TDX_FEATURES Enum. Bits	Class	Field	Description	Type	VM Applic.	Init Value	Field Size (Bytes)	Max Num Fields	Num Elem.	Elem. Size (Bytes)	Base FIELD_ID (Hex)	VMM Access Prod.	VMM Access Debug	Guest Access	VMM Wr Mask Prod.	VMM Wr Mask Debug	Guest Wr Mask
None	Management	VCPU_STATE	The activity state of the VCPU. The values below are provided only for debug, and are subject to change with new TDX module releases. 0x0: VCPU_UNINITIALIZED 0x2: VCPU_READY 0x4: VCPU_ACTIVE 0x8: VCPU_DISABLED 0x10: VCPU_IMPORT	VCPU_STATE		VCPU_READY_ASYNC	1	1	1	1	0xA020000000000000	None	RO	None	0	0	0
None	Management	LAST_TD_EXIT	Type of the last TD exit. The values below are subject to change with new TDX module releases. 0x0: ASYNC_FAULT 0x1: ASYNC_TRAP 0x2: TDVMCALL	LAST_TD_EXIT		ASYNC_FAULT	1	1	1	1	0xA02000000000000F	None	RO	None	0	0	0
Always	Management	VCPU_INDEX	Sequential index of the VCPU in the parent TD. VCPU_INDEX indicates the order of VCPU initialization (by TDH.VP.INIT), starting from 0, and is made available to the TD via TDINFO. VCPU_INDEX is in the range 0 to (TDCS.MAX_VCPUS - 1), up to 0xFFFE	32b Unsigned Integer		From TDCS.NUM_VCPUS, see description	4	1	1	4	0xA020000200000002	RO	RO	RO	0	0	0
Always	Management	NUM_TDVPS_PAGES	Number of pages in this TDVPS	Unsigned Integer		Depends on the number of pages added by TDH.VP.ADDCX	1	1	1	1	0xA020000000000003	RO	RO	None	0	0	0
Always	Management	TDVPS_PAGE_PA	An array of TDVPS_PAGES physical address pointers to the TDVPS physical pages. The actual number of entries is enumerated by NUM_TDVPS_PAGES.	Array of PA		N/A	8	24	1	8	0xA020000300000010	RO	RO	None	0	0	0
Always	Management	ASSOC_LPID	The unique, hardware-derived identifier of the logical processor on which this VCPU is currently associated (either by TDENTER or by other VCPU-specific SEAMCALL flow): • A value of -1 indicates that VCPU is not associated with any LP. • Initialized by TDH.VP.INIT to the LP_ID on which it ran.	Integer		LPID on which TDH.VP.INIT runs	4	1	1	4	0xA020000200000004	RO	RO	None	0	0	0
Always	Management	VCPU_EPOCH	The value of TDCS.TD_EPOCH at the time this VCPU entered TDX non-root mode	Integer		0	8	1	1	8	0xA020000300000006	RO	RO	None	0	0	0
Always	Management	CPUID_SUPERVISOR_VE	When set, the Intel TDX module injects #VE on guest TD execution of CPUID in CPL = 0.	Boolean		FALSE	1	1	1	1	0xA020000000000007	RO	RO	RW	0	0	-1
Always	Management	CPUID_USER_VE	When set, the Intel TDX module injects #VE on guest TD execution of CPUID in CPL > 0.	Boolean		FALSE	1	1	1	1	0xA020000000000008	RO	RO	RW	0	0	-1
None	Management	LAST_EXIT_TSC	Initialized to the value returned rdtsc on TDH.VP.INIT	Unsigned 64b Integer		rdtsc value at TDH.VP.INIT	8	1	1	8	0xA02000030000000A	None	RO	None	0	0	0
Always	Management	PEND_NMI	When set, the Intel TDX module injects an NMI to the guest TD at the next available opportunity (NMI window open after TDENTER). the Intel TDX module then clears PEND_NMI.	Boolean		FALSE	1	1	1	1	0x2020000000000000B	RW	RW	None	-1	-1	0
None	Management	NMI_UNBLOCKING_DUE_TO_IRET	Flags that on the last VM exit NMI unblocing due to IRET was indicated	Boolean		FALSE	1	1	1	1	0xA020000000000040	None	RO	None	0	0	0

