Docker入门教程（五）Docker安全

【编者的话】DockOne组织翻译了Flux7的Docker入门教程，本文是系列入门教程的第五篇，介绍了Docker的安全问题，依然是老话重谈，入门者可以通过阅读本文快速了解。

我们必须高度重视开源软件的安全问题，当开发者在使用Docker时，从本地构建应用程序到生产环境部署是没有任何差异的（译者注：作者的言外之意是更应该重视Docker的安全问题）。当Docker被越来越多的平台使用的时候，我们需要严格保证Docker作为一个项目或者平台的安全性。

因此，我们决定在Docker系列教程的第五篇来讨论Docker安全性的相关问题以及为什么会它们影响到Docker的整体安全性。由于Docker是LXC的延伸，它也很容易使用LXC的安全特性。

在本系列的第一篇文章中，我们知道`docker run`命令可以用来运行容器。那运行这个命令后，Docker做了哪些具体的工作呢？具体如下：

1. `docker run`命令初始化。
2. Docker 运行 lxc-start 来执行run命令。
3. lxc-start 在容器中创建了一组namespace和Control Groups。

对于那些不知道namespace和control groups的概念的读者，我在这里先给他们解释一下：namespace是隔离的第一级，容器是相互隔离的，一个容器是看不到其它容器内部运行的进程情况（译者注：namespace系列教程可以阅读DockerOne上的系列教程）。每个容器都分配了单独的网络栈，因此一个容器不可能访问另一容器的sockets。为了支持容器之间的IP通信，您必须指定容器的公网IP端口。

Control Groups是非常重要的组件，具有以下功能：

- 负责资源核算和限制。
- 提供CPU、内存、I/O和网络相关的指标。
- 避免某种DoS攻击。
- 支持多租户平台。

Docker Daemon的攻击面

Docker Daemon以root权限运行，这意味着有一些问题需要格外小心。
下面介绍一些需要注意的地方：

- 当Docker允许与访客容器目录共享而不限制其访问权限时，Docker Daemon的控制权应该只给授权用户。
- REST API支持Unix sockets，从而防止了cross-site-scripting攻击。
- REST API的HTTP接口应该在可信网络或者VPN下使用。
- 在服务器上单独运行Docker时，需要与其它服务隔离。

一些关键的Docker安全特性包括：

1. 容器以非特权用户运行。
2. Apparmor、SELinux、GRSEC解决方案，可用于额外的安全层。
3. 可以使用其它容器系统的安全功能。

Docker.io API

用于管理与授权和安全相关的几个进程，Docker提供REST API。以下表格列出了关于此API用于维护相关安全功能的一些命令。

Purpose	Command
Add a user	`GET /api/v1.1/users/:username/`
Update user information	`PATCH /api/v1.1/users/:username/`
List emails for the user	`GET /api/v1.1/users/:username/emails/`
Delete a user	`DELETE /api/v1.1/users/:username/emails/`