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	MigTD Access	VMM Wr Mask Prod.	VMM Wr Mask Debug	Guest Wr Mask	MigTD Wr Mask
Always	TD Management	FATAL	Indicates a fatal error, e.g., #MC during TD operation.	Boolean		FALSE	1	1	1	1	0x8010000000000001	RO	RO	None	None	0	0	0	0
Always	TD Management	NUM_TDCX	Number of TDCX pages that have been added by TDH.MNG.ADDCX	32b Unsigned Integer		0	4	1	1	4	0x8010000200000002	RO	RO	None	None	0	0	0	0
Always	TD Management	CHLDCNT	The number of 4KB child pages (including opaque control structure pages) associated with this TDR	64b Unsigned Integer		0	8	1	1	8	0x8010000300000004	RO	RO	None	None	0	0	0	0
Always	TD Management	LIFECYCLE_STATE	The life cycle state of this TD. LIFECYCLE_STATE values below are provided for debug only; they are subject to change in future TDX module versions: 0: TD_HKID_ASSIGNED 1: TD_KEYS_CONFIGURED 2: TD_BLOCKED 3: TD_TEARDOWN	LIFECYCLE_STATE		TD_HKID_ASSIGNED	4	1	1	4	0x8010000200000005	RO	RO	None	None	0	0	0	0
Always	TD Management	TDCX_PA	Physical addresses of the TDCX pages	Array of Physical Address		N/A	8	16	1	8	0x8010000300000010	RO	RO	None	None	0	0	0	0
0	TD Management	TD_UUID	Universally Unique Identifier of the TD	256-bit blob		Random	32	1	4	8	0x8010000300000020	RO	RO	RO	RO	0	0	0	0
Always	Key Management	HKID	Private HKID	16b Unsigned Integer		From TDH.MNG.CREATE input	2	1	1	2	0x8110000100000001	RO	RO	None	None	0	0	0	0
Always	Key Management	PKG_CONFIG_BITMAP	Bitmap that indicates on which package TDH.MNG.KEY.CONFIG was executed successfully using this private key entry	Bitmap		0	8	1	1	8	0x8110000300000002	RO	RO	None	None	0	0	0	0
1	TD Preserving	HANDOFF_VERSION	The handoff version to which this TD is committed	16b Unsigned Integer		MODULE_HV	2	1	1	2	0x8210000100000000	RO	RO	None	None	0	0	0	0
1	TD Preserving	SEAMDB_INDEX	The index of the SEAMDB entry that holds the TDX module's TCB at TD creation time.	64b Unsigned Integer		From SEAMDB_GETREF	8	1	1	8	0x8210000300000001	RO	RO	None	None	0	0	0	0
6	TDX_CONNECT_TDR	TDI_REF_CNT	Number of device interfaces attached to the TD (i.e. DEVIFCS owned by the TD). This TDR page can be reclaimed only if this counter is 0	64-bit unsigned integer		0	8	1	1	8	0x8310000300000001	RO	RO	None	None	0	0	0	0
Always	TD Management	NUM_VCPUS	The number of VCPU that have been successfully initialized (by TDH.VP.INIT) or imported (by TDH.IMPORT.STATE.VP)	32b Unsigned Integer		0	4	1	1	4	0x9010000200000001	RO	RO	RO	None	0	0	0	0
Always	TD Management	NUM_ASSOC_VCPUS	The number of VCPUS associated with LPs – i.e., the LPs might hold TLB translations and/or cached TD VMCS	32b Unsigned Integer		0	4	1	1	4	0x9010000200000002	RO	RO	None	None	0	0	0	0
Always	TD Management	OP_STATE	See the [ABI Spec]	OP_STATE		UNINITIALIZED	4	1	1	4	0x9010000200000004	RO	RO	None	None	0	0	0	0
Always	TD Management	NUM_L2_VMS	Number of L2 VMs	16b Unsigned Integer		0	2	1	1	2	0x9010000100000005	RO	RO	RO	RO	0	0	0	0
50	TD Management	ENABLED_QUOTE_IDS	Bitmap of attestation keys that have been enabled and available for obtaining a TDX Attestation Quote via TDG.VP.VMCALL(QUOTE) API	64-bit bitmap		Global.ENABLED_ATTESTATION_KEYIDS	8	None	1	8	0x9010000300000006	RO	RO	RO	None	0	0	0	0
50	TD Management	QUOTE_MAX_SIZE	Maximum size of the buffer that must be allocated to contain the TDX Quote received from TDX Module	32b Unsigned Integer		Global.QUOTE_MAX_SIZE	4	None	1	4	0x9010000200000008	RO	RO	RO	None	0	0	0	0
Always	Execution Controls	ATTRIBUTES	TD attributes	ATTRIBUTES		From TDH.MNG.INIT input	8	1	1	8	0x1110000300000000	RO	RO	RO	RO	0	0	0	0
Always	Execution Controls	XFAM	Extended Features Available Mask: indicates the extended user and system features which are available for the TD. Copied to each TDVPS on TDH.VP.INIT.	XCR0		From TDH.MNG.INIT input	8	1	1	8	0x1110000300000001	RO	RO	RO	RO	0	0	0	0
