**Virtual Machine Control Structure**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| GUEST STATE AREA | | | | | | | | | | | | | | | |
| CR0 | CR3 | | | | | | | | | | CR4 | | | | |
| DR7 | | | | | | | | | | | | | | | |
| RSP | RIP | | | | | | | | | | RFLAGS | | | | |
| CS | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| SS | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| DS | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| ES | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| FS | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| GS | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| LDTR | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| TR | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| GDTR | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| IDTR | Selector | | | | | Base Address | | | | Segment Limit | | | | Access Right | |
| IA32\_DEBUGCTL | | IA32\_SYSENTER\_CS | | | | | IA32\_SYSENTER\_ESP | | | | | | IA32\_SYSENTER\_EIP | | |
| IA32\_PERF\_GLOBAL\_CTRL | | IA32\_PAT | | | | | IA32\_EFER | | | | | | IA32\_BNDCFGS | | |
| SMBASE | | | | | | | | | | | | | | | |
| Activity state | Interruptibility state | | | | | | | | | | | | | | |
| Pending debug exceptions | | | | | | | | | | | | | | | |
| VMCS link pointer | | | | | | | | | | | | | | | |
| VMX-preemption timer value | | | | | | | | | | | | | | | |
| Page-directory-pointer-table entries | | | | PDPTE0 | | | | | PDPTE1 | | | PDPTE2 | | | PDPTE3 |
| Guest interrupt status | | | | | | | | | | | | | | | |
| PML index | | | | | | | | | | | | | | | |
| HOST STATE AREA | | | | | | | | | | | | | | | |
| CR0 | | | CR3 | | | | | | | | CR4 | | | | |
| RSP | | | | | | | | RIP | | | | | | | |
| CS | Selector | | | | | | | | | | | | | | |
| SS | Selector | | | | | | | | | | | | | | |
| DS | Selector | | | | | | | | | | | | | | |
| ES | Selector | | | | | | | | | | | | | | |
| FS | Selector | | | | Base Address | | | | | | | | | | |
| GS | Selector | | | | Base Address | | | | | | | | | | |
| TR | Selector | | | | Base Address | | | | | | | | | | |
| GDTR | Base Address | | | | | | | | | | | | | | |
| IDTR | Base Address | | | | | | | | | | | | | | |
| IA32\_SYSENTER\_CS | | | IA32\_SYSENTER\_ESP | | | | | | | | IA32\_SYSENTER\_EIP | | | | |
| IA32\_PERF\_GLOBAL\_CTRL | | | IA32\_PAT | | | | | | | | IA32\_EFER | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CONTROL FIELDS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Pin-Based VM-Execution Controls | External-interrupt exiting | | | | | | | | | | | NMI exiting | | | | | | | | | | | Virtual NMIs | | | | | | | |
| Activate VMX-preemption timer | | | | | | | | | | | | | | | | Process posted interrupts | | | | | | | | | | | | | |
| Primary processor-based  VM-execution controls | Interrupt-window exiting | | | | | | | | | | | | | | | | Use TSC offsetting | | | | | | | | | | | | | |
| HLT exiting | | | | | | | INVLPG exiting | | | | | | | | | MWAIT exiting | | | | | | | | | | | RDPMC exiting | | |
| RDTSC exiting | | | | | | | CR3-load exiting | | | | | | | | | CR3-store exiting | | | | | | | | | | | CR8-load exiting | | |
| CR8-store exiting | | | | | | | Use TPR shadow | | | | | | | | | NMI-window exiting | | | | | | | | | | | MOV-DR exiting | | |
| Unconditional I/O exiting | | | | | | | Use I/O bitmaps | | | | | | | | | Monitor trap flag | | | | | | | | | | | Use MSR bitmaps | | |
| MONITOR exiting | | | | | | | | | | | PAUSE exiting | | | | | | | | | | | Activate secondary controls | | | | | | | |
| Secondary processor-based  VM-execution controls | Virtualize APIC accesses | | | | | | | Enable EPT | | | | | | | | | Descriptor-table exiting | | | | | | | | | | | Enable RDTSCP | | |
| Virtualize x2APIC mode | | | | | | | Enable VPID | | | | | | | | | WBINVD exiting | | | | | | | | | | | Unrestricted guest | | |
| APIC-register virtualization | | | | | | | | | | | Virtual-interrupt delivery | | | | | | | | | | | PAUSE-loop exiting | | | | | | | |
