



HVM Devices

Overview



- qemu-dm status
- V2E (Dan Stekloff)
- qemu in stub domains (Jun Nakajima/Dan Stekloff)
- Save/Restore (Jun Nakajima)
- Hypercalls & PV drivers (Keir Fraser)

qemu maintenance



- Based on qemu 0.8.2 (latest release)
- Using a quilt patchset (47 patches)
 - qemu -> qemu-dm
 - bugfixes (64bit)
 - optimizations (vram, hd multithread)
 - acpi support
 - vnc support fixes/improvements
 - xenstore configuration (devices, vnc port)
 - xen platform device

qemu -> qemu-dm



- disable cpu emulator
- map domain memory instead of allocating memory
- reset/shutdown cause domain restart/destroy
- disable devices emulated within xen (i8254, apic)
- disable qemu bios

VNC support



- Integrated in qemu – not using libvncserver anymore
- Entirely client driven – no overhead when no client connected
- Bind to next available port and export port number to xend through xenstore

Configuration from XenStore



- Block devices are configured through XenStore
- Support changing the images used for CD-ROM devices on-the-fly
- TODO: Network device configuration through XenStore

Known Issues



- Limited to about 2.5G of guest memory
- Huge overhead when scanning for screen updates
- Round-trip between domain and qemu in dom0 is expensive
- No authentication for VNC connections