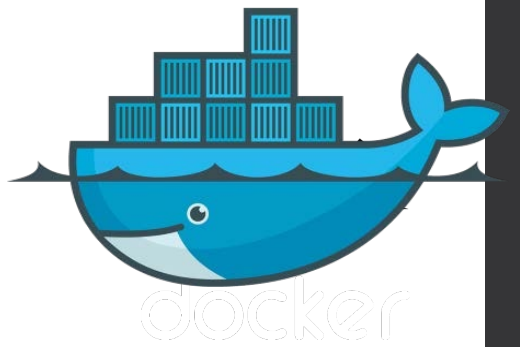

docker

Docker



- داکر یک پلتفرم نرم افزاری برای ساخت اپلیکیشن‌های مبتنی بر Container است. محیط‌های اجرایی کوچک و سبک که به طور مشترک از هسته سیستم عامل استفاده می‌کنند اما در عین حال در یک محیط ایزوله و کاملا جدا از هم قرار دارند. هر چند مفهوم containerیا نگهدارنده از مدت‌ها قبل در حوزه ITمطرح بود اما داکر به عنوان یک پروژه متن باز در سال ۲۰۱۳ معرفی و عرضه شد. در واقع داکر باعث شدcontainer جان تازه ای بگیرد و دوباره محبوب شود

Linux kernel

کانتینر، یک یا چند پراسس ایزوله‌شده و بدون سربار اضافی است که منابع اختصاص‌داده شده به خودش را مصرف می‌کند. درواقع بجای ایزوله‌کردن در لایه‌ی hypervisor، ایزوله‌سازی در سطح کرنل انجام می‌شود

این ایزوله سازی در لینوکس به واسطه دو ویژگی مهم کرنل

A. Namespaces

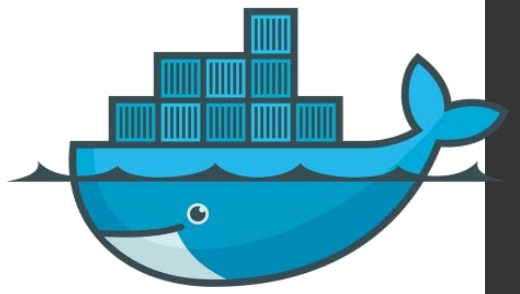
B. Linux Control Groups (cgroups)

انجام می شود.

namespace

Cgrupe

Namespace



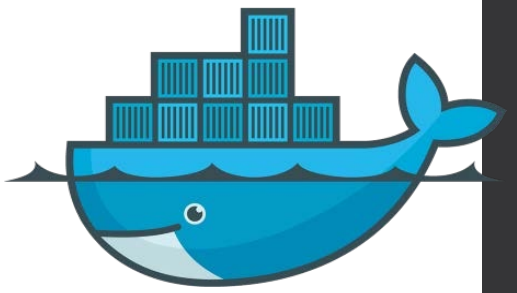
- در لینوکس، Namespaceها باعث می‌شوند که هر پراسس نگاه (Viewخودش را به سیستم داشته باشد، این «زاویه‌ی دید» شامل فایل‌ها، پردازنده، Hostname، اینترفیس شبکه و مواردی از این قبیل است.
- لینوکس بطور پیش‌فرض یک Namespaceدارد که همه منابع سیستم مانند PIDها، UserIDها، اینترفیس‌های شبکه و ... به آن Namespaceتعلق دارند.
- می‌توان Namespaceهای مختلفی را ایجاد و منابع سیستم را برای آن‌ها مدیریت کرد. همچنین اجرای پراسس در آن Namespaceها امکان‌پذیر بوده، بگونه‌ای که پراسس تنها منابع مربوط به آن Namespaceرا مشاهده می‌کند.