| RDRAND exiting | | | | | | | Enable INVPCID | | | | | | | | | Enable VM functions | | | | | | | | | | | VMCS shadowing | | |
| Enable ENCLS exiting | | | | | | | RDSEED exiting | | | | | | | | | Enable PML | | | | | | | | | | | EPT-violation #VE | | |
| Conceal VMX non-root operation from Intel PT | | | | | | | | | | | | | | | | Enable XSAVES/XRSTORS | | | | | | | | | | | | | |
| Mode-based execute control for EPT | | | | | | | | | | | | | | | | Use TSC scaling | | | | | | | | | | | | | |
| Exception Bitmap | | | | | | | I/O-Bitmap Addresses | | | | | | | | | | | | TSC-offset | | | | | | | | | | | |
| Guest/Host Masks for CR0 | | | | Guest/Host Masks for CR4 | | | | | | | | | Read Shadows for CR0 | | | | | | | | | | Read Shadows for CR4 | | | | | | | |
| CR3-target value 0 | | CR3-target value 1 | | | | | | | CR3-target value 2 | | | | | | | | CR3-target value 3 | | | | | | | | | CR3-target count | | | | |
| APIC Virtualization | | APIC-access address | | | | | | | | | | Virtual-APIC address | | | | | | | | | | | | | TPR threshold | | | | | |
| EOI-exit bitmap 0 | | | | | | | EOI-exit bitmap 1 | | | | | | | | EOI-exit bitmap 2 | | | | | | | | | EOI-exit bitmap 3 | | | | |
| Posted-interrupt notification vector | | | | | | | | | | | | | | | Posted-interrupt descriptor address | | | | | | | | | | | | | |
| Read bitmap for low MSRs | | | | Read bitmap for high MSRs | | | | | | | | | Write bitmap for low MSRs | | | | | | | | | | Write bitmap for low MSRs | | | | | | | |
| Executive-VMCS Pointer | | | | | | | Extended-Page-Table Pointer | | | | | | | | | | | | Virtual-Processor Identifier | | | | | | | | | | | |
| PLE\_Gap | | | PLE\_Window | | | | | | | VM-function controls | | | | | | | VMREAD bitmap | | | | | | | | | | VMWRITE bitmap | | | |
| ENCLS-exiting bitmap | | | | | | | | | | | | | | PML address | | | | | | | | | | | | | | | | |
| Virtualization-exception information address | | | | | | | EPTP index | | | | | | | | | | | | | | XSS-exiting bitmap | | | | | | | | | |
| VM-EXIT CONTROL FIELDS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| VM-Exit Controls | Save debug controls | | | | | | | | | | | Host address space size | | | | | | | | | | | Load IA32\_PERF\_GLOBAL\_CTRL | | | | | | | |
| Acknowledge interrupt on exit | | | | | | | | | | Save IA32\_PAT | | | | | Load IA32\_PAT | | | | | | Save IA32\_EFER | | | | | | | | Load IA32\_EFER |
| Save VMX preemption timer value | | | | | | | | | | | Clear IA32\_BNDCFGS | | | | | | | | | | | | Conceal VM exits from Intel PT | | | | | | |
| VM-Exit Controls for MSRs | VM-exit MSR-store count | | | | | | | VM-exit MSR-store address | | | | | | | | | | | | | | | | | | | | | | |
| VM-exit MSR-load count | | | | | | | VM-exit MSR-load address | | | | | | | | | | | | | | | | | | | | | | |
| VM-EXIT INFORMATION FIELDS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Basic VM-Exit Information | Exit reason | | | | | | | | | | | | | | | | | Exit qualification | | | | | | | | | | | | |
| Guest-linear address | | | | | | | | | | | | | | | | | Guest-physical address | | | | | | | | | | | | |
| VM Exits Due to Vectored Events | | | | | VM-exit interruption information | | | | | | | | | | | | | | | VM-exit interruption error code | | | | | | | | | | |
| VM Exits That Occur During Event Delivery | | | | | | IDT-vectoring information | | | | | | | | | | | | | | IDT-vectoring error code | | | | | | | | | | |
| VM Exits Due to Instruction Execution | | | | | | VM-exit instruction length | | | | | | | | | | | | | | VM-exit instruction information | | | | | | | | | | |
| I/O RCX | | | | | | | | | I/O RSI | | | | | I/O RDI | | | | | | | | | I/O RIP | |
| VM-instruction error field | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

* Natural-Width fields.
* 16-bits fields.
* 32-bits fields.
* 64-bits fields.

CopyLeft 2017, [@Noteworthy](https://twitter.com/LordNoteworthy) (Intel Manuel of July 2017)