

Title: High Availability of Virtualized Desktop Applications

We propose a system that builds on an existing data protection and recovery system and exploits existing high availability cluster technology to provide a more reliable and attack-resistant desktop experience. We will provide redundancy and fail-over on a single desktop computer via software, where most application faults occur. Our system is designed to work with or without the hardware redundancy. To provide hardware redundancy and fail-over, the application would need to have its necessary data stored on multiple systems. With hardware redundancy, application data is served in a model similar to the Application Service Provider (ASP) model, in which the application data is served over the network. Without hardware redundancy (only software redundancy), virtual machines are used as the ASPs to provide application data over the virtual network. Our system, by providing application fail-over and attack resistance on the desktop, is an improvement over both existing ASP models, that would not be usable if an external network connection is temporarily unavailable, and existing desktop security mechanisms such as the rapid recovery system, that do not make use of hardware redundancy. The main prototype of the system will be developed in Xen, but some aspects of the architecture will be evaluated with other virtualization technologies, such as OpenVZ. The prototype will also use the network storage software distribution Openfiler as its backend virtual file server.

Storing a user's personal data in a private file server virtual machine and carefully separating applications into their own virtual machines to provide data protection and recovery from attacks has been shown to have a sufficiently low overhead in terms of CPU and IO operations. For years, high availability cluster technology has been successfully deployed on servers to increase system reliability and uptime. As virtualization hardware support has begun to co-evolve with existing virtual machine monitor technologies, such as Xen, performance and support for unmodified guest operating systems continues to greatly improve. The protection, recovery, and cluster techniques we apply will still work with supported paravirtualized guest operating systems. Our system design will utilize a contract system and policy manager to carefully restrict access to both system and user data, while providing adequate redundancy to ensure that applications can maintain a high degree of availability and uptime even under attack.