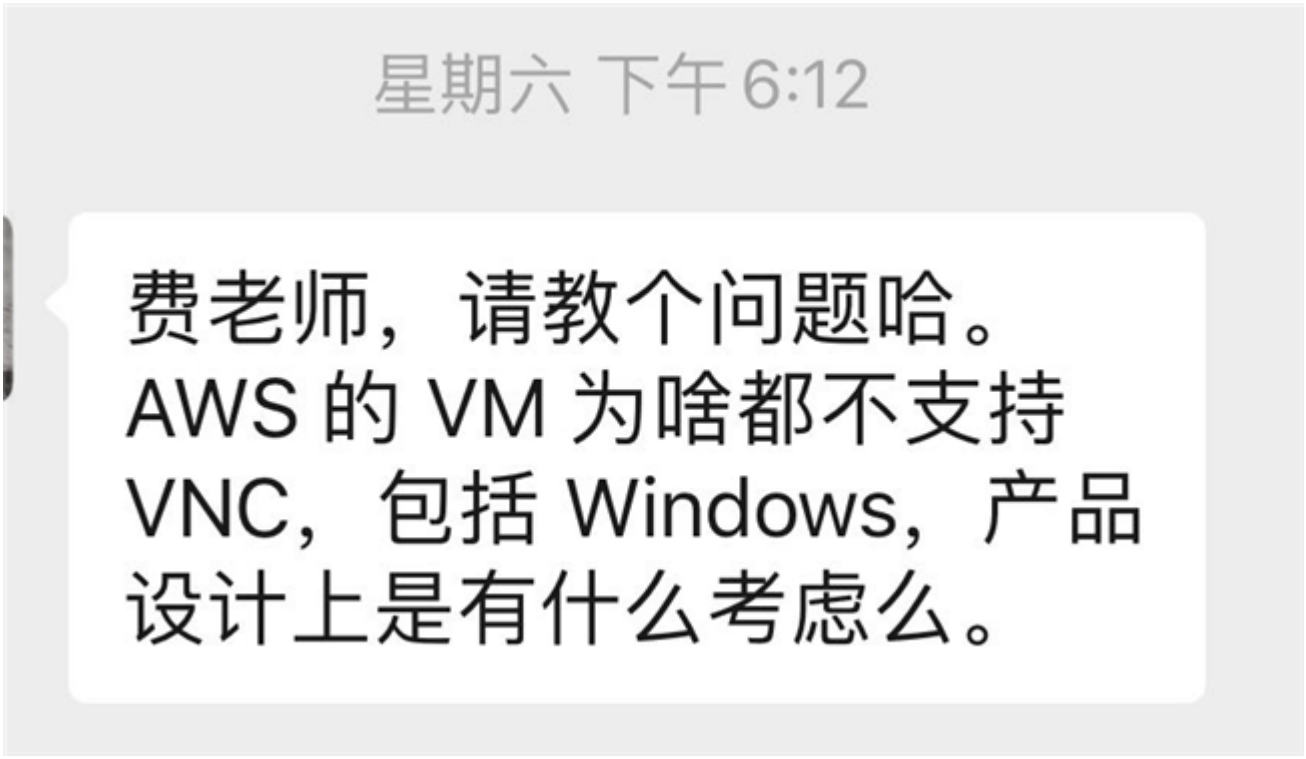
亚马逊AWS官方博客

VNC 还是 RDP? 云上的远程桌面究竟该如何选

by AWS Team | on 29 JUN 2020 | in Security, Identity, & Compliance | Permalink | Share

可以说写下这个题目完全是我临时起意，起因是微信上的一个讨论而引出的思考。话说在上个周末，我在微信上收到了朋友发来的一个问题 –



讲真，我现在很害怕人家以老师相称，也很害怕有人问我技术问题。尤其是现在的“后浪”们思维敏捷，丝毫不惧“前浪”。敷衍且没有深度的答案，注定惹人耻笑。不过，关于 VNC 的这个问题，刚好我在去年有过一些了解。也就有了一吐为快的念头，于是信手写下了这篇博客。

这里说的VNC是什么?