Type of namespace

- Mount (mnt)
- UNIX Time-sharing System (uts)
- Interprocess Communication (ipc)
- Process ID (pid)
- Network (net)
- User ID (user)
- Time

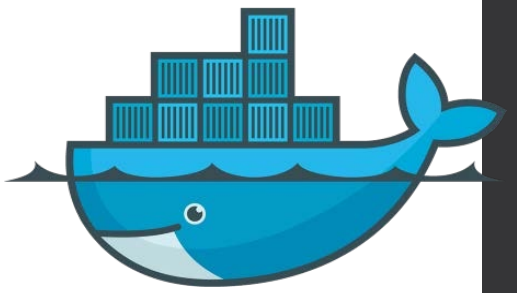
mnt	مانت پوینت ها را برای هر process ایزوله می کند.
pid	هر process id را ایزوله می کند
ipc	این فضای نام System V IPC, POSIX message queues را ایزوله می‌کند
net	دستگاه های شبکه،جداول روتینگ،iptables ها را ایزوله می کند
uts	مقدارhostname را ایزوله می کند
user	آیدی های یوزر ها و گروه هارا ایزوله می‌کند
cgroups	فایل و دایرکتوری مرتبط با cgroup هارو ایزوله می‌کند
time	ساعت های monotonicو boot را ایزوله می کند