None	Management	LAST_EPF_GPA_LIST_IDX	Number of valid entries in LAST_EPF_GPA_LIST	Unsigned Integer		0	1	1	1	1	0xA020000000000000D	None	RO	None	0	0	0
None	Management	POSSIBLY_EPF_STEPPING	Number of possibly legal EPT Faults (EPFs) detected so far at this TD vCPU instruction	Unsigned Integer		0	1	1	1	1	0xA020000000000000E	None	RO	None	0	0	0
None	Management	HP_LOCK_BUSY_START	TSC value at start of the host priority busy period	Unsigned 64b Integer		0	8	1	1	8	0xA020000300000030	None	RO	None	0	0	0
None	Management	HP_LOCK_BUSY	Indicates that the guest has encountered a busy host priority lock	Boolean		FALSE	1	1	1	1	0xA020000000000031	None	RO	None	0	0	0
None	Management	LAST_SEAMDB_INDEX	Value of PL.SEAMDB_INDEX, sampled on last VCPU-to-LP association	64-bit unsigned integer		Copied from PL.SEAMDB_INDEX	8	1	1	8	0xA020000300000032	None	RO	None	0	0	0
None	Management	CURR_VM	VM index currently used for this VCPU	16-bit unsigned integer		0	2	1	1	2	0xA020000100000041	None	RO	None	0	0	0
None	Management	L2_EXIT_HOST_ROUTING	Sticky status of L2-to-L1 routing by the host (TDH.VP.ENTER with RESUME_L1 set): 0: L2 TD exit not routed to L1 1: L2 async TD exit routed to L1 2: L2 sync (TDG.VP.VMCALL) TD exit routed to L1			0	1	1	1	1	0xA020000000000042	None	RO	None	0	0	0
None	Management	VM_LAUNCHED	A Boolean flag per VM, indicating whether the VM has been VMLAUNCH'ed on this LP since it has last been associated with this VCPU. If TRUE, VM entry should use VMRESUME. Else, VM entry should use VMLAUNCH.	Boolean	L1_AND_L2	FALSE	1	4	1	1	0xA020000000000044	None	RO	None	0	0	0
None	Management	LP_DEPENDENT_HPA_UPDATED	A Boolean flag per VM, indicating that the LP-dependent HPA fields have been updated. Cleared after new VCPU-to-LP association.	Boolean	L1_AND_L2	FALSE	1	4	1	1	0xA020000000000048	None	RO	None	0	0	0
None	Management	MODULE_DEPENDENT_FIELDS_UPDATED	A Boolean flag per VM, indicating that the TDX module dependent HPA fields have been updated. Cleared after new VCPU-to-LP association that follows a TD preserving update.	Boolean	L1_AND_L2	FALSE	1	4	1	1	0xA020000000000004C	None	RO	None	0	0	0
7	Management	L2_CTLS	L2 VM control flags, used by the L1 VMM: Bit 0: ENABLE_SHARED_EPTP Bit 1: ENABLE_TDVMCALL Bits 63:2: RESERVED, must be 0	64-bit bitmap	L2_ONLY	0	8	4	1	8	0xA020000300000050	None	RW	RW	0	0x0000000000000003	0x0000000000000003
None	Management	L2_DEBUG_CTLS	L2 VM debug control flags, used by the off-TD debugger: Bit 0: TD_EXIT_ON_L1_TO_L2 Bit 1: TD_EXIT_ON_L2_TO_L1 Bit 2: TD_EXIT_ON_L2_VM_EXIT Bits 63:3: RESERVED, must be 0	64-bit bitmap	L2_ONLY	0	8	4	1	8	0xA020000300000054	None	RW	None	0	0x0000000000000007	0
7	Management	TSC_DEADLINE	TSC deadline, in virtual TSC ticks A value of -1 indicates no TSC deadline Applicable only to L2 VMs	64-bit unsigned integer	L2_ONLY	-1	8	4	1	8	0xA020000300000058	None	RO	RW	0	0	-1
None	Management	SHADOW_TSC_DEADLINE	TSC deadline, in native TSC ticks Applicable only to L2 VMs	64-bit unsigned integer	L2_ONLY	0	8	4	1	8	0xA020000300000005C	None	RO	None	0	0	0

