VTCR_EL2, Virtualization Translation Control Register

The VTCR_EL2 characteristics are:

Purpose

The control register for stage 2 of the EL1&0 translation regime.

Configuration

AArch64 System register VTCR_EL2 bits [31:0] are architecturally mapped to AArch32 System register VTCR[31:0].

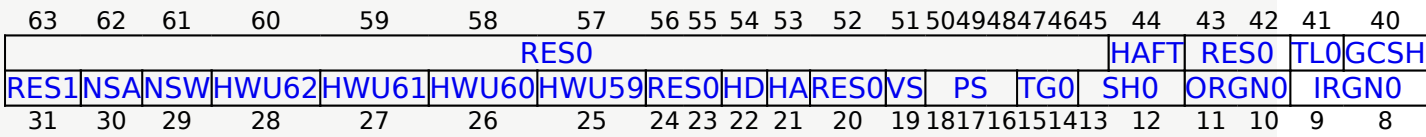
If EL2 is not implemented, this register is res0 from EL3.

This register has no effect if EL2 is not enabled in the current Security state.

Attributes

VTCR_EL2 is a 64-bit register.

Field descriptions



Unless stated otherwise, any of the bits in VTCR_EL2 are permitted to be cached in a TLB.

Bits [63:45]

Reserved, res0.

HAFT, bit [44]

When FEAT_HAFT is implemented:

Hardware managed Access Flag for Tables. Enables the Hardware managed Access Flag for Tables.

HAFT	Meaning
0b0	Hardware managed Access Flag for Tables is disabled.

0b1	Hardware managed Access Flag for Tables is enabled.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Bits [43:42]

Reserved, res0.

TL0, bit [41]
When FEAT_THE is implemented:

Control bit to check for presence of MMU TopLevel0 permission attribute.

TL0	Meaning
0b0	This bit does not have any effect on Stage 2 translations.
0b1	Enables MMU TopLevel0 permission attribute check for TTBR0_EL1 and TTBR1_EL1 translations.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

GCSH, bit [40]
When FEAT_THE is implemented and FEAT_GCS is implemented:

Assured stage 1 translations for Guarded control stacks. Enforces use of the AssuredOnly attribute in stage 2 for the memory accessed by privileged Guarded control stack data accesses.

GCSH	Meaning

0b0	For the memory accessed by privileged Guarded control stack data accesses, the AssuredOnly attribute in stage 2 is not required to be set.
0b1	For the memory accessed by privileged Guarded control stack data accesses, the AssuredOnly attribute in stage 2 is required to be set.

This bit is permitted to be cached in a TLB.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Bit [39]

Reserved, res0.

D128, bit [38]
When FEAT_D128 is implemented:

Enable 128-bit Page Table Descriptors. Enables VMSAv9-128 translation system for the Stage 2 Translation Process.

D128	Meaning
0b0	Translation system follows VMSA-64 translation process.
0b1	Translation system follows VMSAv9-128 translation process.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

S2POE, bit [37]
When FEAT_S2POE is implemented:

Enable Permission Overlay. Enables permission overlay in Stage 2 Permission model.

S2POE	Meaning
0b0	Overlay disabled.
0b1	Overaly enabled.

This bit is not permitted to be cached in a TLB.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

S2PIE, bit [36]
When FEAT_S2PIE is implemented:

Select Permission Model. Enables usage of permission indirection in Stage 2 Permission model.

S2PIE	Meaning
0b0	Direct permission model.
0b1	Indirect permission model.

This field is res1 when VTCR_EL2.D128 is set.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

TL1, bit [35]
When FEAT_THE is implemented:

Control bit to check for presence of MMU TopLevel1 permission attribute.

TL1	Meaning

0b0	This bit does not have any effect on Stage 2 translations.
0b1	Enables MMU TopLevel1 permission attribute check for TTBR0_EL1 and TTBR1_EL1 translations.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

AssuredOnly, bit [34]
When FEAT_THE is implemented:

AssuredOnly attribute enable. Indicates use of bit[58] of the stage 2 translation table block or page descriptor.

AssuredOnly	Meaning
0b0	Bit[58] of each stage 2 translation block or page descriptor do not indicate AssuredOnly attribute.
0b1	Bit[58] of each stage 2 translation block or page descriptor indicate AssuredOnly attribute.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

SL2, bit [33]
When FEAT_LPA2 is implemented and (FEAT_D128 is not implemented or VTCR_EL2.D128 == 0):

Starting level of the stage 2 translation lookup controlled by VTCR_EL2.

If VTCR_EL2.DS == 1, then VTCR_EL2.SL2, in combination with VTCR_EL2.SL0, gives encodings for the stage 2 translation table walk initial lookup level.

If VTCR_EL2.DS == 0, then VTCR_EL2.SL2 is res0.

