**虚拟地址空间**

**本文内容**

1. [用户空间和系统空间](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/virtual-address-spaces#user-space-and-system-space)
2. [分页缓冲池和非分页缓冲池](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/virtual-address-spaces#paged-pool-and-nonpaged-pool)
3. [相关主题](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/virtual-address-spaces#related-topics)

处理器在读取或写入内存位置时使用虚拟地址。 在这些操作期间，处理器将虚拟地址转换为物理地址。

使用虚拟地址访问内存有几个好处：

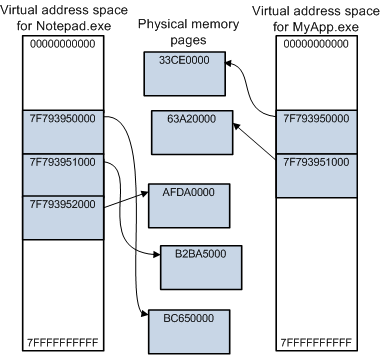
* 程序可以使用连续的虚拟地址范围来访问物理内存中的大型非连续内存缓冲区。
* 程序可以使用一系列虚拟地址来访问大于可用物理内存的内存缓冲区。 当物理内存不足时，内存管理器将物理内存页 (通常) 4 KB 保存到磁盘文件。 系统根据需要在物理内存和磁盘之间移动数据或代码页。
* 不同进程使用的虚拟地址是隔离的。 一个进程中的代码无法更改另一个进程或操作系统正在使用的物理内存。

进程可用的虚拟地址范围称为进程的 *虚拟地址空间*。 每个[用户模式进程](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode)都有其各自的专用虚拟地址空间。

* 32 位进程的虚拟地址空间通常位于 2 GB 范围内，0x00000000 0x7FFFFFFF。
* 64 位 Windows 上的 64 位进程的虚拟地址空间在 128 TB 范围内，0x000'000000000 到 0x7FFF'FFFFFFFF。

一系列虚拟地址有时称为一系列“虚拟内存” 。 有关详细信息，请参阅 [内存和地址空间限制](https://learn.microsoft.com/zh-cn/windows/win32/memory/memory-limits-for-windows-releases#memory-and-address-space-limits)。

下图演示了虚拟地址空间的一些关键功能。



该图显示了两个 64 位进程的虚拟地址空间：Notepad.exe 和 MyApp.exe。 每个进程都有自己的虚拟地址空间，范围从 0x000'0000000 到 0x7FF'FFFFFFFF。 每个阴影块都表示虚拟内存或物理内存的一个页（大小为 4 KB）。 记事本进程使用三个连续页面的虚拟地址，从 0x7F7'93950000 开始。 但是，这三个连续的虚拟地址页映射到物理内存中的不连续页面。 此外，这两个进程都使用从 0x7F7'93950000 开始的虚拟内存页，但这些虚拟页映射到物理内存的不同页。

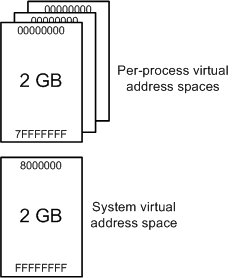
**用户空间和系统空间**

诸如 Notepad.exe 和 MyApp.exe 的进程在用户模式下运行。 核心操作系统组件和多个驱动程序在更有特权的内核模式下运行。 有关处理器模式的详细信息，请参阅[用户模式和内核模式](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode)。

每个用户模式进程都有其各自的专用虚拟地址空间，但在内核模式下运行的所有代码都共享称为“系统空间” 的单个虚拟地址空间。 用户模式进程的虚拟地址空间称为“用户空间” 。