Always	Execution Controls	MAX_VCPUS	Maximum number of VCPUs	32b Unsigned Integer		From TDH.MNG.INIT input	4	1	1	4	0x1110000200000002	RO	RO	RO	None	0	0	0	0
Always	Execution Controls	GPAW	This bit has the same meaning as the VMCS GPAW execution control: 0: GPA.SHARED bit is GPA[47] 1: GPA.SHARED bit is GPA[51]	Boolean		From TDH.MNG.INIT input	1	1	1	1	0x1110000000000003	RO	RO	RO	RO	0	0	0	0

Always	Execution Controls	EPTP	TD-scope Secure EPT pointer: format is the same as the VMCS EPTP execution control; copied to each TD VMCS EPTP on TDH.VP.INIT	EPTP		From TDH.MNG.INIT input	8	1	1	8	0x1110000300000004	RO	RO	None	RO	0	0	0	0
Always	Execution Controls	TSC_OFFSET	TD-scope TSC offset execution control: copied to each TD VMCS TSC-offset execution control on TDH.VP.INIT	64b unsigned Integer		From TSC_FREQUENCY and rdtsc	8	1	1	8	0x111000030000000A	RO	RO	None	None	0	0	0	0
Always	Execution Controls	TSC_MULTIPLIER	TD-scope TSC multiplier execution control: copied to each TD VMCS TSC-multiplier execution control on TDH.VP.INIT	64b Unsigned Integer		From TSC_FREQUENCY	8	1	1	8	0x111000030000000B	RO	RO	None	None	0	0	0	0
Always	Execution Controls	TSC_FREQUENCY	Virtual TSC frequency – in units of 25MHz	16b Unsigned Integer		From TDH.MNG.INIT input	2	1	1	2	0x111000010000000C	RO	RO	RO	None	0	0	0	0
Always	Execution Controls	NUM_CPUID_VALUES	Number of valid fields in CPUID_VALUES	16b Unsigned Integer			2	1	1	2	0x911000010000000E	RO	RO	None	None	0	0	0	0
Always	Execution Controls	XBUFF_SIZE		Unsigned Integer		From CPUID and XFAM	4	1	1	4	0x911000020000000F	RO	RO	None	None	0	0	0	0
Always	Execution Controls	NOTIFY_ENABLES	Enable guest notification of events: Bit 0: Notify when Zero Step attack is suspected Bits 63:1: Reserved, must be 0	Bitmap		0	8	1	1	8	0x9110000300000010	None	RW	RW	None	0	0x0000000000000001	0x0000000000000001	0
Always	Execution Controls	HP_LOCK_TIMEOUT	Host priority timeout value, in usec (internally, stored in TSC tick units)	Unsigned 32b integer		1 sec	8	1	1	8	0x9110000300000011	RW	RW	None	None	-1	-1	0	0
7	Execution Controls	VM_CTLS	An array of 4 per-VM controls that may be modified by the host VMM during guest TD run time See the [ABI Spec] for details.	Array of 64-bit bitmaps	L1_AND_L2	0	8	4	1	8	0x9110000300000012	RW	RW	None	None	0x000000000000000F	0x000000000000000F	0	0
Always	Execution Controls	CONFIG_FLAGS	Non-attested TD configuration flags	64b bitmap		From TDH.MNG.INIT input	8	1	1	8	0x9110000300000016	RO	RO	RO	RO	0	0	0	0
16	Execution Controls	TD_CTLS	A bitmap of TD controls that may be modified by the guest TD during its run time See [ABI Spec] for details	64b bitmap	L1_ONLY	From TDH.MNG.INIT input	8	1	1	8	0x9110000300000017	None	RO	RW	None	0	0	0x8000000000000001F	0
27	Execution Controls	VIRT_MAXPA	Virtual MAXPA A value of 0 is special; it indicates a virtual MAXPA of 52	Unsigned 8-bit integer		Calculated based CPUID(0x80000008).EAX[7:0] configuration	1	1	1	1	0x9110000000000018	RO	RO	None	None	0	0	0	0
20	Execution Controls	TOPOLOGY_ENUM_CONFIGURED	Indicates whether virtual topology enumeration has been successfully configured	Boolean		True, may be cleared during VCPU initializations	1	1	1	1	0x9110000000000019	RO	RO	RO	RO	0	0	0	0
30	Execution Controls	VE_REDUCTION_VALID	Indicates whether #VE reduction has been successfully configured	Boolean		True, may be cleared during VCPU initializations	1	1	1	1	0x911000000000001A	RO	RO	RO	RO	0	0	0	0
None	Execution Controls	CPUID_VALID	Non-architectural - an array of boolean flag, indicating the validity of CPUID_VALUES. Indexed by the internal CPUID lookup table indexing.	Array of boolean		Set to 1 when setting or importing a CPUID_VALUE entry.	1	512	1	1	0x9110000000000080	None	RO	None	None	0	0	0	0