Cgrupe

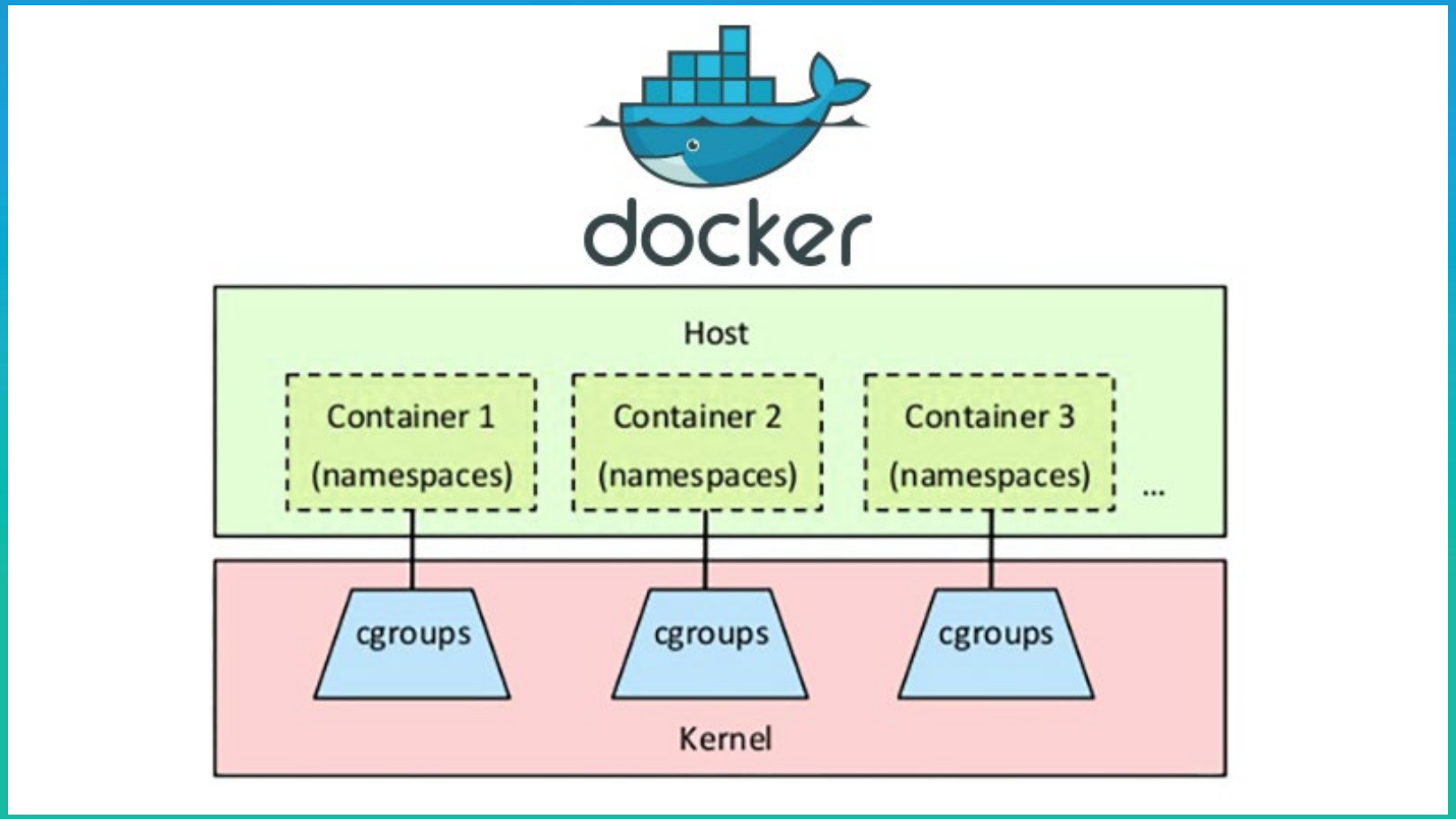


- گروه‌های کنترلی یا Linux Control Groups (cgroups)دومین ویژگی‌ای است که لینوکس برای ایزوله‌کردن کانتینرها بکار می‌گیرد. Cgroupیکی از ویژگی های کرنل لینوکس بوده و محدودیت منابع مصرفی کانتینر و پراسس (یا گروهی از پراسس‌ها) را مشخص می‌کند. پراسس نمی‌تواند بیش از آنچه که بدان اختصاص داده شده است را مصرف کند. همانطور که پراسس‌های دو سیستم مجزا نمی‌توانند منابع یکدیگر را مصرف کنند، این محدودیت منابع نیز باعث می‌شود که پراسس اجازه مصرف منابع سایر پراسس‌ها را نداشته باشد.
- این قابلیت از نسخه ۲.۶.۲۴ در سال ۲۰۰۸ به کرنل اضافه شده است

Type of Cgrupe



- CPU: برای محدود کردن منابع پردازشی مانند زمان پردازش و تعداد هسته‌های مورد استفاده توسط گروه فرآیند.
- Memory: برای محدود کردن مصرف حافظه توسط گروه فرآیند، مانند حداکثر حافظه قابل استفاده و حداکثر حافظه قابل تخصیص.
- I/O: برای کنترل و محدود کردن دسترسی و سرعت ورودی/خروجی دستگاه‌ها برای گروه فرآیند.
- Network: برای محدود کردن پهنای باند و تنظیم قوانین شبکه برای گروه فرآیند.
- Device: برای محدود کردن دسترسی به دستگاه‌ها توسط گروه فرآیند، مانند محدود کردن دسترسی به دستگاه‌های USBیا دستگاه‌های شبکه.
- Freezer: برای تعلیق و از سرگیری گروه فرآیند در حالت تعلیق.
- Perf: برای اندازه‌گیری و نمایش عملکرد سیستم و فرآیندها.


docker
Host
Container 1
(namespaces)
Container 2
(namespaces)
Container 3
(namespaces)
...
cgroups
cgroups
cgroups
Kernel

sudo docker run -it --memory="1g" nginx

```
root@amin-PC:/home/amin/Downloads/namespace# sudo docker run --name mylimit5 -it -d -p8454:80 --memory=512m nginx
9e6a6c8f1ad3f7a561fcfe74745f8994627c246b764b809f906b88dc6c5232b3
root@amin-PC:/home/amin/Downloads/namespace# sudo docker container inspect mylimit5 | grep -i memory
            "Memory": 536870912,
            "MemoryReservation": 0,
            "MemorySwap": 1073741824,
            "MemorySwappiness": null,
root@amin-PC:/home/amin/Downloads/namespace#
```