None	Management	BASE_L2_CR0_GUEST_HOST_MASK	The base guest/host mask used for any L2 CR0 access by the L1 VMM. Bits 5, 29 and 30 can't be written even in debug mode.	64-bit bitmap		The following bits are set to 1, indicating they are owned by the Intel TDX module: • NE (5) • NW (29) • CD (30) • Any bit set to 1 in IA32_VMX_CR0_FIXED0 (i.e., a bit whose value must be 1), except for PE (0) and PG(31) which are set to 0, since the guest TD runs as an unrestricted guest. • Any bit set	8	1	1	8	0xA020000300000080	None	RW	None	0	0xFFFFFFFF9FFFFFDF	0
None	Management	BASE_L2_CR0_READ_SHADOW	The base read shadow used for any L2 CR0 access by the L1 VMM. Bits 0 and 5 can't be written even in debug mode.	64-bit bitmap		The following bits are set to 1: • NE (5) • Any bit set to 1 in IA32_VMX_CR0_FIXED0 (i.e., a bit whose value must be 1), except for PE (0) and PG(31) which are set to 0, since the guest TD runs as an unrestricted guest. All other bits are cleared to 0.	8	1	1	8	0xA020000300000081	None	RW	None	0	0xFFFFFFFF9FFFFFDF	0

None	Management	BASE_L2_CR4_GUEST_HOST_MASK	The base guest/host mask used for any L2 CR4 access by the L1 VMM. Bits 6, 13 and 14 can't be written even in debug mode.	64-bit bitmap		• Bits MCE (6), VMXE (13) and SMXE (14) are set to 1, indicating they are owned by the Intel TDX module. • Bit PKE (22) is set to ~TDCS.XFAM[9] to intercept writes to CR4 If PK is not enabled. • If TDCS.XFAM[12:11] is 11, then bit CET (23) is cleared to 0. Otherwise (CET is not enabled), bit	8	1	1	8	0xA020000300000082	None	RW	None	0	0xFFFFFFFFFFFF9FBF	0
None	Management	BASE_L2_CR4_READ_SHADOW	The base read shadow used for any L2 CR4 access by the L1 VMM. Bit 6 can't be written even in debug mode.	64-bit bitmap		• Bit MCE (6) is set to 1. • Bit VMXE (13) is set to 1. • Any other bit whose value is set to 1 in IA32_VMX_CR4_FIXED0 (i.e., a bit whose value must be 1) is set to 1. • All other bits are cleared to 0.	8	1	1	8	0xA020000300000083	None	RW	None	0	0xFFFFFFFF9FFFFFDF	0
None	Management	SHADOW_CR0_GUEST_HOST_MASK	The L2 VMCS CR0 guest/host mask original value, as set by the L1 VMM. Applicable only to L2	64-bit bitmap	L2_ONLY	For L2: all-1	8	4	1	8	0xA020000300000084	None	RO	None	0	0	0
None	Management	SHADOW_CR0_READ_SHADOW	The L2 VMCS CR0 read shadow original value, as set by the L1 VMM Applicable only to L2	64-bit bitmap	L2_ONLY	For L2: all-0	8	4	1	8	0xA020000300000088	None	RO	None	0	0	0
None	Management	SHADOW_CR4_GUEST_HOST_MASK	The L2 VMCS CR4 guest/host mask original value, as set by the L1 VMM. Applicable only to L2	64-bit bitmap	L2_ONLY	For L2: all-1	8	4	1	8	0xA02000030000008C	None	RO	None	0	0	0
None	Management	SHADOW_CR4_READ_SHADOW	The L2 VMCS CR4 read shadow original value, as set by the L1 VMM. Applicable only to L2	64-bit bitmap	L2_ONLY	For L2: all-0	8	4	1	8	0xA020000300000090	None	RO	None	0	0	0
None	Management	SHADOW_INSTRUCTION_TIMEOUT_CONTROL	Shadow value of VMCS instruction timeout, in crystal clock ticks Applicable to all VMs	32-bit unsigned integer	L1_AND_L2	0	4	4	1	4	0xA020000200000094	None	RO	None	0	0	0
None	Management	SHADOW_PID_HPA	Shadow value of VMCS posted interrupt descriptor address Applicable only to L1	Shared HPA	L1_ONLY	NULL_PA (-1)	8	4	1	8	0xA020000300000098	None	RO	None	0	0	0