If the translation granule size is not 4KB, then this field is res0.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

When FEAT_D128 is implemented and VTCR_EL2.D128 == 1:

This field is IGNORED.

Otherwise:

Reserved, res0.

DS, bit [32]
When FEAT_LPA2 is implemented:

This field affects whether a 52-bit output address can be described by the translation tables of the 4KB or 16KB translation granules.

DS	Meaning
0b0	Bits[49:48] of translation descriptors are res0. Bits[9:8] in Block and Page descriptors encode shareability information in the SH[1:0] field. Bits[9:8] in Table descriptors are ignored by hardware. The minimum value of VTCR_EL2.T0SZ is 16. Any memory access using a smaller value generates a stage 2 level 0 translation table fault. The minimum value of VSTCR_EL2.T0SZ is 16. Any memory access using a smaller value generates a stage 2 level 0 translation table fault. Output address[51:48] is 0000.

0b1	Bits[49:48] of translation descriptors hold output address[49:48]. Bits[9:8] in translation descriptors hold output address[51:50]. The shareability information of Block and Page descriptors for cacheable locations is determined by VTCR_EL2.SH0. The minimum value of VTCR_EL2.T0SZ is 12. Any memory access using a smaller value generates a stage 2 level 0 translation table fault. The minimum value of VSTCR_EL2.T0SZ is 12. Any memory access using a smaller value generates a stage 2 level 0 translation table fault. **Note** As FEAT_LPA must be implemented if VTCR_EL2.DS == 1, the minimum values of VTCR_EL2.T0SZ and VSTCR_EL2.T0SZ are 12, as determined by that extension. For the TLBI range instructions affecting IPA, the format of the argument is changed so that bits[36:0] hold BaseADDR[52:16]. For the 4KB translation granule, bits[15:12] of BaseADDR are treated as 0000. For the 16KB translation granule, bits[15:14] of BaseADDR are treated as 00. **Note** This forces alignment of the ranges used by the TLBI range instructions.

This field is res0 for a 64KB translation granule.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Bit [31]

Reserved, res1.

NSA, bit [30]
When FEAT_SEL2 is implemented:

Non-secure stage 2 translation output address space for the Secure EL1&0 translation regime.

NSA	Meaning
0b0	All stage 2 translations for the Non-secure IPA space of the Secure EL1&0 translation regime access the Secure PA space.
0b1	All stage 2 translations for the Non-secure IPA space of the Secure EL1&0 translation regime access the Non-secure PA space.

This bit behaves as 1 for all purposes other than reading back the value of the bit when one of the following is true:

- The value of VTCR_EL2.NSW is 1.
- The value of VSTCR_EL2.SA is 1.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

NSW, bit [29]
When FEAT_SEL2 is implemented:

Non-secure stage 2 translation table address space for the Secure EL1&0 translation regime.

NSW	Meaning
0b0	All stage 2 translation table walks for the Non-secure IPA space of the Secure EL1&0 translation regime are to the Secure PA space.
0b1	All stage 2 translation table walks for the Non-secure IPA space of the Secure EL1&0 translation regime are to the Non-secure PA space.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

HWU62, bit [28]
When FEAT_HPDS2 is implemented:

Hardware Use. Indicates implementation defined hardware use of bit[62] of the stage 2 translation table Block or Page entry.

HWU62	Meaning
0b0	Bit[62] of each stage 2 translation table Block or Page entry cannot be used by hardware for an implementation defined purpose.
0b1	Bit[62] of each stage 2 translation table Block or Page entry can be used by hardware for an implementation defined purpose.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

HWU61, bit [27]
When FEAT_HPDS2 is implemented:

Hardware Use. Indicates implementation defined hardware use of bit[61] of the stage 2 translation table Block or Page entry.

HWU61	Meaning
0b0	Bit[61] of each stage 2 translation table Block or Page entry cannot be used by hardware for an implementation defined purpose.
0b1	Bit[61] of each stage 2 translation table Block or Page entry can be used by hardware for an implementation defined purpose.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

HWU60, bit [26]
When FEAT_HPDS2 is implemented:

Hardware Use. Indicates implementation defined hardware use of bit[60] of the stage 2 translation table Block or Page entry.

HWU60	Meaning
0b0	Bit[60] of each stage 2 translation table Block or Page entry cannot be used by hardware for an implementation defined purpose.
0b1	Bit[60] of each stage 2 translation table Block or Page entry can be used by hardware for an implementation defined purpose.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

HWU59, bit [25]
When FEAT_HPDS2 is implemented:

Hardware Use. Indicates implementation defined hardware use of bit[59] of the stage 2 translation table Block or Page entry.

HWU59	Meaning
0b0	Bit[59] of each stage 2 translation table Block or Page entry cannot be used by hardware for an implementation defined purpose.
0b1	Bit[59] of each stage 2 translation table Block or Page entry can be used by hardware for an implementation defined purpose.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Bits [24:23]

Reserved, res0.

