Case Study #2

Optimizing Operating Systems for a University Computer Lab

Jiading Zhou

CSYE 6230 – Operating System

College of Engineering, Northeastern University

February 18, 2025

Introduction:

In this advanced case, you will play the role of the Chief Information Officer (CIO) of a prestigious university responsible for managing the university's entire IT infrastructure, including the computer lab. The computer lab houses not only desktop computers but also server infrastructure for student projects and research. Over the past few months, issues have arisen that are affecting not only lab users but also the university's research initiatives and academic programs. Your task is to make strategic decisions regarding the operating system(s) used throughout the university.

Scenario:

The current situation is complex. The lab uses Windows 7, the university's research servers run on Linux, and there is a growing demand for cloud-based services. You must decide whether to standardize the OS environment, and if so, which OS to choose. You also need to consider how these choices will impact a diverse array of users, including students, faculty, and researchers.

Questions:

Why is it essential to consider standardizing the operating systems across the university's infrastructure, including the computer lab, research servers, and potential cloud services? What are the benefits and challenges of standardization?

Standardizing operating systems across the university's infrastructure is essential for several reasons. First, a uniform OS environment reduces complexity in management, maintenance, and support, allowing IT staff to streamline updates, troubleshoot issues quickly, and maintain security more effectively. A consistent platform across desktop computers, research servers, and cloud services means that patches and security protocols can be applied uniformly, reducing vulnerabilities and ensuring that users—whether students, faculty, or researchers—benefit from reliable and secure computing environments. Additionally, standardization can lead to cost savings through economies of scale, as purchasing, licensing, and support can be consolidated, and training needs for users and IT personnel are simplified. This uniformity also facilitates integration and interoperability among different parts of the university's infrastructure, easing the transition to or integration with cloud-based services.

However, standardization also presents several challenges. One major concern is the potential loss of flexibility—different user groups may have specialized requirements that a single OS may not fully address. For example, research servers might require a more customizable environment than a typical lab desktop and forcing a one-size-fits-all approach might hinder innovation or the performance of specific applications. Furthermore, the migration process itself can be complex and costly, especially when legacy systems are involved, and there may be resistance from users accustomed to a different operating system. Balancing the benefits of streamlined management and enhanced security with the need for flexibility to support diverse academic and research needs is therefore critical when considering standardization across the university's IT infrastructure.

Discuss the strategic advantages and disadvantages of upgrading to Windows 11 as the new OS for the university's computer lab and research servers. How might it impact user experience and research outcomes?

Upgrading the university's computer lab and research servers to Windows 11 could offer several strategic advantages. For instance, Windows 11 introduces a modernized, intuitive interface—with features such as a centered Start menu, Snap Layouts, and enhanced multitasking tools—that can streamline daily operations and boost productivity for both students and faculty. This improved user experience may reduce the time spent navigating the OS and allow researchers and lab users to focus more on their core tasks. In addition, Windows 11's robust security framework (including mandatory TPM 2.0, Windows Hello, and BitLocker) enhances data protection and could be especially beneficial for protecting sensitive research data and academic records. Its improved integration with cloud-based services and Microsoft 365 further supports hybrid work environments, enabling smoother collaboration across remote and on-campus settings.

However, the upgrade also presents some challenges. Windows 11 has more stringent hardware requirements compared to previous versions, which means many existing lab and server systems may require costly upgrades or replacements—especially if they lack TPM 2.0 or use older CPUs. Compatibility issues may arise too; some legacy software or specialized research applications might not run as smoothly on the new OS, potentially disrupting established workflows until adequate testing and updates are completed. Additionally, while the redesigned interface is a significant improvement for many users, there is an inherent learning curve that might temporarily affect productivity as users adapt to the new features. For research

servers, where stability and compatibility are paramount, the migration process could introduce risks that need careful planning and validation.

Overall, if the transition is well-managed—with sufficient hardware investment, thorough testing for compatibility with research applications, and effective change management strategies—the move to Windows 11 could lead to a more secure, efficient, and modern computing environment. This, in turn, may enhance research outcomes by reducing downtime and improving overall operational efficiency, while offering a better end-user experience in the computer lab.

What are the primary challenges in migrating from Windows 7 to Windows 11 in an environment with both desktop and server infrastructure?

Migrating from Windows 7 to Windows 11 in an environment that includes both desktop and server infrastructure poses several significant challenges. First, hardware compatibility is a major concern. Windows 11 enforces strict requirements—such as the need for TPM 2.0, UEFI firmware, and supported, modern CPUs—that many legacy Windows 7 machines may not meet. This often forces organizations to either upgrade or completely replace older devices, potentially driving up costs and extending downtime during the transition.

Another challenge is ensuring software and application compatibility. Many legacy applications and custom software solutions built for Windows 7 might not run properly—or at all—on Windows 11 without updates or reconfiguration. This is especially critical for server applications that support research and academic operations, where even minor disruptions can

lead to significant setbacks. Testing, patching, and, in some cases, redeveloping these applications becomes a complex and resource-intensive task.

Security and configuration differences further complicate the migration. Windows 11 is built with advanced security features such as Windows Hello, BitLocker, and virtualization-based security that differ fundamentally from the legacy security model of Windows 7. These changes require IT administrators to reconfigure security policies, update group policies, and possibly integrate new management tools (such as Microsoft Intune), ensuring that both desktops and servers are not only secure but also compliant with modern standards.

