MiServer and MiDatabase SLE

Service Definition

Service Description
MiServer and MiDatabase are private cloud service offerings that support the University of Michigan. This service allows units to configure CPU, Memory and storage to meet current requirements and grow as needed. Backup and disaster recovery requirements can also be configured as needed.

The MiServer services includes virtual servers with the option of fully Managed Operating System (MOS) Windows Server, RHEL Linux Server or a Core Server with no OS.

The MiDatabase service offers 2 configurations - MS SQL Server windows, MySQL on Linux, both in a shared and dedicated version. All databases run on the MiServer MOS offering. The MiDatabase service includes patching and tuning for database and OS software.

Intended Consumers
The service is available for all faculty and staff members at the Ann Arbor, Dearborn and Flint Campuses of University of Michigan.

Value Statement
The service will add value for customers by providing a flexible service that scales from a virtual infrastructure to a fully managed Operating System or Database. By providing different levels of services, customers can choose features that support their business needs and can potentially reduce their overall operational costs. Customers who are running systems on this service will find value in not having to buy and maintain physical servers, networking and security infrastructure, as well as data center. This also allows users to greatly reduce the time it takes to acquire, setup and begin using computing resources. MOS and MiDatabase services also reduce the operating expense of maintaining Operating Systems (OS) and Database Management Systems (DBMS)

Service Details

<table>
<thead>
<tr>
<th>Feature or Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiServer Service</td>
<td>1-18 CPU, 1-64GB RAM</td>
</tr>
<tr>
<td>Managed OS Service</td>
<td>Preconfigured Servers running the latest 2 versions of Microsoft Windows and Red Hat Enterprise Linux</td>
</tr>
</tbody>
</table>
Managed DB Service

| Preconfigured latest 2 versions of Microsoft SQL, Oracle or MySQL on Managed OS virtual machines |

MiServer Core Features:

- 24/7 Host System Monitoring
- High availability (Protection from host failure)
- Clustering (0 Downtime host maintenance)
- Web interface for managing all virtual servers
- Integrated firewall
- 10GB network capable VM’s
- HIPAA Compliance
- Business day or less to Provision
- Access to TSM backup infrastructure
- Hardware refresh

Managed Operating System (MOS) Added benefits:

- Managed Windows & Red Hat Enterprise Linux (latest two versions) operating systems
- Operating system Patch management
- Operating system Upgrades
- Managed Backup and Recovery
- Managed Antivirus Software (Windows)
- Operating system Monitoring
- HIPAA Compliance

Managed Database Added Benefits (built on MOS)

- MS SQL, MySQL, and Oracle (latest two versions)
- Option for dedicated or shared instance
- Built on, and including features of, MiServer w/Managed OS
- DBMS Patch management
- Database Backup and recovery management
- HIPAA Compliance

Service Expectations
Service Availability

Service Hours
The MiServer and MiDatabase will be available 24x7 with the exception of any unexpected outage or system maintenance.

Planned Maintenance
- Planned maintenance will be announced and communicated 30 days prior to any system outage and is anticipated to be used 2 to 3 times per year during the maintenance window described below.
- ITS will announce all disruptive system maintenance changes in advance through the ITS Service Status page at: http://status.its.umich.edu/.
- Unified maintenance window for MiServer/MiDB service occurs every Saturday 11:00 p.m. – Sunday 7:00 a.m.
- Regularly scheduled patching will not take place during Production Freeze unless there are critical security updates required.
- All changes that require downtime will be required to be scheduled during the unified maintenance window. All other changes will be scheduled and followed by the change management process. * Critical security exploit patches and failed patches can be completed at any time with appropriate emergency change management processes and appropriate communication prior to completion.

Emergency Maintenance
Emergency maintenance is any maintenance that needs to be implemented immediately to prevent a services outage. ITS will use the standard communication plan prior to any emergency maintenance to alert impacted customers. The communication plan will include system notifications and updates to system status Web pages. Customer who are part of miserver.notify@umich.edu and midatabase.notify@umich.edu will receive notification of emergency maintenance.