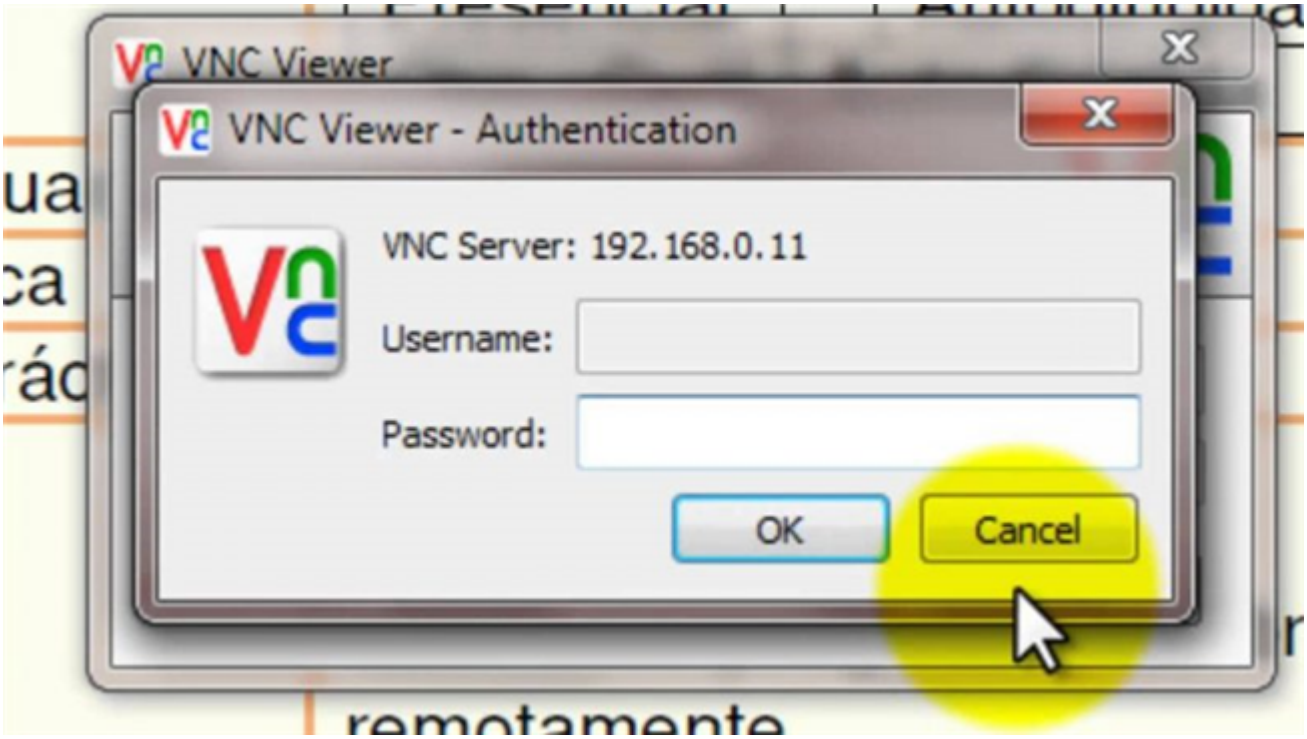
简单来说，所谓的 VNC（Virtual Network Computing ）是一种图形化的桌面共享系统，它使用远程帧缓冲协议 (RFB) 来远程控制另一台计算机。它将键盘和鼠标事件从一台计算机传输到另一台计算机，通过网络向另一个方向转发图形屏幕更新。

类似这样的技术VNC不是绝无仅有，但VNC 的流行和普及却因为其具有的过人之处 –

- VNC是平台无关的—— 有多种客户端和服务器的实现，几乎涵盖了所有的主流平台。甚至一些VNC的实现被称“无客户端”，这是因为不需要安装插件或客户端软件而，而是依靠HTML5技术，只需要一个浏览器就可以访问远程桌面了。
- VNC 是开源的—— VNC最初是在英国剑桥的Olivetti & Oracle研究实验室开发的。原始的VNC源代码和许多现代的衍生品在GNU通用公共许可证下是开放源码的。
- VNC的协议是简单、普适的—— VNC使用的是 RFB(Remote Framebuffer) 协议。这是一个开放且简单的协议。因为它在framebuffer级别工作，协议是基于像素的所以适用于所有窗口系统和应用程序，包括Microsoft Windows、macOS和X Window系统。这个协议的性能表现是很出色的。

说起来满满的都是优点，那么

访问云上的实例，为什么不选择VNC呢?