Additionally, the migration process itself—whether for desktops or servers—demands meticulous planning and robust change management strategies. Organizations must schedule upgrades in phases to minimize disruption, particularly in a research environment where downtime can hinder ongoing projects. Coordinating the transition across diverse user groups also means training staff to adapt to a completely redesigned user interface and new productivity features, which introduces a learning curve that can temporarily affect efficiency.

In summary, the primary challenges in migrating from Windows 7 to Windows 11 in such an environment include meeting the hardware prerequisites, ensuring compatibility of legacy applications, reconfiguring security and management settings, and managing the overall complexity of a phased, minimally disruptive migration. Addressing these challenges requires not only financial and technical investments but also a strong commitment to change management and user training to ensure that the new platform enhances rather than disrupts critical academic and research functions.

Explain the advantages and disadvantages of switching to Linux for the entire university's IT infrastructure. How might this choice impact software availability and development?

Switching the entire university's IT infrastructure to Linux brings a mix of significant advantages and notable disadvantages. On the plus side, Linux is open-source and generally available at low or no licensing cost, which can reduce overall IT expenditure—especially important in large-scale deployments across hundreds or thousands of devices. Its high degree of customizability allows IT teams to tailor the operating system to the university's specific academic, research, and administrative needs. Furthermore, Linux is renowned for its stability, robust security model, and flexibility in server environments, making it a popular choice for academic research servers and high-performance computing clusters. This flexibility also extends to development; many modern development tools and languages are natively supported on Linux, fostering an ecosystem conducive to innovation and collaborative, open-source projects.

On the other hand, there are critical challenges that must be considered. One major disadvantage is software availability—many specialized, commercial, or legacy applications used in academic settings have been designed for Windows or macOS, and their Linux counterparts may be limited or require workarounds such as compatibility layers (e.g., Wine) or virtual machines. This can hinder both day-to-day productivity and specialized research software development. Additionally, while Linux offers powerful customization options, its heterogeneous landscape (with multiple distributions and desktop environments) can lead to fragmentation, complicating support and maintenance in a standardized university environment. The migration also demands a steep learning curve for both IT staff and end users accustomed to Windows, potentially increasing training costs and causing temporary productivity drops. Lastly, integration with existing enterprise systems—such as Active Directory or proprietary academic platforms—

might require additional development efforts or middleware solutions, affecting both software development timelines and system interoperability.

In summary, while Linux could offer long-term cost savings, enhanced security, and a flexible, developer-friendly environment for academic research and server operations, the potential downsides in terms of software compatibility, user retraining, and integration complexity must be carefully weighed. The university would need to plan for a gradual transition, invest in retraining and support, and possibly develop or adopt alternative software solutions to ensure that academic and administrative functions are not disrupted.

What considerations should be made regarding cybersecurity, compliance, and data protection when selecting and implementing a new OS for the entire university?

When selecting and implementing a new OS across the university, cybersecurity, compliance, and data protection must be front and center. First, the OS should come with robust security features such as advanced encryption protocols, secure boot mechanisms, and integrated tools for multi-factor authentication and identity management. For example, modern operating systems like Windows 11 enforce TPM 2.0 and include native solutions like BitLocker, which are designed to protect sensitive data on both desktops and servers. This is critical when handling sensitive academic research and personal student data.

In addition, the chosen OS must comply with regulatory requirements relevant to the university's operations. For institutions in the United States, compliance with laws such as FERPA (Family Educational Rights and Privacy Act) is mandatory, while international institutions may need to consider GDPR or similar frameworks. It's essential to ensure that the

OS supports centralized management and audit capabilities so that security incidents can be quickly detected and reported, and that software updates and patches can be deployed rapidly to address emerging vulnerabilities.

Another key consideration is integration with existing security and data management infrastructure. The new OS should work seamlessly with current endpoint management systems (such as Microsoft Intune or other MDM solutions), SIEM platforms, and backup and disaster recovery processes. This ensures that the transition does not create new vulnerabilities or data silos. Pilot testing in a controlled environment is critical to assess any compatibility issues and to refine the deployment strategy, so that both IT staff and end users are prepared for the change.

Overall, the university should adopt a comprehensive strategy that encompasses not only the technical security features of the OS but also the policies and processes needed to support continuous compliance and data protection. This holistic approach will help ensure that the entire IT ecosystem remains secure, efficient, and resilient in the face of evolving cyber threats.

Reference

Anslinger, J. (2021, November 15). *Should you standardize your IT infrastructure?*. Lieberman Technologies. https://ltnow.com/blog/should-you-standardize-your-it-infrastructure/

Peter. (2024, October 21). *Bridging the gap: It standardization across facilities: Matrix-Ndi*. Matrix. https://www.matrix-ndi.com/resources/bridging-the-gap-it-standardization-across-facilities/

R/windows11 on reddit: Reasons to switch to Windows 11? also pros and cons. (n.d.). https://www.reddit.com/r/Windows11/comments/1cu9ilm/reasons_to_switch_to_windows_11_also_pros_and_cons/

Udt. (2024, June 26). *Why education needs to transition to Windows 11 now*. UDT. https://udtonline.com/why-learning-institutions-need-to-transition-to-windows-11-now/

Warren, T. (2024, December 4). *Microsoft closes the door on Windows 11 supporting older hardware*. The Verge. https://www.theverge.com/2024/12/4/24312928/microsoft-windows-11-older-hardware-tpm-support

Windows 11 upgrade: U-M LSA LSA Technology Services. LSA. (2024). https://lsa.umich.edu/technology-services/services/computer-desktop-support/desktop-support/windows-11-upgrade.html