HCRX_EL2, Extended Hypervisor Configuration Register

The HCRX_EL2 characteristics are:

Purpose

Provides configuration controls for virtualization, including defining whether various operations are trapped to EL2.

Configuration

This register is present only when FEAT_HCX is implemented. Otherwise, direct accesses to HCRX_EL2 are undefined.

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

The bits in this register behave as if they are 0 for all purposes other than direct reads of the register if:

- EL2 is not enabled in the current Security state.
- SCR_EL3.HXEn is 0.

Attributes

HCRX_EL2 is a 64-bit register.

Field descriptions

63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44
RES0																			

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12
RES0									GCSEn	EnIDCP128	EnSDERR	TMEA	EnSNERR	D128En	PTTWI	SCTLR2En	TCR2En	RES0	

Bits [63:23]

Reserved, res0.

GCSEn, bit [22]
When FEAT_GCS is implemented:

Guarded Control Stack enable. Controls Guarded Control Stack behavior at EL1 and EL0.

GCSEn	Meaning

0b0	The Guarded Control Stack is disabled at EL1 and EL0.
0b1	Guarded Control Stack behavior at EL1 and EL0 is not affected by mechanism.

This field is ignored by the PE and treated as one when EL2 is disabled in the current Security state or HCR_EL2.<E2H,TGE> == {1,1}.

This field is ignored by the PE and treated as zero when EL2 is enabled in the current Security state and HCR_EL2.<E2H,TGE> != {1,1} and SCR_EL3.HXEn == 0.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

EnIDCP128, bit [21]
When FEAT_SYSREG128 is implemented and HCR_EL2.[E2H,TGE] != 0b11:

Enables access to implementation defined 128-bit System registers.

EnIDCP128	Meaning
0b0	If EL2 is implemented and enabled in the current Security state, accesses at EL1, EL0 to implementation defined 128-bit System registers are trapped to EL2 using an ESR_EL2.EC value of 0x14, unless the access generates a higher priority exception. Disables the functionality of the 128-bit implementation defined System registers that are accessible at EL2.
0b1	No accesses are trapped by this control.

The reset behavior of this field is:

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

Otherwise:

Reserved, res0.

EnSDERR, bit [20]
When FEAT_ADERR is implemented:

Enable Synchronous Device Read Error. Override SCTLR2_EL1.EnADERR.

EnSDERR	Meaning
0b0	This field has no effect on External aborts on Device memory reads at EL1 and EL0.
0b1	External abort on Device memory reads generate synchronous Data Abort exceptions in the EL1&0 translation regime.

Setting this field to 1 does not guarantee that the PE is able to take a synchronous Data Abort exception for an External abort on a Device memory read in every case.

Setting this field to 1 might have a performance impact for Device memory reads.

This field is ignored by the PE and treated as zero when any of the following are true:

- SCR_EL3.HXEn == 0.
- EL2 is disabled in the current Security state.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

TMEA, bit [19]
When FEAT_DoubleFault2 is implemented:

Trap Masked External Aborts. Controls whether a masked error exception at a lower Exception level is taken to EL2.

TMEA	Meaning
0b0	Synchronous External Abort exceptions and SError exceptions at EL1 and EL0 are unaffected by this mechanism.
0b1	Synchronous External Abort exceptions when PSTATE.A is 1 and masked SError exceptions at EL1 and EL0 are taken to EL2, unless routed to another Exception level by a higher priority control.

This field is ignored by the PE and treated as zero when any of the following are true:

- SCR_EL3.HXEn == 0.
- HCR_EL2.{E2H,TGE} == {1,1}.
- EL2 is disabled in the current Security state.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

EnSNERR, bit [18]
When FEAT_ANERR is implemented:

Enable Synchronous Normal Read Error. Override SCTLR2_EL1.EnANERR.

EnSNERR	Meaning
0b0	This field has no effect on External aborts on Normal memory reads at EL1 and EL0.