Service Support

Requesting Support
User requests for support regarding ITS services are processed through the ITS Service Center. To contact the Service Center:
- Submit a Service Request Online (login required)
- Call 734-764-HELP (734-764-4357)
- Email 4HELP@umich.edu

Support Hours
ITS Service Center Hours are:
Monday–Thursday: 7 a.m.–7 p.m.
Friday: 7 a.m.–6 p.m.
Sunday: 2 p.m.–7 p.m.

ITS Operations: 24/7
During non-business hours Call 734-764-HELP (734-764-4357) you will be prompted to speak to operations who will page technical staff.

Incidents and Outages
[Specify the targets for restoration of service, and identify types of incidents and outages that would fit the different priority levels. Refer to the Service Restoration Definitions for priority, impact, and urgency definitions. Edit only the last column and indicate any specific need to deviate from the standard response time expectations for this service. ]

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
<th>Target to Restore Services</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Incidents are classified as critical priority when there is a major, immediate risk to the university's ability to conduct its mission, because of disruption to users’ ability to perform a function related to that mission.</td>
<td>4 hours</td>
<td>Any disruption to shared components impacting multiple vServers. This includes but is not limited to Physical Servers, Network or Storage.</td>
</tr>
<tr>
<td>High</td>
<td>Incidents are classified as high priority when there is an elevated risk to the university's ability to conduct its mission, because of disruption to users’ ability to perform a function related to that mission.</td>
<td>1 day</td>
<td>Any disruption to a supporting Service of the Core Infrastructure, MOS or MiDB limiting ITS’s or the customers ability to manage or maintain the health of the systems or meet the SLE or restoration of an individuals vServer meeting criteria in the description column</td>
</tr>
<tr>
<td>Medium</td>
<td>Incidents are classified as medium priority when users’ ability to perform a function is impaired, and a risk to the university's</td>
<td>5 days</td>
<td>Any disruption to a vServer when ability to perform a function is impaired, and a risk to the university's ability to</td>
</tr>
</tbody>
</table>
ability to conduct its mission is present, but the university can manage around that risk over a short period of time.

| Low     | Incidents are classified as low priority when users’ ability to perform a function is impaired, but there is minimal risk to the university’s ability to perform its mission. | 10 days | Information requests. |

**Disaster Recovery and Backup & Restoration**

A disaster is declared when a catastrophic event occurs that prevents use of a data center and/or a significant portion of its computing equipment. A data center disaster is not declared for issues with individual virtual servers.

Two key metrics are used to measure the response to a disaster:

**Recovery Time Objective (RTO)**

The amount of time that elapses from the point of the disaster until the service is restored at an agreed upon level. For example, if an a RTO is 72 hours, all systems would back online within 3 days. The true recovery time would depend on the extent of the disaster.

**Recovery Point Objective (RPO)**

Defines the maximum tolerable period in which data might be lost due to a major incident (measured in time). For example, if a RPO is 1 hour, the maximum amount of data loss would be no more than 1 hour.

The two options are Async and No Sync. When you select Async, all data on your server is replicated to a secondary data center every hour. With No Sync, your server is not replicated to a secondary data center. Replication is critical when there is a datacenter loss.

In addition to the recovery objectives, customers should design and architect their applications properly for their individual availability needs. ITS staff are available to consult on architecture.