Always	Execution Controls	XBUFF_OFFSETS	XSAVE buffer components offsets – calculated by TDH.MNG.INIT based on XFAM	Unsigned Integer		From CPUID and XFAM	4	32	1	4	0x9110000200000800	RO	RO	None	None	0	0	0	0
22	Execution Controls	RATE_LIMIT_TIMEOUT_TSC	Timeout value, used for limiting the rate at which long-latency guest-side interface functions can be called, in TSC units	64-bit unsigned integer		Calculated based on a constant timeout in usec	8	1	1	8	0x9110000300000020	RO	RO	None	None	0	0	0	0
30	Execution Controls	CPUID_FIXED0_BITMAP	Bitmap of CPUID leaves which return fixed-0 values. See the [ABI Spec] for details	64-bit bitmap		From lookup table	8	1	1	8	0x9110000300000021	RO	RO	None	RO	0	0	0	0
None	Execution Controls	CPUID4_NATIVE_VALUES	Native values of CPUID(4) sub-leaves 0 through 3 at the time of TD initialization	Array of CPUID_VALUES		From CPUID(4)	16	16	4	4	0x9110000200000200	None	RO	None	None	0	0	0	0
30	Execution Controls	FEATURE_PARAVIRT_CTLS	Guest TD fine-granined control of CPU feaures paravirtualization. See the [ABI Spec] for details	64-bit bitmap		All-0	8	1	1	8	0x9110000300000022	None	RO	RW	None	0	0	0x00000FFF	0

24	Execution Controls	FILTERED_EVENTS_COUNT	Counter of the number of times a Perfmon event setting by the guest TD has been filtered out	64-bit unsigned integer	L1_AND_L2	0	8	4	1	8	0x9110000300000023	RO	RO	None	None	0	0	0	0
41	Execution Controls	FIELD_SUPPORT_AT_INIT	Indicates support of various fields at TD initialization time (TDH.MNG.INIT and TDH.IMPORT.STATE.IMMUTABLE) or migration initalization time (TDH.*PORT.STATE.IMMUTABLE). This field is used to support backward compatibility on TD-preserving updates where the TD was created or imported by an older TDX module. For details, see the [ABI Spec].	32-bit bitmap		See the [ABI Spec]	4	1	1	4	0x9110000200000028	RO	RO	None	None	0	0	0	0
41	Execution Controls	BLOCKED_COUNT	Size of TD private GPA space which had been accessible by the guest TD and is currently blocked, in multiples of 4KB	64-bit unsigned integer		0	8	1	1	8	0x9110000300000029	RO	RO	None	None	0	0	0	0
41	Execution Controls	PENDING_BLOCKED_COUNT	Size of TD private GPA space which was PENDING and could have been accepted by the guest TD and is currently blocked, in multiples of 4KB	64-bit unsigned integer		0	8	1	1	8	0x911000030000002A	RO	RO	None	None	0	0	0	0
41	Execution Controls	MEM_COUNT	Number of TD private memory pages, in multiples of 4KB	64-bit unsigned integer		0	8	1	1	8	0x911000030000002B	RO	RO	None	None	0	0	0	0
45	Execution Controls	INTR_CONFIG_STATE	Array of per-VM interrupt virtualization configuration state. See the [Interrupt Virtualization Spec] section title "Enhanced Posted Interrupt Configuration" for details.	8-bit unsigned integer	L1_AND_L2	0	1	4	1	1	0x911000000000002C	RO	RO	None	None	0	0	0	0
45	Execution Controls	PIDPT_NUM_PAGES	Array of per-VM number of PIDPT pages	16-bit unsigned integer	L1_AND_L2	0	2	4	1	2	0x9110000100000030	RO	RO	None	None	0	0	0	0
45	Execution Controls	PIDPT_NUM_ENTRIES	Array of per-VM fields, each indicating the number of PIDPT entries allocated by the host VMM for its respective VM	16-bit unsigned integer	L1_AND_L2	0	2	4	1	2	0x9110000100000034	RO	RO	RO	None	0	0	0	0
45	Execution Controls	PIDPT_HPA	Array of per-VM PIDPT HPA (incl. HKID)	Shared HPA	L1_AND_L2	NULL_PA (-1)	8	4	1	8	0x9110000300000038	RO	RO	None	None	0	0	0	0
45	Execution Controls	PIR_MASK	Array of per-VM 256-bit bit masks for filtering Shared PID. Each mask is accessible as 4 64-bit elements.	256-bit bitmaps	L1_AND_L2	0	32	4	4	8	0x911000030000003C	None	RO	RW	None	0	0	-1	0
