM will address all issues involving power, cooling, network access and virtualization infrastructure hardware and software. TOSM will also provide operating system support for systems under this agreement. The resolution of application issues not related to the items above will be the sole responsibility of the Customer.

6.2 Data center infrastructure, virtualization infrastructure or operating system issues identified by the Customer should be reported to TOSM as soon as they are identified via email addressed to serversupport.tosm@ttu.edu. Issues of an emergent nature where production systems critical to the University are not available should be reported using our on-call procedures. This information can be found at https://www.texastech.edu/offices/information-technology/tosm/contact/oncall.php or by visiting our website at http://www.tosm.ttu.edu and clicking on the Contact Us link. Other issues will be handled during business hours unless other arrangements have been previously coordinated with TOSM.

6.3 Issues identified by TOSM will be communicated to the Customer via email and/or phone.

6.4 Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the Customer is responsible for immediately notifying their institution’s Information Security Office (ISO) per the IT Security Policies of the institution. As a courtesy, we’d also appreciate an email to TOSM at security.tosm@ttu.edu with the details of the incident to help us ensure the integrity of other systems within the data center.

7.0 Costs for VM Shared Server Management services

7.1 All costs for services described in this agreement are included in the annual base VM fee unless otherwise specified.