None	Management	SHADOW_PINBASED_EXEC_CTLS	Shadow value of VMCS pin-based execution controls Applicable only to L1	32-bit bitmap	L1_ONLY	Same as VMCS field	4	4	1	4	0xA02000020000009C	None	RO	None	0	0	0
None	Management	SHADOW_PLE_GAP	Shadow value of VMCS PLE_GAP, in virtual TSC ticks Applicable only to L2 VMs	32-bit unsigned integer	L2_ONLY	0	4	4	1	4	0xA0200002000000A4	None	RO	None	0	0	0
None	Management	SHADOW_PLE_WINDOW	Shadow value of VMCS PLE_WINDOW, in virtual TSC ticks Applicable only to L2 VMs	32-bit unsigned integer	L2_ONLY	0	4	4	1	4	0xA0200002000000A8	None	RO	None	0	0	0
None	Management	SHADOW_POSTED_INT_NOTIFICATION_VECTOR	Shadow value of VMCS posted interrupt notification vector Applicable only to L1	16-bit unsigned integer	L1_ONLY	0xFFFF	2	4	1	2	0xA0200001000000AC	None	RO	None	0	0	0
None	Management	SHADOW_PROCBASED_EXEC_CTLS2	Shadow value of VMCS secondary processor based execution controls Applicable to all VMs	32-bit bitmap	L1_AND_L2	Same as VMCS field	4	4	1	4	0xA0200002000000B0	None	RO	None	0	0	0
None	Management	SHADOW_SHARED_EPTP	Shadow value of VMCS shared EPTP Applicable to all VMs	HPA	L1_AND_L2	NULL_PA (-1)	8	4	1	8	0xA0200003000000B4	None	RO	None	0	0	0
None	Management	L2_ENTER_GUEST_STATE_GPA	GPA of TDG.VP.ENTER guest state output buffer Applicable only to L2 VMs	GPA	L2_ONLY	NULL_PA (-1)	8	4	1	8	0xA0200030000100	None	RO	None	0	0	0
None	Management	L2_ENTER_GUEST_STATE_HPA	HPA (incl. HKID) of TDG.VP.ENTER guest state output buffer Applicable only to L2 VMs	HPA	L2_ONLY	NULL_PA (-1)	8	4	1	8	0xA0200030000104	None	RO	None	0	0	0
None	Management	VE_INFO_GPA	Shadow GPA of the VE_INFO area Applicable only to L2 VMs	GPA	L2_ONLY	NULL_PA (-1)	8	4	1	8	0xA0200030000108	None	RO	None	0	0	0
None	Management	VE_INFO_HPA	Shadow HPA (incl. HKID) of the VE_INFO area Applicable only to L2 VMs	HPA	L2_ONLY	NULL_PA (-1)	8	4	1	8	0xA020000300000010C	None	RO	None	0	0	0
None	Management	L2_VAPIC_GPA	Shadow GPA of the L2 virtual APIC address (used by the L1 VMM) Applicable only to L2 VMs	GPA	L2_ONLY	NULL_PA (-1)	8	4	1	8	0xA0200030000110	None	RO	None	0	0	0
None	Management	L2_VAPIC_HPA	Shadow HPA (incl. HKID) of the L2 virtual APIC address Applicable only to L2 VMs	HPA	L2_ONLY	NULL_PA (-1)	8	4	1	8	0xA0200030000114	None	RO	None	0	0	0
None	EPT Violation Log	LAST_EPF_GPA_LIST	Array of GPAs that caused EPF so far at this TD vCPU instruction	GPA		N/A	8	None	1	8	0xA2200030000200	None	RO	None	0	0	0
Always	CPUID Control	CPUID_CONTROL	Bit 0: When set, the Intel TDX module injects #VE on guest TD execution of CPUID in CPL = 0. Bit 1: When set, the Intel TDX module injects #VE on guest TD execution of CPUID in CPL > 0. Other: Reserved, must be 0.	Array of 8-bit bitmaps		0	1	512	1	1	0xA1200000000000	None	RO	RW	0	0	0x03
None	VAPIC	VAPIC	Virtual APIC Page	Page		0	8	128	1	8	0x0120000300000000	None	RO	None	0	0	0
None	VE_INFO	EXIT_REASON				0	4	1	1	4	0x0220000200000000	None	RO	None	0	0	0
None	VE_INFO	VALID	0xFFFFFFFF: valid 0x00000000: not valid			0	4	1	1	4	0x0220000200000001	None	RO	None	0	0	0
None	VE_INFO	EXIT_QUALIFICATION				0	8	1	1	8	0x0220000300000002	None	RO	None	0	0	0
None	VE_INFO	GLA				0	8	1	1	8	0x0220000300000003	None	RO	None	0	0	0
