GCSCR_EL2, Guarded Control Stack Control (EL2)

The GCSCR_EL2 characteristics are:

Purpose

Controls the Guarded control stack at EL2.

Configuration

This register is present only when FEAT_GCS is implemented. Otherwise, direct accesses to GCSCR_EL2 are undefined.

Attributes

GCSCR_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	43	42	41	40	39	38	37	36	35	34	33
RES0																														
RES0																						STREn	PUSHMEn	RES0	EXLOCKEN	RVCHKEN	RES0			PC

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
RES0																						STREn	PUSHMEn	RES0	EXLOCKEN	RVCHKEN	RES0				

Bits [63:10]

Reserved, res0.

STREn, bit [9]

Execution of the following instructions are trapped:

- GCSSTR.
- GCSSTTR if any of the following are true.
  - HCR_EL2.{E2H,TGE} is not {1,1}.
  - HCR_EL2.{E2H,TGE} is {1,1} and PSTATE.UAO is 1.

STREn	Meaning
0b0	Execution of any of the specified instructions at EL2 cause a GCS exception.
0b1	This control does not cause any instructions to be trapped.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

PUSHMEn, bit [8]

Trap GCSPUSHM instruction.

PUSHMEn	Meaning
`0b0`	Execution of a GCSPUSHM instruction at EL2 causes a Trap exception.
`0b1`	This control does not cause any instructions to be trapped.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

Bit [7]

Reserved, res0.

EXLOCKEN, bit [6]

Exception state lock.

Prevents `MSR` instructions from writing to ELR_EL2 or SPSR_EL2.

EXLOCKEN	Meaning
`0b0`	EL2 exception state locking disabled.
`0b1`	EL2 exception state locking enabled.

The reset behavior of this field is:

- On a Warm reset, this field resets to `0`.

RVCHKEN, bit [5]

Return value check enable.

RVCHKEN	Meaning
`0b0`	Return value checking disabled at EL2.
`0b1`	Return value checking enabled at EL2.

The reset behavior of this field is:

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

Bits [4:1]

Reserved, res0.

PCRSEL, bit [0]

Guarded control stack procedure call return enable selection.

PCRSEL	Meaning
0b0	Guarded control stack at EL2 is not PCR Selected.
0b1	Guarded control stack at EL2 is PCR Selected.

The reset behavior of this field is:

- On a Warm reset, this field resets to 0.

Accessing GCSCR_EL2

When FEAT_VHE is implemented, and HCR_EL2.E2H is 1, without explicit synchronization, accesses from EL2 using the register name GCSCR_EL2 or GCSCR_EL1 are not guaranteed to be ordered with respect to accesses using the other register name.

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

MRS <Xt>, GCSCR_EL2

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0101	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if 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.GCSEn == '0' then
```

```
            UNDEFINED;
        elsif HaveEL(EL3) && SCR_EL3.GCSEn == '0' then
            if Halted() && EDSCR.SDD == '1' then
                UNDEFINED;
            else
                AArch64.SystemAccessTrap(EL3, 0x18);
        else
            X[t, 64] = GCSCR_EL2;
    elsif PSTATE.EL == EL3 then
        X[t, 64] = GCSCR_EL2;
```

MSR GCSCR_EL2, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b100	0b0010	0b0101	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if 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.GCSEn == '0' then
        UNDEFINED;
    elsif HaveEL(EL3) && SCR_EL3.GCSEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    else
        GCSCR_EL2 = X[t, 64];
elsif PSTATE.EL == EL3 then
    GCSCR_EL2 = X[t, 64];
```

MRS <Xt>, GCSCR_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0101	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
```

```
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.GCSEn == '0' then
        UNDEFINED;
    elsif EL2Enabled() &&
IsFeatureImplemented(FEAT_FGT) && (!HaveEL(EL3) ||
SCR_EL3.FGTEn == '1') && HFGRTR_EL2.nGCS_EL1 == '0'
then
        AArch64.SystemAccessTrap(EL2, 0x18);
    elsif HaveEL(EL3) && SCR_EL3.GCSEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    elsif EL2Enabled() && HCR_EL2.<NV2,NV1,NV> ==
'111' then
        X[t, 64] = NVMem[0x8D0];
    else
        X[t, 64] = GCSCR_EL1;
elsif PSTATE.EL == EL2 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.GCSEn == '0' then
        UNDEFINED;
    elsif HaveEL(EL3) && SCR_EL3.GCSEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    elsif HCR_EL2.E2H == '1' then
        X[t, 64] = GCSCR_EL2;
    else
        X[t, 64] = GCSCR_EL1;
elsif PSTATE.EL == EL3 then
    X[t, 64] = GCSCR_EL1;
```

MSR GCSCR_EL1, <Xt>

op0	op1	CRn	CRm	op2
0b11	0b000	0b0010	0b0101	0b000

```
if PSTATE.EL == EL0 then
    UNDEFINED;
elsif PSTATE.EL == EL1 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.GCSEn == '0' then
        UNDEFINED;
    elsif EL2Enabled() &&
IsFeatureImplemented(FEAT_FGT) && (!HaveEL(EL3) ||
SCR_EL3.FGTEn == '1') && HFGWTR_EL2.nGCS_EL1 == '0'
then
        AArch64.SystemAccessTrap(EL2, 0x18);
```

```
    elsif HaveEL(EL3) && SCR_EL3.GCSEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    elsif EL2Enabled() && HCR_EL2.<NV2,NV1,NV> ==
'111' then
        NVMem[0x8D0] = X[t, 64];
    else
        GCSCR_EL1 = X[t, 64];
elsif PSTATE.EL == EL2 then
    if Halted() && HaveEL(EL3) && EDSCR.SDD == '1'
&& boolean IMPLEMENTATION_DEFINED "EL3 trap priority
when SDD == '1'" && SCR_EL3.GCSEn == '0' then
        UNDEFINED;
    elsif HaveEL(EL3) && SCR_EL3.GCSEn == '0' then
        if Halted() && EDSCR.SDD == '1' then
            UNDEFINED;
        else
            AArch64.SystemAccessTrap(EL3, 0x18);
    elsif HCR_EL2.E2H == '1' then
        GCSCR_EL2 = X[t, 64];
    else
        GCSCR_EL1 = X[t, 64];
elsif PSTATE.EL == EL3 then
    GCSCR_EL1 = X[t, 64];
```

28/03/2023 16:02; 72747e43966d6b97dcbd230a1b3f0421d1ea3d94