vmcb

vmcb的全称是Virtual machine control block，简单说就是控制虚拟机的一堆register。

因为一般在电脑上可以同时跑多个虚拟机，所以其实这VMCB是存储在system memory空间上的，通过一个MSR指出其baseaddr，然后从该baseaddr开始映射为VMCB.

The VMCB is divided into two areas:

- —the first one contains various control bits including the intercept vector，占用1024byte，
- the second one contains saved guest state.

其中第二个区域，save state area又可分为两种:

- 当 SEV-ES is not enabled时,从baseaddr 的400h地址开始。
- 当 SEV-ES is enabled时, 由 VMCB Save State Pointer指定save state area起始地址。

地址信息：

SEV-ES， -- VMCB 090h

VMCB Save State Pointer，-- VMCB 108h