None	VE_INFO	GPA				0	8	1	1	8	0x0220000300000004	None	RO	None	0	0	0
None	VE_INFO	EPTP_INDEX				0	2	1	1	2	0x0220000100000005	None	RO	None	0	0	0
None	VE_INFO	INSTRUCTION_LENGTH				0	4	1	1	4	0x8220000200000010	None	RO	None	0	0	0
None	VE_INFO	INSTRUCTION_INFORMATION				0	4	1	1	4	0x8220000200000011	None	RO	None	0	0	0
None	VE_INFO	VE_CATEGORY	Category of #VE exception, see [ABI Spec]			0	1	1	1	1	0x8220000000000013	None	RO	None	0	0	0
None	VE_INFO	EXTENDED_INSTRUCTION_INFORMATION				0	8	1	1	8	0x8220000300000012	None	RO	None	0	0	0
None	VE_INFO	INTERRUPTIBILITY_STATE	VMCS Interruptibility State at the time of #VE injection			0	4	1	1	4	0x8220000200000014	None	RO	None	0	0	0
None	Guest GPR State	RAX				0	8	1	1	8	0x1020000300000000	None	RW	None	0	-1	0
None	Guest GPR State	RCX	Init value is provided as an input to TDH.VP.INIT (same value as R8)			Provided as an input to TDH.VP.INIT (same value as R8)	8	1	1	8	0x1020000300000001	None	RW	None	0	-1	0

None	Guest GPR State	RDX	Init Value: • Bits [31:00]: Same as RESET value, matches CPUID.1:EAX. CPU version information includes Family, Model and Stepping • Bits [63:32]: Set to 0			Bits [31:00]: Same as RESET value, matches CPUID.1:EAX. CPU version information: Family, Model and Stepping Bits [63:32]: Set to 0	8	1	1	8	0x1020000300000002	None	RW	None	0	-1	0
None	Guest GPR State	RBX	Init Value: • Bits [05:00]: GPAW is the effective GPA width (in bits) for this TD (do not confuse with MAXPA); SHARED bit is at GPA bit GPAW-1; only GPAW values 48 and 52 are possible • Bits [63:06]: Reserved for future additional details, set to 0, must be ignored by vBIOS			Bits [05:00]: GPAW: the effective GPA width (in bits) for this TD (don't confuse with MAXPA). SHARED bit is at GPA bit GPAW-1. In TDX1, only GPAW values 48 and 52 are possible. Bits [63:06]: Reserved for future additional details, set to 0, must be ignored by vBIOS	8	1	1	8	0x1020000300000003	None	RW	None	0	-1	0
None	Guest GPR State	RBP	Init Value: • Bits [31:00]: Virtual CPU index, starting from 0 and allocated sequentially on each successful TDH.VP.INIT • Bits [63:32]: Set to 0			0	8	1	1	8	0x1020000300000005	None	RW	None	0	-1	0
None	Guest GPR State	RSI				Bits [31:00]: Virtual CPU index, starting from 0 and allocated sequentially on each successful TDH.VP.INIT Bits [63:32]: Set to 0	8	1	1	8	0x1020000300000006	None	RW	None	0	-1	0
None	Guest GPR State	RDI	Init value is provided as an input to TDH.VP.INIT (same value as RCX)			0	8	1	1	8	0x1020000300000007	None	RW	None	0	-1	0
None	Guest GPR State	R8				Provided as an input to TDH.VP.INIT (same value as RCX)	8	1	1	8	0x1020000300000008	None	RW	None	0	-1	0
None	Guest GPR State	R9				0	8	1	1	8	0x1020000300000009	None	RW	None	0	-1	0
None	Guest GPR State	R10				0	8	1	1	8	0x102000030000000A	None	RW	None	0	-1	0

None	Guest GPR State	R11				0	8	1	1	8	0x102000030000000B	None	RW	None	0	-1	0
None	Guest GPR State	R12				0	8	1	1	8	0x102000030000000C	None	RW	None	0	-1	0
None	Guest GPR State	R13				0	8	1	1	8	0x102000030000000D	None	RW	None	0	-1	0
None	Guest GPR State	R14				0	8	1	1	8	0x102000030000000E	None	RW	None	0	-1	0
None	Guest GPR State	R15				0	8	1	1	8	0x102000030000000F	None	RW	None	0	-1	0