45	Execution Controls	WAKEUP_VIRT_VECTOR	Array of per-VM wakeup virtual interrupt vectors, each used as a notification interrupts to notify L1 that posted interrupt is waiting for that VM. A value of 0 indicates no wakeup vector. Values 31 through 255 are legal wakeup vectors. Other values are illegal.	8-bit unsigned integer	L2_ONLY	0	1	4	1	1	0x911000000000004C	None	RO	RW	None	0	0	-1	0
45	Execution Controls	MAIN_NV	Array of per-VM main notification vectors	8-bit unsigned integer	L1_AND_L2	0	1	4	1	1	0x9110000000000050	RO	RO	None	None	0	0	0	0
45	Execution Controls	SHR_NV	Array of per-VM shared notification vectors	8-bit unsigned integer	L1_AND_L2	0	1	4	1	1	0x9110000000000054	RO	RO	None	None	0	0	0	0
45	Execution Controls	MAIN_NV_SHARED	Array of per-VM flags, indicating that MAIN_NV is not unique.	Boolean	L1_AND_L2	0	1	4	1	1	0x9110000000000058	RO	RO	None	None	0	0	0	0
45	Execution Controls	PID_MODE	Array of per-VM PID modes. See the [ABI Spec] for details.	8-bit unsigned integer	L1_AND_L2	0	1	4	1	1	0x911000000000005C	RO	RO	RO	None	0	0	0	0
48	Execution Controls	INIT_CPUSVN	CPUSVN from the original creation of this TD. Serves as the lowest bar for its security.	Array of 8-bit unsigned integers		0	16	1	2	8	0x1110000300000060	RO	RO	RO	RO	0	0	0	0
48	Execution Controls	INIT_TEE_TCB_SVN	TEE_TCB_SVN from the original creation of this TD. Serves as the lowest bar for its security.	TEE_TCB_SVN		0	16	1	2	8	0x1110000300000062	RO	RO	RO	RO	0	0	0	0
48	Execution Controls	INIT_TEE_MODEL	Model information corresponding to the model that INIT_TEE_TCB_SVN was captured on. See TEE_MODEL_STRUCT for more info.	TEE_MODEL_STRUCT		0	12	1	3	4	0x1110000200000064	RO	RO	RO	RO	0	0	0	0
Always	TLB Epoch Tracking	TD_EPOCH	The TD epoch counter: incremented by the host VMM using the TDH.MEM.TRACK function	64b Integer		1	8	1	1	8	0x9210000300000000	RO	RO	None	None	0	0	0	0

Always	TLB Epoch Tracking	REFCOUNT	Each REFCOUNT counts the number of LPs which may have TLB entries created during a specific TD_EPOCH and are currently executing in TDX non-root mode.	16b Unsigned Integer		0	2	2	1	2	0x9210000100000001	RO	RO	None	None	0	0	0	0
Always	Measurement	MRTD	Measurement of the initial contents of the TD	SHA384_HASH		0	48	1	6	8	0x1310000300000000	RO	RO	RO	None	0	0	0	0
Always	Measurement	MRCONFIGID	Software-defined ID for non-owner-defined configuration of the guest TD – e.g., run-time or OS configuration	SHA384_HASH		From TDH.MNG.INIT input	48	1	6	8	0x1310000300000010	RO	RO	RO	None	0	0	0	0
Always	Measurement	MROWNER	Software-defined ID for the guest TD’s owner	SHA384_HASH		From TDH.MNG.INIT input	48	1	6	8	0x1310000300000018	RO	RO	RO	None	0	0	0	0
Always	Measurement	MROWNERCONFIG	Software-defined ID for owner-defined configuration of the guest TD – e.g., specific to the workload rather than the run-time or OS	SHA384_HASH		From TDH.MNG.INIT input	48	1	6	8	0x1310000300000020	RO	RO	RO	None	0	0	0	0
Always	Measurement	RTMR	Array of NUM_RTMRS run-time extendable measurement registers	Array of SHA384_HASH		0	48	4	6	8	0x1310000300000040	None	RO	RO	None	0	0	0	0
22	Measurement	MRCONFIGSVN	Software defined SVN for non-owner-defined configuration or the guest TD. E.g., runtime or OS configurations.	16-bit unsigned integer		0	2	1	1	2	0x1310000100000080	None	RO	RO	None	0	0	0	0
22	Measurement	MROWNERCONFIGSVN	Software defined SVN for owner-defined configuration or the guest TD. E.g., specific to workload rather than the runtime or OS.	16-bit unsigned integer		0	2	1	1	2	0x1310000100000081	None	RO	RO	None	0	0	0	0
22	Measurement	MRSIGROOT	Hash of Root Signing that signed MRSIGNER	SHA384_HASH		0	48	1	6	8	0x1310000300000082	None	RO	RO	None	0	0	0	0