### 在 32 位 Windows 中，可用的虚拟地址空间共计为 2^32 字节（4 GB）。

通常，较低的 2 GB 用于用户空间，而上 2 GB 用于系统空间。



在 32 位 Windows 中，可以在启动时指定 (，) 超过 2 GB 可用于用户空间。 但是，这意味着可用于系统空间的虚拟地址更少。 可以将用户空间的大小增加到 3 GB，系统空间仅保留 1 GB。 若要增大用户空间的大小，请使用 [**BCDEdit /set increaseuserva**](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/devtest/bcdedit--set)。

在 64 位 Windows 中，虚拟地址空间的理论大小为 2^64 字节（16 艾字节），但实际上仅使用 16 艾字节范围的一小部分。

在用户模式下运行的代码可以访问用户空间，但无法访问系统空间。 此限制可防止用户模式代码读取或更改受保护的操作系统数据结构。 在内核模式下运行的代码可以访问用户空间和系统空间。 也就是说，在内核模式下运行的代码可以访问系统空间和当前用户模式进程的虚拟地址空间。

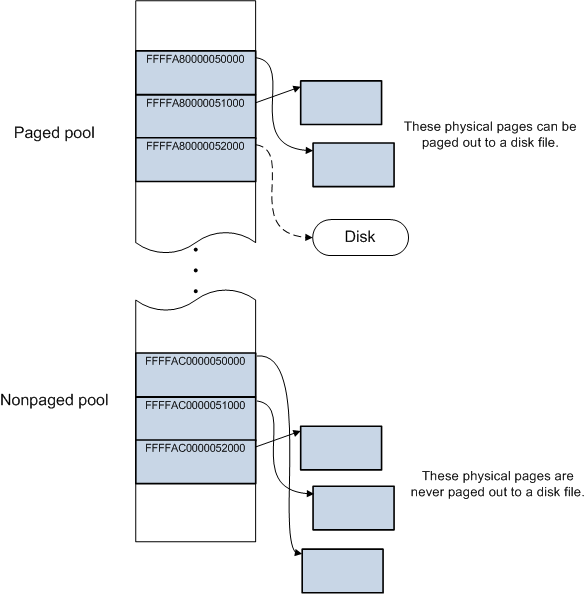
在内核模式下运行的驱动程序在直接读取或写入用户空间中的地址时必须小心。 以下方案说明了原因。

1. 用户模式程序发起从设备读取某些数据的请求。 程序提供用于接收数据的缓冲区的起始地址。
2. 内核模式下运行的设备驱动程序例程启动读取操作并将控制权返回给其调用程序。
3. 稍后，设备会中断当前运行的线程，以指示读取操作已完成。 内核模式驱动程序例程处理此任意线程（属于任意进程）上的中断。
4. 此时，驱动程序不得将数据写入用户模式程序在步骤 1 中提供的起始地址。 此地址位于发起请求的进程虚拟地址空间中，这可能与当前进程不同。

**分页缓冲池和非分页缓冲池**

在用户空间中，所有物理内存页面都可以根据需要调出到磁盘文件。 在系统空间中，某些物理页面可以分页，而其他物理页面则无法分页。 系统空间具有用于动态分配内存的两个区域：分页缓冲池和非分页缓冲池。

分页缓冲池中分配的内存可以根据需要调出到磁盘文件。 非分页缓冲池中分配的内存永远无法调出到磁盘文件。



**相关主题**

[设备节点和设备堆栈](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/device-nodes-and-device-stacks)

[用户模式和内核模式](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode)

0x0000000000000000~0x0000FFFFFFFFFFFF；  
内核模式地址的范围：0xFFFF000000000000~0xFFFFFFFFFFFFFFFF。  
此内核虚拟地址范围总计为 128 TB，但实际在使用的是8TB

X64 CPU 已经限制了虚拟地址中可用的比特数为 48 位，Windows 做出了进一步的限制，将其削减为 44 位。因而，能够存储这类数据结构的虚拟地址跨度被限制为 2^44 ，换言之，当前 64 位 Windows 的系统（内核）虚拟地址空间被限制为 8TB，即 0xFFFFF80000000000~0xFFFFFFFFFFFFFFFF。