None	Guest State	XCR0				1	8	1	1	8	0x1120000300000020	None	RO	None	0	0	0
Always	Guest State	VCPU_STATE_DETAILS	See [ABI Spec]			N/A	8	1	1	8	0x9120000300000100	RO	RO	RO	0	0	0
None	Guest MSR State	IA32_SPEC_CTRL				All-0, except bit 8 (DDPD_U) which is set to 1 if the CPU supports DDPD_U (h/w CPUID(7.2).EDX[3] == 1) but (virtual CPUID(7.2).EDX[3] == 0)	8	1	1	8	0x1320000300000048	None	RW	None	0	-1	0
None	Guest MSR State	IA32_UMWAIT_CONTROL				0	8	1	1	8	0x13200003000000E1	None	RW	None	0	-1	0
None	Guest MSR State	IA32_TSX_CTRL				0	8	1	1	8	0x1320000300000122	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PMC_GP_CFG_Ax				0	8	16	1	8	0x1320000300000186	None	RW	None	0	-1	0
None	Guest MSR State	MSR_OFFCORE_RSPx				0	8	2	1	8	0x13200003000001A6	None	RW	None	0	-1	0
None	Guest MSR State	IA32_XFD				0	8	1	1	8	0x13200003000001C4	None	RO	None	0	0	0
None	Guest MSR State	IA32_XFD_ERR				0	8	1	1	8	0x13200003000001C5	None	RO	None	0	0	0
None	Guest MSR State	IA32_PMC_FX_CTRx				0	8	16	1	8	0x1320000300000309	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PERF_METRICS				0	8	1	1	8	0x1320000300000329	None	RW	None	0	-1	0
None	Guest MSR State	IA32_FIXED_CTR_CTRL				0	8	1	1	8	0x132000030000038D	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PERF_GLOBAL_STATUS				0	8	1	1	8	0x132000030000038E	None	RO	None	0	0	0
None	Guest MSR State	IA32_PEBS_ENABLE				0	8	1	1	8	0x13200003000003F1	None	RW	None	0	-1	0
None	Guest MSR State	MSR_PEBS_DATA_CFG				0	8	1	1	8	0x13200003000003F2	None	RW	None	0	-1	0
None	Guest MSR State	MSR_PEBS_LD_LAT				0	8	1	1	8	0x13200003000003F6	None	RW	None	0	-1	0
None	Guest MSR State	MSR_PEBS_FRONTEND				0	8	1	1	8	0x13200003000003F7	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PMC_GP_CTRx				0	8	16	1	8	0x13200003000004C1	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PMC_FX_CFG_Bx				0	8	16	1	8	0x1320000300010200	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PMC_FX_CFG_Cx				0	8	16	1	8	0x1320000300010000	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PMC_GP_CFG_Bx				0	8	16	1	8	0x1320000300010300	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PMC_GP_CFG_Cx				0	8	16	1	8	0x1320000300010100	None	RW	None	0	-1	0
None	Guest MSR State	IA32_XSS				0	8	1	1	8	0x1320000300000DA0	None	RO	None	0	0	0

None	Guest MSR State	IA32_LBR_DEPTH				(n + 1) * 8, where n is the index of the highest bit set to 1 in CPUID(0x1C,0) .EAX[7:0]	8	1	1	8	0x13200003000014CF	None	RW	None	0	-1	0
None	Guest MSR State	IA32_UARCH_MISC_CTL				0	8	1	1	8	0x1320000300001B01	None	RW	None	0	-1	0
None	Guest MSR State	IA32_FRED_RSP0				0	8	1	1	8	0x13200003000001CC	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PL0_SSP	This field is only used if FRED is enabled and CET is disabled			0	8	1	1	8	0x13200003000006A4	None	RW	None	0	-1	0
None	Guest MSR State	IA32_USER_MSR_CTL				0	8	1	1	8	0x132000030000001C	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PEBS_BASE				0	8	1	1	8	0x13200003000003F4	None	RW	None	0	-1	0
None	Guest MSR State	IA32_PEBS_INDEX				0	8	1	1	8	0x13200003000003F5	None	RW	None	0	-1	0
