**הקדמה**

הופעתם של התקני אחסון מהירים גרמו לכך שצוואר הבקבוק בגישה למידע השמור מוזז משכבות החמרה לשכבות התכנה. בסביבות וירטואליות, שבהן גם רץ המנהל של המחשב המארח -\L{hypervisor} , וגם מכונה וירטואלית, שינוי זה מורגש אף יותר. על מנת למזער את התקורה של התכנה בזמן הגישה להתקן האחסון, ניתן לאפשר למכונה וירטואלית לגשת ישירות להתקן ללא התערבות ה - \L{hypervisor} ובכך להאיץ את זמן הגישה הכולל להתקן. אולם, גישה ישירה ללא התערבות ה - \L{hypervisor} מבטלת את מנגנוני ההגנה וההפרדה שמסופקים על ידי המערכת קבצים משום שלהתקן אין מושג של משתמשים - \L{clients}.

The emergence of high-speed, multi GB/s storage devices has shifted the performance bottleneck of storage virtualization to the software layers of the hypervisor. The hypervisor overheads can be avoided by allowing the virtual machine (VM) to directly access the storage device (a method known as direct device assignment), but this method voids all protection guarantees provided by filesystem permissions, since the device has no notion of client isolation.

Recently, following the introduction of 10Gbs and higher networking interfaces, the PCIe specification was extended to include the Single Root IO Virtualization (SR-IOV) specification for self-virtualizing devices, which allows a single physical device to present multiple virtual interfaces on the PCIe interconnect. Using SR-IOV, a hypervisor can directly assign a virtual PCIe device interface to each of its VMs. However, as networking interfaces simply multiplex packets sent from/to different clients, the specification does not dictate the semantics of a virtual storage device and how to maintain data isolation in a self virtualizing device.

**רקע ומוטיבציה**

**ארכיטקטורת המערכת**

**תוצאות**

**סיכום המחקר**