0b1	External abort on Normal memory reads generate synchronous Data Abort exceptions in the EL1&0 translation regime.

Setting this field to 1 does not guarantee that the PE is able to take a synchronous Data Abort exception for an External abort on a Normal memory read in every case.

Setting this field to 1 might have a performance impact for Normal memory reads.

This field is ignored by the PE and treated as zero when any of the following are true:

- SCR_EL3.HXEn == 0.
- EL2 is disabled in the current Security state.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

D128En, bit [17]
When FEAT_D128 is implemented:

128-bit System Register trap control. Enable access to 128-bit System Registers via MRRS, MSRR instructions.

- If EL1 is using AArch64 state, accesses to the following registers are trapped to EL2 and reported using EC syndrome value 0x14:
  - TTBR0_EL1.
  - TTBR1_EL1.
  - If FEAT_THE is implemented, RCWMASK_EL1, RCWSMASK_EL1.
  - PAR_EL1.

D128En	Meaning

0b0	EL1 accesses to the specified registers are disabled, and trapped to EL2.
0b1	This control does not cause any instructions to be trapped.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

PTTWI, bit [16]
When FEAT_THE is implemented:

Permit Translation Table Walk Incoherence.

Permits RCWS instructions to have Reduced Coherence property.

PTTWI	Meaning
0b0	If EL2 is implemented and enabled in the current Security state, write accesses generated by RCWS at EL1&0 do not have the Reduced Coherence property.
0b1	Write accesses generated by RCWS at EL1&0 have the Reduced Coherence property, if enabled by TCR2_EL1.PTTWI.

This bit is permitted to be cached in TLB.

This bit is permitted to be built as a read-only bit with a fixed value of 0.

The reset behavior of this field is:

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

Otherwise:

Reserved, res0.

SCTLR2En, bit [15]
When FEAT_SCTLR2 is implemented:

SCTLR2_EL1 Enable. In AArch64 state, accesses to SCTLR2_EL1 are trapped to EL2 and reported using EC syndrome value `0x18`.

SCTLR2En	Meaning
`0b0`	Accesses to SCTLR2_EL1 at EL1 are trapped to EL2, unless the access generates a higher priority exception. The value in SCTLR2_EL1 is treated as 0.
`0b1`	This control does not cause any instructions to be trapped.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to `0`.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

TCR2En, bit [14]
When FEAT_TCR2 is implemented:

TCR2_EL1 Enable. In AArch64 state, accesses to TCR2_EL1 are trapped to EL2 and reported using EC syndrome value `0x18`.

TCR2En	Meaning
`0b0`	Accesses to TCR2_EL1 at EL1 are trapped to EL2, unless the access generates a higher priority exception. The value in TCR2_EL1 is treated as 0.
`0b1`	This control does not cause any instructions to be trapped.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to `0`.

- Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Bits [13:12]

Reserved, res0.

MSCEn, bit [11]
When FEAT_MOPS is implemented:

Memory Set and Memory Copy instructions Enable. Enables execution of the CPY*, SETG*, SETP*, SETM*, and SETE* instructions at EL1 or EL0.

MSCEn	Meaning
0b0	Execution of the Memory Copy and Memory Set instructions is undefined at EL1 or EL0.
0b1	This control does not cause any instructions to be undefined.

This bit behaves as if it is 1 if any of the following are true:

- EL2 is not implemented or enabled.
- The value of HCR_EL2.{E2H, TGE} is {1, 1}.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

MCE2, bit [10]
When FEAT_MOPS is implemented:

Controls Memory Copy and Memory Set exceptions generated as part of attempting to execute the Memory Copy and Memory Set instructions from EL1.

MCE2	Meaning

0b0	Memory Copy and Memory Set exceptions generated from EL1 are taken to EL1.
0b1	Memory Copy and Memory Set exceptions generated from EL1 are taken to EL2.