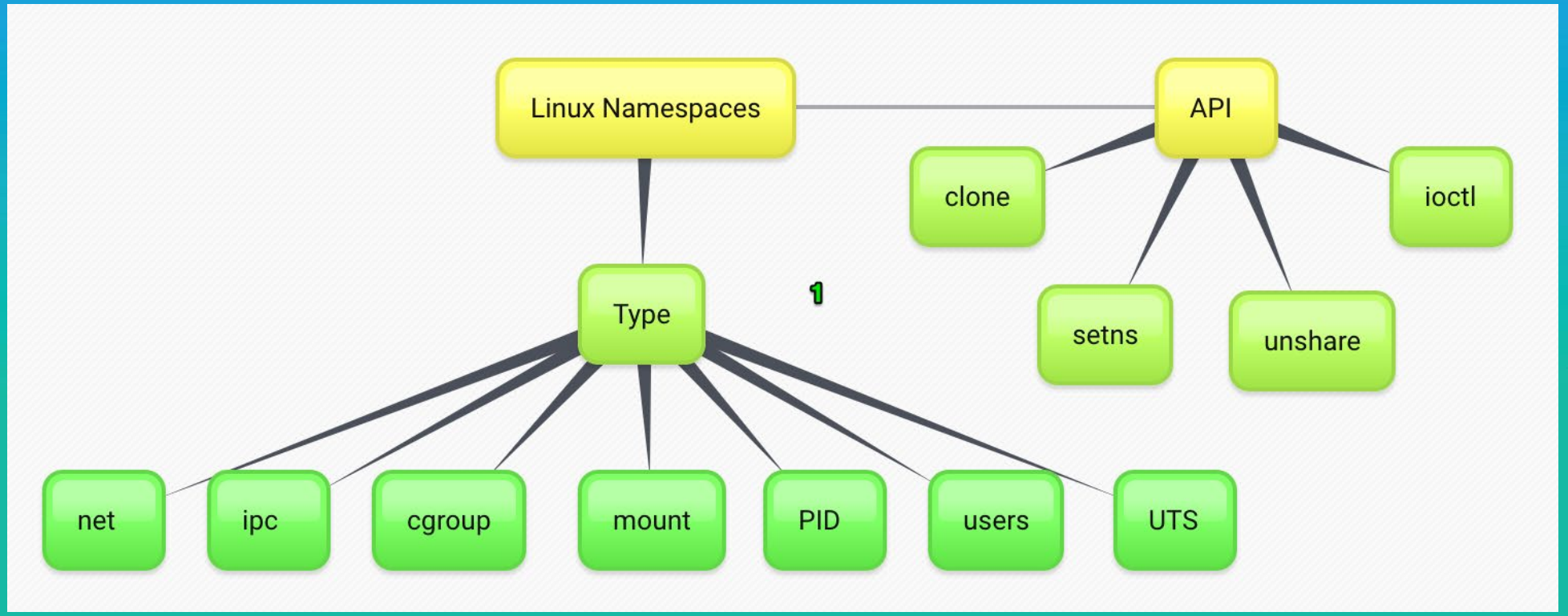
Kernel Syscalls

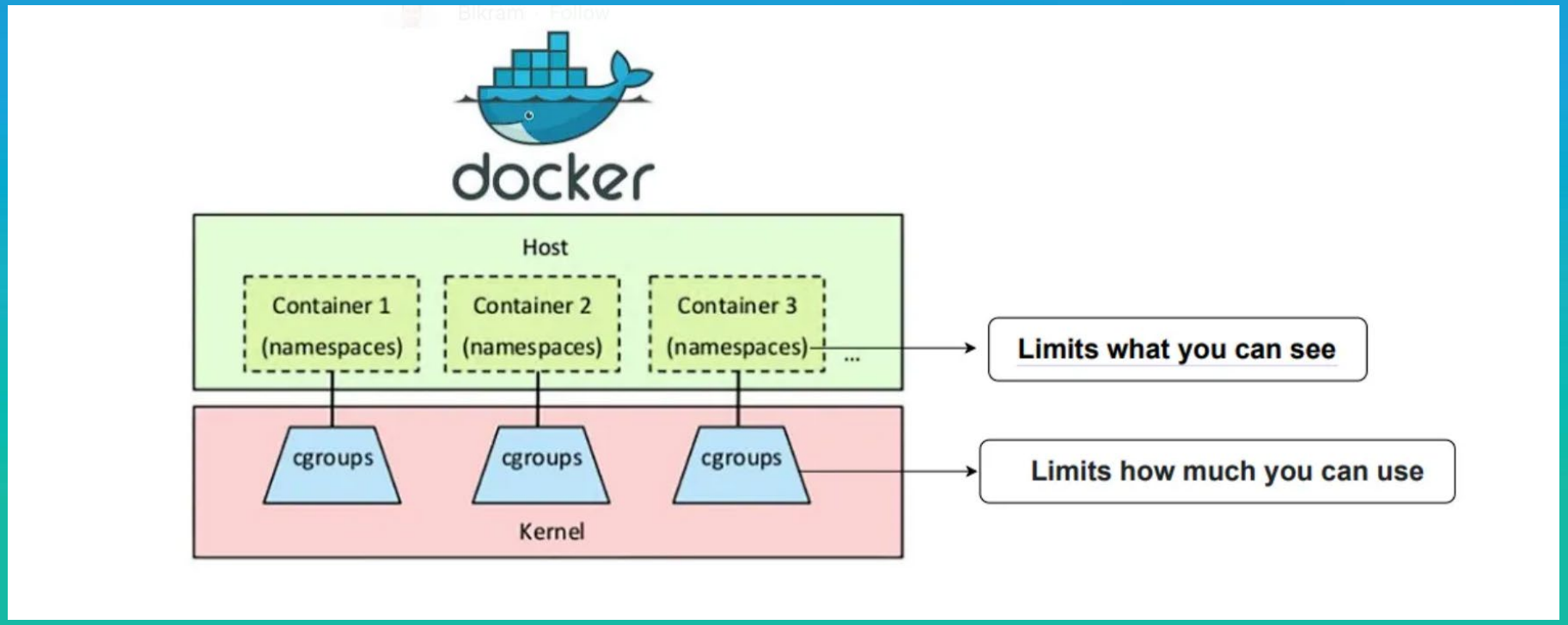
1) **clone** ایجاد process جدید داخل ns

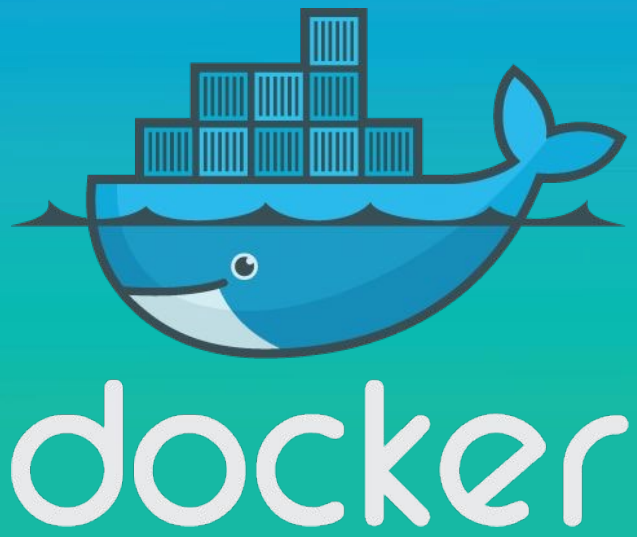
2) **Setns** به یک process اجازه جا به جایی میان ns های موجود را می دهد.

3) **unshare** ایجاد ns جدید و انتقال پراسس فراخوانی شده به آن فضا

4) **ioctl**دریافت اطلاعات درباره یک ns


Linux Namespaces
API
clone
ioctl
Type
1
setns
unshare
net
ipc
cgroup
mount
PID
users
UTS


docker
Host
Container 1
(namespaces)
Container 2
(namespaces)
Container 3
(namespaces)
...
cgroups
cgroups
cgroups
Kernel
Limits what you can see
Limits how much you can use


docker