MVM/DOS personality

This is an infrastructure for running VM's with unmodified OS's

MVM server

The MVM server is a central server of the MVM personality – the infrastructure for running multiple virtual machines on top of L4 microkernel. It is almost separate from OS/2 personality, but can be controlled by OS/2 programs via DosOpenVDD/DosCloseVDD/DosRequestVDD API's.

So, the MVM server exposes some interfaces to other OS personalities to be controlled by them. Also, it starts VM's, which are executed in the context of a VM monitor, running a guest OS (DOS, for example). The VM environment is defined by the VDD's ¹⁾ loaded. The MVM server loads VDD's, which are a kind of plugins. Also, it exports some helper API's for VDD's via MVDM.DLL.

Virtual Device Drivers (VDD's)

A VDD is like a plugin for MVM Server, and it can communicate with outside programs via request API (DosRequestVDD for OS/2 programs). On the other side, from the VM point of view, the VDD emulates some BIOS services/Option ROM's, a hardware devices of guest platform. It installs interrupt handlers, catches I/O ports or MMIO registers accesses from inside the guest OS. A VDD implements its services based on VDD helpers API, served by the MVM server.

Originally, the MV(D)M were used to emulate a 8086 machine with BIOS and DOS/Win 3.1. But now it is a trend for many OS'es to have the kernel virtual machines, like kvm in Linux or VirtualPC in WinNT. Our MVM personality is our solution of the same kind, but it not so monolithic like qemu/kvm – it decomposed to several parts, in best IBM solutions design traditions. The VDD's are like plugins for MVM server, allowing to extend the MVM environment. They're loadable modules (DLL's).

Also, as we're told previously, to share the screen with OS/2 apps and apps of other personalities, IBM created the solution of "Seamless WinOS/2". This is the possibility for Win 3.1 programs to share the same screen with OS/2 PM ones.

This is done with a special VDD's, like VVIDEO (VVGA, VSVGA, etc) implementiing a video mode support in a DOS window (or fullscreen). The DOS window is implemented as a special DLL (pmvdmp.dll) which was loaded by PM. It communicates with a VM via DosRequestVDD and implement the video functions via GPI calls (for windowed mode, so it is a PM application, based on VIO Shield (pmviop.dll), working via BVH drivers, like bvhwndw.dll for windowed OS/2 and DOS sessions, or bvhvga.dll+bvhsvga for fullscreen OS/2 or DOS sessions).

For windowed WinOS/2 sessions, it existed the solution of using a so-called PM shield (seamless.dll) and WinOS/2 shield (winsheld.exe). The 1st one is an "avatar" of Windows application in OS/2 PM world. And vice versa, the WinOS/2 shield is a representative of a PM app in WinOS/2 world.

Also, the second solution exists, based on GRADD video driver model. It works via VVMI (vmanwin.sys in the Intel OS/2). It is the VDD related to the communication of windows video driver (ifgdi2vm.drv for fullscreen, isgdi2vm.drv for seamless mode) with GRADD's VMAN². The special thread in VMAN polls the VVMI driver to communicate with Windows driver. So, the Windows driver is a generic one,

but it communicates with a "real" driver. This results in WinOS/2 and OS/2 PM shared the same screen using access to a common video driver. See the GRADD-related section for more details about multiple graphics engines sharing the same screen/video driver.

Virtual Machine Monitor

The VMM ³⁾ is a program implementing the environment of guest hardware platform, with help of VDD's. It maintains the contexts of all VM's, and handles the traps redirecting them to the needed VDD, loads the IST ⁴⁾ for different processor instruction sets, utilizes the hardware emulation features of the CPU, like VM86, AMD SVM, Intel VT-x etc.

It maintains the address space layout of a VM application, loads a firmware (for BIOS, the SeaBIOS can be used) and DOS emulation kernel.

The DOS emulation kernel (doskrnl)

The DOS emulation kernel is a special rehosted DOS kernel working via OS/2 (or PN ⁵) services. For example, file system API's of int 21h are implemented via OS/2 (or PN) file API's. Access to OS/2 API's done via SVC API (supervisor call?) which is trap of HLT instruction followed by call number and inverted call number. Also DOSKRNL provides MVM specific API for DOS applications.

Instruction Set Translator (IST)

The IST is a DLL, emulating the instructions of Guest hardware via Host CPU instructions. It exports a set of entry points, each corresponding the emulated instruction.

The similar component exist in QEMU – but it is linked statically with the emulator binary.

VM86 on Intel, and Hardware-assisted virtualization

Some processors implement special compatibility modes (VM86 allows creation of special task in protected mode, which emulates a virtual i8086 processor) or special instruction to assist the Virtual Machine Monitors creation. (Like "hypercall" to change context to a hypervisor, to execute its service and exit "hypervisor" mode). Also, the very new processors implement the IOMMU (a hardware support for sharing a hardware).