None	Guest MSR State	IA32_MISC_ENABLE	Shadow of IA32_MISC_ENABLE. Value is never written to the h/w.			See the [ABI Spec]	8	1	1	8	0x13200003000001A0	None	RW	None	0	-1	0
None	Guest MSR State	MSR_SMI_COUNT	Shadow of MSR_SMI_COUNT. Value is never written to the h/w.			0	8	1	1	8	0x1320000300000034	None	RW	None	0	-1	0
None	Guest State	DR0				0	8	1	1	8	0x1120000300000000	None	RW	None	0	-1	0
None	Guest State	DR1				0	8	1	1	8	0x1120000300000001	None	RW	None	0	-1	0
None	Guest State	DR2				0	8	1	1	8	0x1120000300000002	None	RW	None	0	-1	0
None	Guest State	DR3				0	8	1	1	8	0x1120000300000003	None	RW	None	0	-1	0
None	Guest State	DR6				0xFFFF0FF0	8	1	1	8	0x1120000300000006	None	RW	None	0	0x00000000FFFFFFFF	0
None	Guest State	CR2				0	8	1	1	8	0x1120000300000028	None	RW	None	0	-1	0
None	Guest MSR State	IA32_DS_AREA				0	8	1	1	8	0x1320000300000600	None	RW	None	0	-1	0
None	Guest MSR State	IA32_STAR				0	8	1	1	8	0x1320000300002081	None	RO	None	0	0	0
None	Guest MSR State	IA32_LSTAR				0	8	1	1	8	0x1320000300002082	None	RO	None	0	0	0
None	Guest MSR State	IA32_KERNEL_GS_BASE				0	8	1	1	8	0x1320000300002102	None	RO	None	0	0	0
None	Guest MSR State	IA32_TSC_AUX				0	8	1	1	8	0x1320000300002103	None	RW	None	0	-1	0
None	Guest MSR State	IA32_FMASK				0x00020200	8	1	1	8	0x1320000300002084	None	RO	None	0	0	0
None	Guest Ext. State	XBUFF		XSAVES buffer		0	8	4096	1	8	0x1220000300000000	None	RW	None	0	-1	0
7	MSR Bitmaps[1]	L2_MSR_BITMAPS_1	MSR exit bitmaps page, controlling L2 VM RDMSR/WRMSR VM exit. On L1 write, original value is stored in the shadow bitmap; the MSR bitmap value is calculated as a bitwise or of the original value and TDCS.MSR_BITMAP value. On L1 read, value is returned from the shadow bitmap.	MSR Exit Bitmaps		All-1	8	512	1	8	0x2520000300000000	None	RW	RW	0	-1	-1
None	MSR Bitmaps Shadow[1]	L2_SHADOW_MSR_BITMAPS_1	Shadow MSR exit bitmaps page, defining the L2 VM policy for handling MSR access, set by the L1 VMM	MSR Exit Bitmaps		All-1	8	512	1	8	0xA620000300000000	None	RO	None	0	0	0
7	MSR Bitmaps[2]	L2_MSR_BITMAPS_2	MSR exit bitmaps page, controlling L2 VM RDMSR/WRMSR VM exit. On L1 write, original value is stored in the shadow bitmap; the MSR bitmap value is calculated as a bitwise or of the original value and TDCS.MSR_BITMAP value. On L1 read, value is returned from the shadow bitmap.	MSR Exit Bitmaps		All-1	8	512	1	8	0x2D20000300000000	None	RW	RW	0	-1	-1
None	MSR Bitmaps Shadow[2]	L2_SHADOW_MSR_BITMAPS_2	Shadow MSR exit bitmaps page, defining the L2 VM policy for handling MSR access, set by the L1 VMM	MSR Exit Bitmaps		All-1	8	512	1	8	0xAE20000300000000	None	RO	None	0	0	0

7	MSR Bitmaps[3]	L2_MSR_BITMAPS_3	MSR exit bitmaps page, controlling L2 VM RDMSR/WRMSR VM exit. On L1 write, original value is stored in the shadow bitmap; the MSR bitmap value is calculated as a bitwise or of the original value and TDCS.MSR_BITMAP value. On L1 read, value is returned from the shadow bitmap.	MSR Exit Bitmaps		All-1	8	512	1	8	0x3520000300000000	None	RW	RW	0	-1	-1
None	MSR Bitmaps Shadow[3]	L2_SHADOW_MSR_BITMAPS_3	Shadow MSR exit bitmaps page, defining the L2 VM policy for handling MSR access, set by the L1 VMM	MSR Exit Bitmaps		All-1	8	None	1	8	0xB620000300000000	None	RO	None	0	0	0