22	Measurement	MRSIGNER	Hashes of SIGSTRUCT signing key	SHA384_HASH		0	48	1	6	8	0x1310000300000088	None	RO	RO	None	0	0	0	0
22	Measurement	ISVSVN	ISV-assigned SVN of the TD	16-bit unsigned integer		0	2	1	1	2	0x131000010000008E	None	RO	RO	None	0	0	0	0
22	Measurement	ISVPRODID	Product ID of the TD	128-bit		0	16	1	2	8	0x131000030000008F	None	RO	RO	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_BASIC	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000480	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_MISC	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000485	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_CR0_FIXED0	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000486	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_CR0_FIXED1	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000487	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_CR4_FIXED0	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000488	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_CR4_FIXED1	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000489	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_PROCBASED_CTLS2	Virtual value of MSR	64-bit integer			8	1	1	8	0x961000030000048B	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_EPT_VPID_CAP	Virtual value of MSR	64-bit integer			8	1	1	8	0x961000030000048C	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_TRUE_PINBASED_CTLS	Virtual value of MSR	64-bit integer			8	1	1	8	0x961000030000048D	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_TRUE_PROCBASED_CTLS	Virtual value of MSR	64-bit integer			8	1	1	8	0x961000030000048E	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_TRUE_EXIT_CTLS	Virtual value of MSR	64-bit integer			8	1	1	8	0x961000030000048F	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_TRUE_ENTRY_CTLS	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000490	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_VMFUNC	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000491	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_PROCBASED_CTLS3	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000492	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_VMX_EXIT_CTLS2	Virtual value of MSR	64-bit integer			8	1	1	8	0x9610000300000493	None	RO	None	None	0	0	0	0
None	Virt. MSR Values	VIRTUAL_IA32_ARCH_CAPABILITIES	Virtual value of MSR	64-bit integer			8	1	1	8	0x961000030000010A	None	RO	None	None	0	0	0	0

Always	CPUID	CPUID_VALUES	Values returned by CPUID leaves/sub-leaves: Element 0[31:0]: EAX Element 0[63:32]: EBX Element 1[31:0]: ECX Element 1[63:32]: EDX Field code is composed as follows: Bits 31:17 Reserved, must be 0 Bit 16 Leaf number bit 31 Bits 15:9 Leaf number bit 6:0 Bit 8 Sub-leaf not applicable flag Bits 7:1 Sub-leaf number bits 6:0 Bit 0 Element index within field	CPUID_RET		From TDH.MNG.INIT input	16	512	2	8	0x9410000300000000	RO	RO	None	RO	0	0	0	0
0, 13	Migration	MIG_DEC_KEY_SET	Set when a new MIG_DEC_KEY is written, cleared when the MIG_DEC_KEY is copied to MIG_DEC_WORKING_KEY	Boolean		FALSE	1	1	1	1	0x9810000000000001	RO	RO	None	None	0	0	0	0
0, 13	Migration	EXPORT_COUNT	Counts the number of times this TD has been exported, included aborted export sessions. Incremented at the beginning of each export session (TDH.EPORT.STATE.IMMUTABLE).	32b Unsigned Integer		0	4	1	1	4	0x9810000200000002	RO	RO	None	RO	0	0	0	0
0, 13	Migration	IMPORT_COUNT	Counts the number of times this TD has been imported. Incremented by TDH.IMPORT.COMMIT.	32b Unsigned Integer		0	4	1	1	4	0x9810000200000003	RO	RO	None	RO	0	0	0	0
0, 13	Migration	MIG_EPOCH	Migration epoch Starts from 0 on migration session start, incremented by 1 on each epoch token. A value of 0xFFFFFFFF indicates out-of-order phase.	32b Unsigned Integer		0	4	1	1	4	0x9810000200000004	RO	RO	None	None	0	0	0	0