<table>
<thead>
<tr>
<th>Replication Type</th>
<th>Recovery Time Objective</th>
<th>Recovery Point Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Async</td>
<td>8 hours</td>
<td>1 Hour</td>
</tr>
</tbody>
</table>
MiDatabase – Recovery Options
Units that purchase a Shared MiDatabase will have Async as their recovery option as they are in a shared instance with other customers. For Units that purchase a Dedicated Instance they can choose between Async or No Sync. The configuration option selected will determine what replication can be used, and therefore what RPO and RTO are available for the system. The two configuration options are:

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Replication Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
<td>Async</td>
</tr>
<tr>
<td>Dedicated</td>
<td>Async or No Sync</td>
</tr>
</tbody>
</table>

ROLES AND RESPONSIBILITIES

Role Definitions:

Customer - Department/Unit personnel within University of Michigan requesting and managing MiServer and/or MiDatabase services. Customers are responsible for anything not listed below in the different service tiers (Core, Managed OS, Managed DB). This also includes non server/service administration included but not limited to:

- Manage authorization and data access on servers and within databases.
- Pay all charges associated with services rendered and adhering to all funding restrictions for the source of funds used to pay for this service. Update shortcode with ITS if it changes.
- Adhere to data management, security, and compliance policies to comply with university policies, state and federal laws and regulations.

ITS Service Desk - (4-HELP) Central access point for customers to ask a question, log incidents and initiate service requests. The ITS Service Desk provides entry level support for service, and triages requests to the appropriate support group in ITS. All requests are recorded in the Service Link tool. Customers can check the status in the tool.

ITS Support responsibilities for a Core Virtual Server:
- Maintain all hardware and software lifecycle used to support the environment
- Provision servers or databases to specifications ordered in the ITS services portal
- Modify server specifications as requested by customers (additional RAM, CPU, disk space)
- Notify customers of patching and maintenance in advance.
- Maintain and accurately perform chargeback and rate management
Additional ITS Support for Managed OS and Managed DB:
- Regular patching of Operating System and Database Software to stay at current vendor supported levels.
- Set up monitoring and alerting for key performance metrics
- Respond to service requests and incidents created by customers
- Perform server/database restoration and recovery actions as requested by customer.
- Address customer requests to meet SLE requirements during regular support hours. Emergency changes and high priority incidents will be addressed after hours.

Service Performance

Service Metrics & Reporting

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Expectation</th>
<th>How Measured</th>
<th>How Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability</td>
<td>Report on availability, which includes availability, recoverability and any metrics that pertains to this agreement around availability as developed by the Service Manager.</td>
<td>Overall Availability: 99.7%</td>
<td>SUM (period of time where any or all of MiServer/MiDatabases are inaccessible due to ITS run infrastructure)</td>
<td>Monthly report provided to service customers via email Not yet available</td>
</tr>
<tr>
<td>Service Responsiveness</td>
<td>TBD</td>
<td>TBD</td>
<td></td>
<td>Not yet available</td>
</tr>
<tr>
<td>Request Fulfillment</td>
<td>Provisioning time for the service takes 1 Business Days for MOS and 2 Business Days for MiDB</td>
<td></td>
<td>Number of request fulfillment incidents that exceed 1 business day for MOS and 2 business days for MiDB</td>
<td>Service Link Report...Not Yet available</td>
</tr>
<tr>
<td>Incident Resolution</td>
<td>Metric describing if ITS is meeting Service incident response time as</td>
<td></td>
<td>Metric describing if ITS is meeting Service incident response time as defined in this doc under</td>
<td>Not yet available</td>
</tr>
</tbody>
</table>
Responses to Missed Service Expectations

Missed Service Level Expectations will be reviewed by the MiServer/MiDatabase leadership team. Root cause analysis will be done. Applicable corrective action will be taken. The Service Manager will follow up with Impacted customer(s).

Document Review & Approval

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Reviewed by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft (Created by Service Owner)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QA Review</td>
<td>Lynne Ertel</td>
<td>6/28/13</td>
</tr>
<tr>
<td>SPO Review</td>
<td>Bill Wrobleksi</td>
<td>6/28/13</td>
</tr>
<tr>
<td>Update</td>
<td>Keila Walton</td>
<td>4/29/15</td>
</tr>
<tr>
<td>Service Owner Approval</td>
<td>Chris Wood</td>
<td>5/19/15</td>
</tr>
</tbody>
</table>