ITS Strategic Roadmap – FY20 Planning

Server Support

Author: *Donald Enfinger*
Date last updated: *December 27, 2018*

Background

Software applications and systems are at the core of the business that runs Metropolitan Government departments and agencies. These programs run on a combination of physical servers, Metro private cloud and public/commercial cloud technology. On-premise systems are primarily hosted within Metro's Primary Data Center. Certain ITS-managed physical servers and related equipment are housed remotely at Metro owned facilities for backup purposes and for when otherwise required.

ITS has established a baseline of Microsoft Windows Server and Red Hat Linux Operating Systems as the primary standard to run servers supporting applications in use across Metro departments and agencies. Due to specialized application requirements, we also support a wide variety of UNIX operating systems on virtual appliances.

Our hardware platforms include rack servers configured with SSD drives and spinning disks; as well as Dell and Cisco chassis with blade server technology using dual 16 core processors and multiple 32 GB memory chips. This platform houses our private cloud services we provide for Metro Departments. We also run multiple other hardware platforms to provide the most value and efficiency for the services we provide.

ITS also supports the Health department for IBM AS/400 technology. This is a requirement to utilize State of Tennessee Health Department computing services.

ITS services are provided for most general government departments with the exception of Metro Nashville Police Department, Davidson County Sheriff's Office, Justice Integration Systems and Metro Nashville Public Schools. These agencies maintain separate and distinct server management for their departments.

Current Strategic Drivers

1. **Industry Direction: Cloud Computing** (Game-changing) – The widespread public acceptance of cloud for services that employees and citizens use every day, along with the potential for positive financial impact and effective cloud vendor security stances make cloud infrastructure services appealing.
2. **Customer Demand: High Availability** (High) – Customers and the citizens they serve demand extremely high availability of data center services to meet their business-critical needs, and for some departmental customers, life-safety responsibilities they hold.
3. **Demand for Secure Government systems** (High) – With massive data breaches in the news on a regular basis, we must strive at all times to protect the security, availability and integrity of all systems and services entrusted to our management.

4. **End of Life Cycle: Server Hardware and Operating Systems** (High) – As the server hardware platforms and operating systems reach their end of life/end of support, they need to be updated or replaced to ensure availability.
5. **End of Life Cycle: Applications** (High) – As with hardware, software systems have a lifecycle, often dictated through end of vendor support or require security enhancements. Certain customers continue to use out of date applications that are not compatible with current technology requirements. If unaddressed, this puts their applications at high risk for outages and puts Metro at higher risk for security breaches.

On the Horizon Strategic Drivers

1. **Additional Data Center(s)** (High) – Planning on the new Data Center 2 and associated space constraints would suggest that additional Data Center type facilities may be needed to house specialty services, such as the Department of Emergency Communications, should a new facility be built in the future.
2. **EOL Departmental Systems** (Medium) – As departmental systems reach end of life, the availability of viable secure cloud-based alternatives could impact our support model and staffing needs.
3. **Technology End of Life Support: Server Operating System** (High) – Windows 2008 R2, EOL January 2020 is end of life in January 2020and Windows Windows 2012, EOL October 2023, Operating systems, become end of life in 2023.

Short Term Goals (0-6 months) 7/1/19 – 12/31/19

#	Goal/Objective	Est. Start	Est. Duration
1	Replace current EOL hardware for servers supported by ITS. Requires capital funding.	07/2019	6 months
2	Plan to implement enhanced automation for vulnerability testing and remediation by using upgraded systems from Security and tracking remediation progress through monthly reporting. Present plan to ELT for review.	07/2019	6 months
3	Semiannual reviews of Server build processes and File Sharing procedures with our Security team to ensure best practices.	07/2019	1 month
4	Automate the Server inventory to be updated by SCCM. Requires consultant funding.	07/2019	6 months
5	Review Vendor technology roadmaps and approve next generation hardware models.	09/2019	3 months

Medium Term Goals (6-18 months) 1/1/20 – 12/31/20

#	Goal/Objective	Est. Start	Est. Duration
1	Continue to replace EOL hardware for servers supported by ITS per plan.	01/2020	ongoing
2	Work with customers to update EOL software in their environment	01/2020	ongoing
3	Implement Red Hat Satellite and Insight to manage the Linux environment	01/2020	3 months

Long Term Goals (18-36 months) 1/1/21 – 06/30/22

#	Goal/Objective	Est. Start	Est. Duration
1	The AS400 was upgraded to State of TN standards in 2018. The state is looking for a total system replacement and when the technology is chosen, we will develop a plan to migrate to it. Capital funding required.	01/2021	12 months
2	Rebuild servers to current supportable Operating System – Capital funding required	01/2021	ongoing

Related Roadmaps

- Data Center and Environmental
- Server Infrastructure
- Office 365