0, 13	Migration	BW_EPOCH	For Write-Blocking Export, holds the value of TD_EPOCH at last time TDH.EXPORT.BLOCKW blocked a page for writing. For Non-Blocking Export, holds the value of TD_EPOCH at the time of TDH.EXPORT.STATE.IMMUTABLE.	64b Unsigned Integer		0	8	1	1	8	0x9810000300000005	RO	RO	None	None	0	0	0	0
0, 13	Migration	TOTAL_MB_COUNT	The total number of migration bundles exported or imported during the current migration sessions	Unsigned Integer		0	8	1	1	8	0x9810000300000006	RO	RO	None	None	0	0	0	0
0	Migration	MIG_DEC_KEY	Migration decryption key, as written by the Migration TD Special write behaviour: - Acquire a shared lock on TDCS.OP_STATE to prevent concurrent migration session start. - Set MIG_DEC_KEY_SET	KEY_256		0	32	1	4	8	0x9810000300000010	None	None	None	RW	0	0	0	-1
0, 13	Migration	MIG_DEC_WORKING_KEY	Migration decryption working key Copied from MIG_DEC_KEY at the beginning of a migration session and used throughout the session.	KEY_256		0	32	1	4	8	0x9810000300000014	None	None	None	RO	0	0	0	0
0	Migration	MIG_ENC_KEY	Migration encryption key This key is first generated by the TDX module on TDH.MNG.ADDCX, and is re-generated at the beginning of each migration session (TDH.EXPORT/IMPORT.STATE.IMMUTABLE) for use in a following session.	KEY_256		Random	32	1	4	8	0x9810000300000018	None	None	None	RO	0	0	0	0
0, 13	Migration	MIG_ENC_WORKING_KEY	Migration encryption working key Copied from MIG_ENC_KEY at the beginning of a migration session (before a new MIG_ENC_KEY is generated) and used throughout the session.			0	32	1	4	8	0x981000030000001C	None	None	None	RO	0	0	0	0
0	Migration	MIG_VERSION	Migration protocol version, as written by the migration TD	16b Unsigned Integer		0	2	1	1	2	0x9810000100000020	RO	RO	None	RW	0	0	0	-1
0, 13	Migration	MIG_WORKING_VERSION	Migration working protocol version, copied from MIG_VERSION at the beginning of a migration session and used throughout the session	16b Unsigned Integer		0	2	1	1	2	0x9810000100000021	RO	RO	None	RO	0	0	0	0

0, 13	Migration	DIRTY_COUNT	Counts of the number of pages that must be re-exported, because their contents have been modified since they have been exported, before a start token may be generated	64b Unsigned Integer		0	8	1	1	8	0x9810000300000030	RO	RO	None	None	0	0	0	0
0, 13	Migration	MIG_COUNT	Counts the number of SEPT entries that need to be cleaned up after an aborted migration	64b Unsigned Integer		0	8	1	1	8	0x9810000300000031	RO	RO	None	None	0	0	0	0
0, 13	Migration	NUM_MIGS	Number of Migration Stream Context (MIGSC) pages that have been allocated (including the backward and forward MIGSC pages)	16b Unsigned Integer		0	2	1	1	2	0x9810000100000032	RO	RO	None	None	0	0	0	0
0, 13	Migration	NUM_MIGRATED_VCPUS	Number of VCPUs that have been migrated	32b Unsigned Integer		0	4	1	1	4	0x9810000200000034	RO	RO	None	None	0	0	0	0
0	Migration	PRE_IMPORT_UUID	The original value of TD_UUID before it was overwritten as part of the immutable state import	256-bit blob		0	32	1	4	8	0x9810000300000040	RO	RO	RO	RO	0	0	0	0
41	Migration	NUM_MEM_SCAN_RANGES	Number of memory scan GPA ranges, configured by TDH.MEM.SCAN.CONFIG	8-bit unsigned integer		0	1	1	1	1	0x1810000000000037	RO	RO	None	None	0	0	0	0
41	Migration	NUM_MEM_SCAN_RANGES_COMPLETED	Number of memory scan GPA ranges for which TDH.MEM.SCAN.COMP completed the scan	8-bit unsigned integer		0	1	1	1	1	0x1810000000000038	RO	RO	None	None	0	0	0	0
41	Migration	MEM_SCAN_OPERATION	Operation done by the current comprehensive memory scan. See the [ABI Spec] definition of TDH.MEM.SCAN.COMP for details.	8-bit unsigned integer		0	1	1	1	1	0x1810000000000039	RO	RO	None	None	0	0	0	0