HD, bit [22]
When FEAT_HAFDBS is implemented:

Hardware management of dirty state in stage 2 translations when EL2 is enabled in the current Security state.

HD	Meaning

0b0	Stage 2 hardware management of dirty state disabled.
0b1	Stage 2 hardware management of dirty state enabled, only if the VTCR_EL2.HA bit is also set to 1.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

HA, bit [21]
When FEAT_HAFDBS is implemented:

Hardware Access flag update in stage 2 translations when EL2 is enabled in the current Security state.

HA	Meaning
0b0	Stage 2 Access flag update disabled.
0b1	Stage 2 Access flag update enabled.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Bit [20]

Reserved, res0.

VS, bit [19]
When FEAT_VMID16 is implemented:

VMID Size.

VS	Meaning

0b0	8-bit VMID. The upper 8 bits of VTTBR_EL2 are ignored by the hardware, and treated as if they are all zeros, for every purpose except when reading back the register.
0b1	16-bit VMID. The upper 8 bits of VTTBR_EL2 are used for allocation and matching in the TLB.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

PS, bits [18:16]

Physical address Size for the second stage of translation.

PS	Meaning	Applies when
0b000	32 bits, 4GB.	
0b001	36 bits, 64GB.	
0b010	40 bits, 1TB.	
0b011	42 bits, 4TB.	
0b100	44 bits, 16TB.	
0b101	48 bits, 256TB.	
0b110	52 bits, 4PB.	
0b111	56 bits, 64PB.	When FEAT_D128 is implemented

All other values are reserved.

The reserved values behave in the same way as the 0b101 or 0b110 encoding, but software must not rely on this property as the behavior of the reserved values might change in a future revision of the architecture.

If the translation granule is not 64KB and FEAT_LPA2 is not implemented, the value 0b110 is treated as reserved.

It is implementation defined whether an implementation that does not implement FEAT_LPA supports setting the value of `0b110` for the 64KB translation granule size or whether setting this value behaves as the `0b101` encoding.

In an implementation that supports 52-bit PAs, if the value of this field is not `0b110` or a value treated as `0b110`, then bits[51:48] of every translation table base address for the stage of translation controlled by VTCR_EL2 are `0b0000`.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

TG0, bits [15:14]

Granule size for the VTTBR_EL2.

TG0	Meaning
`0b00`	4KB.
`0b01`	64KB.
`0b10`	16KB.

Other values are reserved.

If FEAT_GTG is implemented, ID_AA64MMFR0_EL1.{TGran4_2, TGran16_2, TGran64_2} indicate which granule sizes are supported for stage 2 translation.

If FEAT_GTG is not implemented, ID_AA64MMFR0_EL1.{TGran4, TGran16, TGran64} indicate which granule sizes are supported.

If the value is programmed to either a reserved value or a size that has not been implemented, then the hardware will treat the field as if it has been programmed to an implementation defined choice of the sizes that has been implemented for all purposes other than the value read back from this register.

It is implementation defined whether the value read back is the value programmed or the value that corresponds to the size chosen.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

SH0, bits [13:12]

Shareability attribute for memory associated with translation table walks using VTTBR_EL2 or VSTTBR_EL2.

SH0	Meaning
0b00	Non-shareable.
0b10	Outer Shareable.
0b11	Inner Shareable.

Other values are reserved. The effect of programming this field to a Reserved value is that behavior is constrained unpredictable.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

ORGN0, bits [11:10]

Outer cacheability attribute for memory associated with translation table walks using VTTBR_EL2 or VSTTBR_EL2.

ORGN0	Meaning
0b00	Normal memory, Outer Non-cacheable.
0b01	Normal memory, Outer Write-Back Read-Allocate Write-Allocate Cacheable.
0b10	Normal memory, Outer Write-Through Read-Allocate No Write-Allocate Cacheable.
0b11	Normal memory, Outer Write-Back Read-Allocate No Write-Allocate Cacheable.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

IRGN0, bits [9:8]

Inner cacheability attribute for memory associated with translation table walks using VTTBR_EL2 or VSTTBR_EL2.

IRGN0	Meaning
0b00	Normal memory, Inner Non-cacheable.
0b01	Normal memory, Inner Write-Back Read-Allocate Write-Allocate Cacheable.
0b10	Normal memory, Inner Write-Through Read-Allocate No Write-Allocate Cacheable.

0b11	Normal memory, Inner Write-Back Read-Allocate No Write-Allocate Cacheable.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

SL0, bits [7:6]
When FEAT_TTST is implemented and (FEAT_D128 is not implemented or VTCR_EL2.D128 == 0):

Starting level of the stage 2 translation lookup, controlled by VTCR_EL2. The meaning of this field depends on the value of VTCR_EL2.TG0.