When the value of HCR_EL2.{E2H, TGE} is {1, 1}, this control does not affect any exceptions due to the higher priority SCTLR_EL2.MSCEn control.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

CMOW, bit [9]
When FEAT_CMOW is implemented:

Controls cache maintenance instruction permission for the following instructions executed at EL1 or EL0.

- IC IVAU, DC CIVAC, DC CIGDVAC and DC CIGVAC.
- ICIMVAU, DCCIMVAC.

CMOW	Meaning
0b0	These instructions executed at EL1 or EL0 with stage 2 read permission, but without stage 2 write permission do not generate a stage 2 permission fault.
0b1	These instructions executed at EL1 or EL0, if enabled as a result of SCTLR_EL1.UCI==1, with stage 2 read permission, but without stage 2 write permission generate a stage 2 permission fault.

For this control, stage 2 has write permission if S2AP[1] is 1 or DBM is 1 in the stage 2 descriptor. The instructions do not cause an update to the dirty state.

This bit is permitted to be cached in a TLB.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to `0`.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

VFNMI, bit [8]
When FEAT_NMI is implemented:

Virtual FIQ Interrupt with Superpriority. Enables signaling of virtual FIQ interrupts with Superpriority.

VFNMI	Meaning
`0b0`	When HCR_EL2.VF is 1, a signaled pending virtual FIQ interrupt does not have Superpriority.
`0b1`	When HCR_EL2.VF is 1, a signaled pending virtual FIQ interrupt has Superpriority.

When HCR_EL2.VF is 0, this bit has no effect.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to `0`.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

VINMI, bit [7]
When FEAT_NMI is implemented:

Virtual IRQ Interrupt with Superpriority. Enables signaling of virtual IRQ interrupts with Superpriority.

VINMI	Meaning

0b0	When HCR_EL2.VI is 1, a signaled pending virtual IRQ interrupt does not have Superpriority.
0b1	When HCR_EL2.VI is 1, a signaled pending virtual IRQ interrupt has Superpriority.

When HCR_EL2.VI is 0, this bit has no effect.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

TALLINT, bit [6]
When FEAT_NMI is implemented:

Traps the following writes at EL1 using AArch64 to EL2, when EL2 is implemented and enabled:

- MSR (register) writes of ALLINT.
- MSR (immediate) writes of ALLINT with a value of 1.

TALLINT	Meaning
0b0	This control does not cause any instructions to be trapped.
0b1	The specified MSR accesses at EL1 using AArch64 are trapped to EL2.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

SMPME, bit [5]
When FEAT_SME is implemented:

Streaming Mode Priority Mapping Enable.

Controls mapping of the value of SMPRI_EL1.Priority for streaming execution priority at EL0 or EL1.

SMPME	Meaning
0b0	The effective priority value is taken from SMPRI_EL1.Priority.
0b1	The effective priority value is: • When the current Exception level is EL2 or EL3, the value of SMPRI_EL1.Priority. • When the current Exception level is EL0 or EL1, the value of the SMPRIMAP_EL2 field corresponding to the value of SMPRI_EL1.Priority.

When SMIDR_EL1.SMPS is '0', this field is res0.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

FGTnXS, bit [4]
When FEAT_XS is implemented:

Determines if the fine-grained traps in HFGITR_EL2 that apply to each of the TLBI maintenance instructions that are accessible at EL1 also apply to the corresponding TLBI maintenance instructions with the nXS qualifier.

FGTnXS	Meaning

0b0	The fine-grained trap in the HFGITR_EL2 that applies to a TLBI maintenance instruction at EL1 also applies to the corresponding TLBI instruction with the nXS qualifier at EL1.
0b1	The fine-grained trap in the HFGITR_EL2 that applies to a TLBI maintenance instruction at EL1 does not apply to the corresponding TLBI instruction with the nXS qualifier at EL1.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

FnXS, bit [3]
When FEAT_XS is implemented:

Determines the behavior of TLBI instructions affected by the XS attribute.