41	Migration	MEM_SCAN_QUALIFIER	Operation qualifier for the current comprehensive memory scan. See the [ABI Spec] definition of TDH.MEM.SCAN.COMP for details.	8-bit unsigned integer		0	1	1	1	1	0x181000000000003A	RO	RO	None	None	0	0	0	0
41	Migration	MEM_SCAN_STATE	State of the comprehensive memory scan. See the [ABI Spec] for details.	8-bit unsigned integer		0	1	1	1	1	0x181000000000003B	RO	RO	None	None	0	0	0	0
41	Migration	MEM_SCAN_EPOCH	TD epoch value recorded by TDH.MEM.SCAN.COMP(PRECLEAR) after clearing all SEPT non-leaf entries A bits	64-bit unsigned integer		0	8	1	1	8	0x981000030000003C	RO	RO	None	None	0	0	0	0
60	Migration	REMOVED_COUNT	Counts memory size, in multiples of 4KB, of pages whose SEPT entry state is REMOVED, i.e., they were removed by TDH.MEM.PAGE.REMOVE during an import session, or that their import was cancelled by TDH.IMPORT.MEM CANCEL operation	64-bit unsigned integer		0	8	1	1	8	0x981000030000003D	RO	RO	None	None	0	0	0	0
60	Migration	PREALLOC_COUNT	Counts memory size, in multiples of 4KB, that has been locally pre-allocated during import by TDH.MEM.PAGE.AUG, or that their import has been cancelled by TDH.IMPORT.MEM CANCEL operation with NO_REOWN	64-bit unsigned integer		0	8	1	1	8	0x981000030000003E	RO	RO	None	None	0	0	0	0
0	Service TD	SERVTD_HASH	SHA384 hash of the bound or pre-bound service TDs	SHA384_HASH		0	48	1	6	8	0x9910000300000000	RO	RO	RO	RO	0	0	0	0
0	Service TD	SERVTD_NUM	Number of bound or pre-bound service TDs	16-bit unsigned integer		0	2	1	1	2	0x9910000100000006	RO	RO	RO	RO	0	0	0	0
0	Service TD	SERVTD_BINDINGS_TABLE	An array of service TD binding information entries The number of entries is enumerated by SERVTD_NUM.	Array of SERVTD_BINDING entries		0	128	16	16	8	0x9910000300000080	RO	RO	RO	None	0	0	0	0
48	Service TD	SERVTD_BINDING_STATE	Service TD 0 binding state, see [ABI FAS]	SERVTD_BINDING_STATE		0	1	1	1	1	0x1910000000000200	RO	RO	RO	RO	0	0	0	0
48	Service TD	SERVTD_TYPE	Service TD 0 TYPE, see [ABI FAS]	SERVTD_TYPE		0	2	1	1	2	0x1910000100000201	RO	RO	RO	RO	0	0	0	0
48	Service TD	SERVTD_ATTR	Service TD 0 ATTR, see [ABI FAS]	SERVTD_ATTR		0	8	1	1	8	0x1910000300000202	RO	RO	RO	RO	0	0	0	0
48	Service TD	SERVTD_UUID	Service TD 0 UUID, see [ABI FAS]	256-bit blob		0	32	1	4	8	0x1910000300000203	RO	RO	RO	RO	0	0	0	0
48	Service TD	SERVTD_INFO_HASH	Service TD 0 INFO_HASH, see [ABI FAS]	SHA384_HASH		0	48	1	6	8	0x1910000300000207	RO	RO	RO	RO	0	0	0	0
48	Service TD	SERVTD_INIT_ATTR	Initial Service TD 0 ATTR, see [ABI FAS]	SERVTD_ATTR		0	8	1	1	8	0x191000030000020D	RO	RO	RO	RO	0	0	0	0
48	Service TD	SERVTD_INIT_INFO_HASH	Initial Service TD 0 INFO_HASH, see [ABI FAS]	SHA384_HASH		0	48	1	6	8	0x191000030000020E	RO	RO	RO	RO	0	0	0	0

48	Service TD	SERVTD_ACCEPT_SERVTD_EXT_HASH	Hash of SERVTD_EXT that the new Service TD 0 (i.e., rebound Service TD or MigTD on the destination platform) believes is the SERVTD_EXT for this TD.	SHA384_HASH		0	48	1	6	8	0x1910000300000214	RO	RO	RW	RW	0	0	-1	-1
48	Service TD	SERVTD_REBIND_TOKEN	Rebind session token, set by TDG.SERVTD.REBIND.APPROVE.	256-bit blob		0	32	1	4	8	0x191000030000021A	None	RO	None	None	0	0	0	0
48	Service TD	SERVTD_REBIND_ACCEPT_TOKEN	Rebind session token held by the Service TD. This field is written by the ServiceTD executing TDG.VM.WR.	256-bit blob		0	32	1	4	8	0x191000030000021E	None	RO	RW	None	0	0	-1	0
48	Service TD	SERVTD_REBIND_ATTR	The intended SERVTD_ATTR for the Service TD about to be bound to the TD.	SERVTD_ATTR		0	8	1	1	8	0x1910000300000222	RO	RO	RW	None	0	0	-1	0
48	Service TD	SERVTD_EXT_HASH	SHA384 digest of the SERVTD_EXT.	SHA384_HASH		0	48	1	6	8	0x1910000300000223	RO	RO	RO	RO	0	0	0	0