SL0	Meaning
0b00	If VTCR_EL2.TG0 is 0b00 (4KB granule): • If FEAT_LPA2 is not implemented, start at level 2. • If FEAT_LPA2 is implemented and VTCR_EL2.SL2 is 0b0, start at level 2. • If FEAT_LPA2 is implemented and VTCR_EL2.SL2 is 0b1, start at level -1. If VTCR_EL2.TG0 is 0b10 (16KB granule) or 0b01 (64KB granule), start at level 3.

`0b01` If VTCR_EL2.TG0 is `0b00` (4KB granule):

- If FEAT_LPA2 is not implemented, start at level 1.
- If FEAT_LPA2 is implemented and VTCR_EL2.SL2 is `0b0`, start at level 1.
- If FEAT_LPA2 is implemented, the combination of VTCR_EL2.SL0 == 01 and VTCR_EL2.SL2 == 1 is reserved.

If VTCR_EL2.TG0 is `0b10` (16KB granule) or `0b01` (64KB granule), start at level 2.

`0b10` If VTCR_EL2.TG0 is `0b00` (4KB granule):

- If FEAT_LPA2 is not implemented, start at level 0.
- If FEAT_LPA2 is implemented and VTCR_EL2.SL2 is `0b0`, start at level 0.
- If FEAT_LPA2 is implemented, the combination of VTCR_EL2.SL0 == 10 and VTCR_EL2.SL2 == 1 is reserved.

If VTCR_EL2.TG0 is `0b10` (16KB granule) or `0b01` (64KB granule), start at level 1.

0b11	If VTCR_EL2.TG0 is 0b00 (4KB granule): • If FEAT_LPA2 is not implemented, start at level 3. • If FEAT_LPA2 is implemented and VTCR_EL2.SL2 is 0b0, start at level 3. • If FEAT_LPA2 is implemented, the combination of VTCR_EL2.SL0 == 11 and VTCR_EL2.SL2 == 1 is reserved. If VTCR_EL2.TG0 is 0b10 (16KB granule) and FEAT_LPA2 is implemented, start at level 0.

If this field is programmed to a value that is not consistent with the programming of VTCR_EL2.T0SZ, then a stage 2 level 0 Translation fault is generated.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Otherwise:

Starting level of the stage 2 translation lookup, controlled by VTCR_EL2. The meaning of this field depends on the value of VTCR_EL2.TG0.

SL0	Meaning
0b00	If VTCR_EL2.TG0 is 0b00 (4KB granule), start at level 2. If VTCR_EL2.TG0 is 0b10 (16KB granule) or 0b01 (64KB granule), start at level 3.
0b01	If VTCR_EL2.TG0 is 0b00 (4KB granule), start at level 1. If VTCR_EL2.TG0 is 0b10 (16KB granule) or 0b01 (64KB granule), start at level 2.

0b10	If VTCR_EL2.TG0 is 0b00 (4KB granule), start at level 0. If VTCR_EL2.TG0 is 0b10 (16KB granule) or 0b01 (64KB granule), start at level 1.

All other values are reserved. If this field is programmed to a reserved value, or to a value that is not consistent with the programming of VTCR_EL2.T0SZ, then a stage 2 level 0 Translation fault is generated.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

T0SZ, bits [5:0]

The size offset of the memory region addressed by VTTBR_EL2. The region size is $2^{(64-T0SZ)}$ bytes.

The maximum and minimum possible values for T0SZ depend on the level of translation table and the memory translation granule size, as described in 'The AArch64 Virtual Memory System Architecture'.

If this field is programmed to a value that is not consistent with the programming of SL0, then a stage 2 level 0 Translation fault is generated.

Note

For the 4KB translation granule, if FEAT_LPA2 is implemented and this field is less than 16, the translation table walk begins with a level -1 initial lookup.

For the 16KB translation granule, if FEAT_LPA2 is implemented and this field is less than 17, the translation table walk begins with a level 0 initial lookup.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally unknown value.

Accessing VTCR_EL2

Unless stated otherwise, any of the bits in VTCR_EL2 are permitted to be cached in a TLB.

Accesses to this register use the following encodings in the System register encoding space:

MRS <Xt>, VTCR_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b010

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        X[t, 64] = NVMem[0x040];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    X[t, 64] = VTCR_EL2;
elsif PSTATE.EL == EL3 then
    X[t, 64] = VTCR_EL2;
```

MSR VTCR_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0001	0b010

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        NVMem[0x040] = X[t, 64];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    VTCR_EL2 = X[t, 64];
elsif PSTATE.EL == EL3 then
    VTCR_EL2 = X[t, 64];
```

28/03/2023 16:01; 72747e43966d6b97dcbd230a1b3f0421d1ea3d94