This control bit also determines whether an AArch64 DSB instruction behaves as a DSB instruction with an nXS qualifier when executed at EL0 and EL1.

FnXS	Meaning
0b0	This control does not have any effect on the behavior of the TLBI maintenance instructions.

0b1	A TLBI maintenance instruction without the nXS qualifier executed at EL1 behaves in the same way as the corresponding TLBI maintenance instruction with the nXS qualifier. An AArch64 DSB instruction executed at EL1 or EL0 behaves in the same way as the corresponding DSB instruction with the nXS qualifier executed at EL1 or EL0.

This bit is permitted to be cached in a TLB.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

EnASR, bit [2]
When FEAT_LS64_V is implemented:

When HCR_EL2.{E2H, TGE} != {1, 1}, traps execution of an ST64BV instruction at EL0 or EL1 to EL2.

EnASR	Meaning
0b0	Execution of an ST64BV instruction at EL0 is trapped to EL2 if the execution is not trapped by SCTLR_EL1.EnASR. Execution of an ST64BV instruction at EL1 is trapped to EL2.
0b1	This control does not cause any instructions to be trapped.

A trap of an ST64BV instruction is reported using an ESR_ELx.EC value of 0x0A, with an ISS code of 0x0000000.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.

- Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

EnALS, bit [1]
When FEAT_LS64 is implemented:

When HCR_EL2.{E2H, TGE} != {1, 1}, traps execution of an LD64B or ST64B instruction at EL0 or EL1 to EL2.

EnALS	Meaning
0b0	Execution of an LD64B or ST64B instruction at EL0 is trapped to EL2 if the execution is not trapped by SCTLR_EL1.EnALS. Execution of an LD64B or ST64B instruction at EL1 is trapped to EL2.
0b1	This control does not cause any instructions to be trapped.

A trap of an LD64B or ST64B instruction is reported using an ESR_ELx.EC value of 0x0A, with an ISS code of 0x0000002.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

EnAS0, bit [0]
When FEAT_LS64_ACCDATA is implemented:

When HCR_EL2.{E2H, TGE} != {1, 1}, traps execution of an ST64BV0 instruction at EL0 or EL1 to EL2.

EnAS0	Meaning

0b0	Execution of an ST64BV0 instruction at EL0 is trapped to EL2 if the execution is not trapped by SCTLR_EL1.EnAS0. Execution of an ST64BV0 instruction at EL1 is trapped to EL2.
0b1	This control does not cause any instructions to be trapped.

A trap of an ST64BV0 instruction is reported using an ESR_ELx.EC value of 0x0A, with an ISS code of 0x0000001.

The reset behavior of this field is:

- On a Warm reset:
  - When EL3 is not implemented, this field resets to 0.
  - Otherwise, this field resets to an architecturally unknown value.

Otherwise:

Reserved, res0.

Accessing HCRX_EL2

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

MRS <Xt>, HCRX_EL2

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

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        X[t, 64] = NVMem[0xA0];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.HXEn == '0' then
        UNDEFINED;
```

```
    elsif HaveEL(EL3) && SCR_EL3.HXEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    else
        X[t, 64] = HCRX_EL2;
elsif PSTATE.EL == EL3 then
    X[t, 64] = HCRX_EL2;
```

MSR HCRX_EL2, <Xt>

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

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.<NV2,NV> == '11' then
        NVMem[0xA0] = X[t, 64];
    elsif EL2Enabled() && HCR_EL2.NV == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        UNDEFINED;
elsif PSTATE.EL == EL2 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.HXEn == '0' then
        UNDEFINED;
    elsif HaveEL(EL3) && SCR_EL3.HXEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    else
        HCRX_EL2 = X[t, 64];
elsif PSTATE.EL == EL3 then
    HCRX_EL2 = X[t, 64];
```


28/03/2023 16:01; 72747e43966d6b97dcbd230a1b3f0421d1ea3d94