20	X2APIC_IDS	X2APIC_IDS	Array of per-VCPU unique virtual x2APIC IDs	32-bit integer		0	4	4096	1	4	0x9C10000200000000	RO	RO	None	RO	0	0	0	0
6	TDX_CONNECT	CURR_IOTLB_CNT	Total IOTLB agents currently attached to this TD via IOMMU mapped PTE.	64-bit unsigned integer		0	8	1	1	8	0x9B10000300000000	RO	RO	None	None	0	0	0	0
6	TDX_CONNECT	PREV_IOTLB_CNT	Total IOTLB agents from previous TD_EPOCH that require IOTLB invalidation for tracking to be done.	64-bit unsigned integer		0	8	1	1	8	0x9B10000300000001	RO	RO	None	None	0	0	0	0
32	TDX_CONNECT	REQ_ACTIVE	Invalidation tracker which keeps the type of the current TD invalidation request (e.g. DMAR or IOTLB). This internal flag is used for correct TDX Module enforcements when the host VMM actually fulfills the TD invalidation request with TDH.IQ.INV.REQUEST. For details, see the [TDX Connect ABI Spec].	8-bit enumerated value		0	1	1	1	1	0x9B10000000000002	RO	RO	None	None	0	0	0	0
32	TDX_CONNECT	INV_VM_INDEX	VM index for which the IOTLB invalidation was requested	8-bit unsigned integer		0	1	1	1	1	0x9B10000000000004	RO	RO	None	None	0	0	0	0
32	TDX_CONNECT	REQ_DATA	Invalidation request data: - For L1 IOTLB invalidation request (see TDG.IQ.INV.REQUEST Leaf), REQ_DATA keeps the requested number of GPA ranges to invalidate in the request. - For L1 DMAR invalidation (see TDG.DMAR.RELEASE Leaf), REQ_DATA keeps the RID_PASID (from the FUNCTION_ID).	16-bit unsigned integer		0	2	1	1	2	0x9B10000100000005	RO	RO	None	None	0	0	0	0
32	TDX_CONNECT	REQ_IOMMU_BM	Active TD IOMMU bitmask. 128 bits for all possible NUM_TOTAL_IOMMUs	128-bit bit mask		0	16	1	2	8	0x9B10000300000006	RO	RO	None	None	0	0	0	0
6	TDX_CONNECT	IOTLB_TRACK_ARRAY	IOTLB invalidation tracker	Array of IOTLB_INV_TRACKER_T		0	8	128	1	8	0x9B10000300000200	RO	RO	None	None	0	0	0	0
32	TDX_CONNECT	IOTLB_COMMITTED	Array of NUM_TOTAL_IOMMUs, counter of descriptors in COMMITTED state per IOMMU index	Array of 8-bit unsigned integers		0	2	128	1	2	0x9B10000100000400	RO	RO	None	None	0	0	0	0
32	TDX_CONNECT	IOTLB_COMPLETE	Array of NUM_TOTAL_IOMMUs, counter of descriptors in COMPLETE state per IOMMU index	Array of unsigned 8-bit		0	2	128	1	2	0x9B10000100000600	RO	RO	None	None	0	0	0	0
None	MSR Bitmaps	MSR_BITMAPS	TD-scope RDMSR/WRMSR exit control bitmaps	MSR Exit Bitmaps		See MSR Handling spreadsheet	8	512	1	8	0x2010000300000000	None	RO	None	None	0	0	0	0
None	Secure EPT Root	SEPT_ROOT	Secure EPT root page (PML5 or PML4)	Secure EPT Entry		All entries: bit 63 set, other bits clear	8	512	1	8	0x2110000300000000	None	RO	None	None	0	0	0	0

0, 13	MIGSC Links	MIGSC_LINKS	An array of links to Migration Stream Contexts. - Entry 0 is for the backward migration stream. - Entry [i + 1] is for forward migration stream i. Each entry contains the following information: Bit 51:12: MIGSC_HPA: Bits 52:12 of the MIGSC page HPA (without the HKID bits) Bit 0: LOCK: Mutex for controlling access to the MIGSC Bit 1: INITIALIZED: A boolean flag, indicating that the MIGSC has been initialized. Bit 2: ENABLED: A boolean flag, indicating that the MIGS is enabled The flags are held here, not in the MIGSC itself, to enable efficient state-related operations on all migration streams, e.g., disabling all streams.	MIGSC_LINK		0	8	512	1	8	0x9A10000300000000	RO	RO	None	None	0	0	0	0
None	L2 Secure EPT Root [1]	L2_SEPT_ROOT_1	L2 VM's Secure EPT root page (PML5 or PML4)	Secure EPT Entry		0	8	512	1	8	0x2510000300000000	None	RO	None	None	0	0	0	0
None	L2 Secure EPT Root [2]	L2_SEPT_ROOT_2	L2 VM's Secure EPT root page (PML5 or PML4)	Secure EPT Entry		0	8	512	1	8	0x2910000300000000	None	RO	None	None	0	0	0	0
None	L2 Secure EPT Root [3]	L2_SEPT_ROOT_3	L2 VM's Secure EPT root page (PML5 or PML4)	Secure EPT Entry		0	8	512	1	8	0x2D10000300000000	None	RO	None	None	0	0	0	0