These extensions can be used to run unmodified OS'es on top of a hypervisor (it is supported in newer versions of Xen, VBox, VMWare, VPC).

Microkernels as Hypervisors

Microkernels and Hypervisors are very similar things. Microkernels implement similar features. For example, the Fiasco.OC microkernel supports SVM and VT-x and allows to run unmodified Linux in very thin VM's. This feature can be utilized in our MVM personality too.

SVC API

Superviser calls API aimed to call host services from VM.

0Image: constraint of the section of the	Ordinal	Description
1 Image: Additional and a section of the parent process from AX 3 Image: Additional and a section of the parent process from AX 3 Reset disk buffers 5 Image: Additional and the parent process from AX 4 Reset disk buffers 5 Image: Additional and the parent process from AX 6 Image: Additional and the parent process from AX 7 Set DTA from DS:DX 8 Image: Additional and the parent process from AX 9 Image: Additional and the parent process from AX 9 Image: Additional and the parent process from AX 9 Image: Additional and the parent process from AX 9 Image: Additional and the parent process from AX 9 Image: Additional and the parent process from AX 10 Image: Additional and the parent process from AX 11 Image: Additional and the parent process from AX 12 Image: Additional and the parent process from AX 13 Image: Additional and the parent process from AX 14 Image: Additional and the parent process from Additional and		
2 Terminate MVM and return code to parent process from AX 3 Reset disk buffers 5 6 7 Set DTA from DS:DX 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 216 227 238 240 251 262 273 284 295 206		
3Reset disk buffers567Set DTA from DS:DX89101111121314151617181920212223242526272829Delete file using FCB DS:DX → unopened FCB ES → environment segment31333435363738393939		Terminate MVM and return code to parent process from AX
4Reset disk buffers567Set DTA from DS:DX8991011111213141516171819101112131415161718192021222324252627282929210311312313314315316317318319319320331332333334335336337338339340341342343344344345346 <td< td=""><td></td><td></td></td<>		
5Image: Image: Ima		Reset disk buffers
6Set DTA from DS:DX8999109101011101210131014101510161017101810191020102110221023102410251026102710281029Delete file using FCB DS:DX → unopened FCB ES → environment segment30103110321033103410351036103710381039103910	L	
7 Set DTA from DS:DX 8		
8		Set DTA from DS:DX
9		
10 Interpretation 11 Interpretation 12 Interpretation 13 Interpretation 14 Interpretation 15 Interpretation 16 Interpretation 17 Interpretation 18 Interpretation 19 Interpretation 20 Interpretation 21 Interpretation 22 Interpretation 23 Interpretation 24 Interpretation 25 Interpretation 26 Interpretation 27 Interpretation 28 Interpretation 29 Delete file using FCB DS:DX → unopened FCB ES → environment segment 30 Interpretation 31 Interpretation 32 Interpretation 33 Interpretation 34 Interpretation 35 Interpretation 36 Interpretation 37 Interpretation 38 Interpretation 39 <td< td=""><td></td><td></td></td<>		
11 Image: state st		
12 Image:		
13 Image: I		
14 Image: style sty		
15 Image: I		
16		
17 Image: style sty		
18 Image: Second S		
19		
20		
21 1 22 1 23 1 24 1 25 1 26 1 27 1 28 1 29 Delete file using FCB DS:DX → unopened FCB ES → environment segment 30 1 31 1 32 1 33 1 34 1 35 1 36 1 37 1 38 1 39 1		
22		
232324242525262727282829Delete file using FCB DS:DX \rightarrow unopened FCB ES \rightarrow environment segment303131323334343536373839		
242526272829Delete file using FCB DS:DX → unopened FCB ES → environment segment30313233343536373839		
25		
26		
2727282829Delete file using FCB DS:DX → unopened FCB ES → environment segment3031313232333333435353637383939		
282829Delete file using FCB DS:DX → unopened FCB ES → environment segment301311321331341351361371381391		
29Delete file using FCB DS:DX → unopened FCB ES → environment segment301311321331341351361371381391		
30		Delete file using FCB DS:DX \rightarrow unopened FCB ES \rightarrow environment segment
31		
32 33 34 35 36 37 38 39		
33 33 34 35 35 36 36 37 38 39		
34		
35		
36		
37 38 39		
38 39		
39		
	40	

mvm

3/5

Ordinal	Description
41	•
42	
43	
44	Set VERIFY flag from AL
45	
46	
47	
48	
49	
49 50	
50	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	

1)

Virtual Device Drivers ²⁾ Video Manager ³⁾ Virtual Machine Monitor ⁴⁾ Instruction Set Translator ⁵⁾ Personality Neutral

From: http://www.osfree.org/doku/ - **osFree wiki**

Permanent link: http://www.osfree.org/doku/doku.php?id=en:docs:general:mvm&rev=170092011

Last update: 2023/11/25 13:48



5/5