[v13,12/12] KVM: x86: Disable Intel PT when VMXON in L1 guest

10654375 | diff (/patch/10654375/raw/) | mbox (/patch/10654375/mbox/) | series (/series/34463/mbox/)

Message ID	1540368316-12998-13-git-send-email-luwei.kang@intel.com
State	New
Headers	show
Series	Intel Processor Trace virtualization enabling
Related	show

Commit Message

Kang, Luwei (/project/kvm/list/?submitter=168537) Oct. 24, 2018, 8:05 a.m. UTC

```
Currently, Intel Processor Trace do not support tracing in L1 guest
VMX operation(IA32_VMX_MISC[bit 14] is 0). As mentioned in SDM,
on these type of processors, execution of the VMXON instruction will
clears IA32_RTIT_CTL.TraceEn and any attempt to write IA32_RTIT_CTL
causes a general-protection exception (#GP).

Signed-off-by: Luwei Kang <luwei.kang@intel.com>
---
 arch/x86/kvm/vmx.c | 8 +++++++-
 1 file changed, 7 insertions(+), 1 deletion(-)
```

Patch

10654375 | diff (/patch/10654375/raw/) | mbox (/patch/10654375/mbox/) | series (/series/34463/mbox/)

```
diff --git a/arch/x86/kvm/vmx.c b/arch/x86/kvm/vmx.c
index ed247dd..5001049 100644
--- a/arch/x86/kvm/vmx.c
+++ b/arch/x86/kvm/vmx.c
@@ -4556,7 +4556,8 @@  static int vmx_set_msr(struct kvm_vcpu *vcpu, struct msr_data *msr_info)
                break;
        case MSR_IA32_RTIT_CTL:
                if ((pt_mode != PT_MODE_HOST_GUEST) ||
-                       vmx_rtit_ctl_check(vcpu, data))
+                       vmx_rtit_ctl_check(vcpu, data) ||
+                       vmx->nested.vmxon)
                        return 1;
                vmcs_write64(GUEST_IA32_RTIT_CTL, data);
                pt_set_intercept_for_msr(vmx, !(data & RTIT_CTL_TRACEEN));
@@ -8760,6 +8761,11 @@  static int handle_vmon(struct kvm_vcpu *vcpu)
        if (ret)
                return ret;

+       if (pt_mode == PT_MODE_HOST_GUEST) {
+               vmx->pt_desc.guest.ctl = 0;
+               pt_set_intercept_for_msr(vmx, 1);
+       }
+
        return nested_vmx_succeed(vcpu);
 }
```