VNC 的优点很多，很多场景下都能看到VNC。例如，访问树莓派的桌面，对 headless 服务器的管理等等。但是，对于云上实例的远程图形化的访问VNC却不是好的选择。考虑到我们的使用场景是通过互联网来访问云上的主机，这就引出了否定 VNC 最主要的原因– 安全性。

默认情况下，RFB并不是一个安全的协议。虽然这个协议下密码不以明文方式发送，但如果能从网络中嗅出加密密钥和已编码的密码，还是有可能破解成功的。因此，建议密码至少有8个字符。另一方面，VNC的一些版本也有8个字符的限制； 如果发送的密码超过8个字符，则删除多余的字符，并将截断的字符串与密码进行比较。

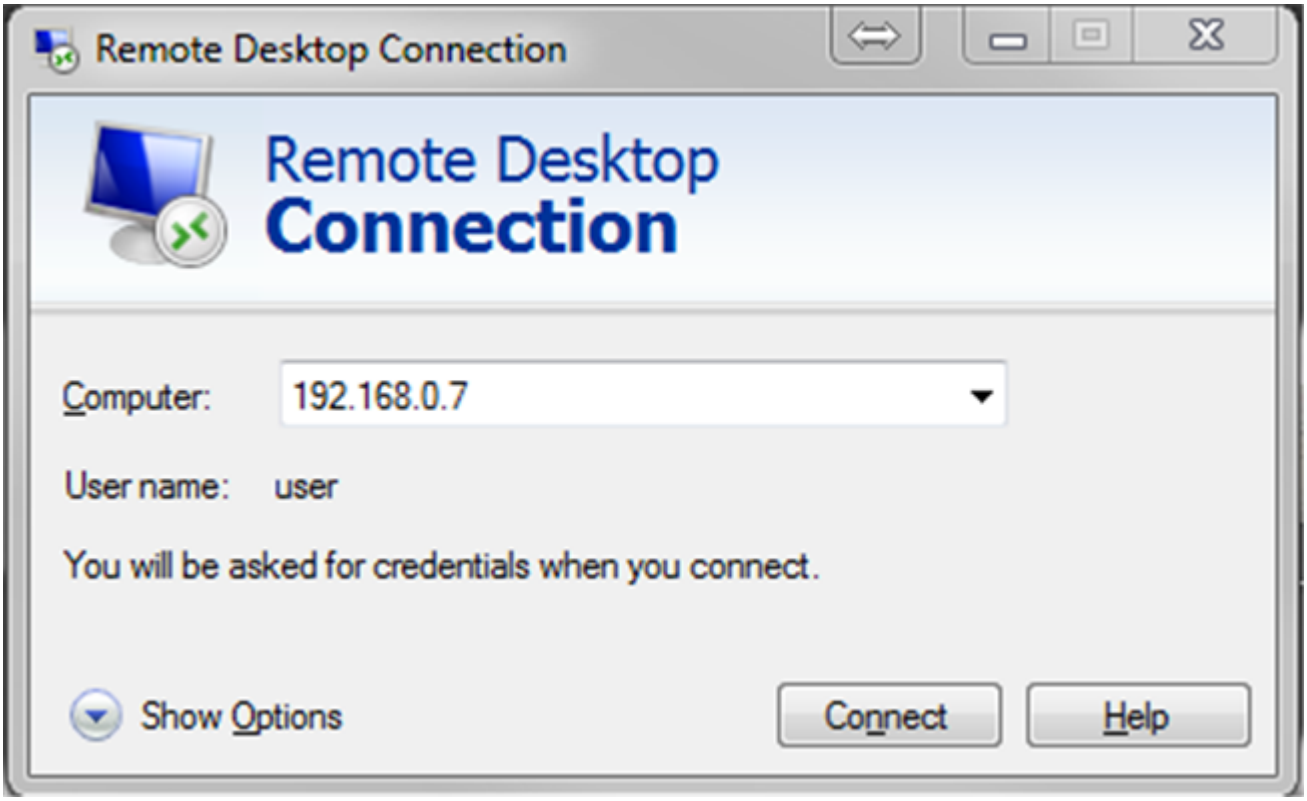
在VNC生态系统中，”Big Four” 指的是LibVNC、UltraVNC、Tight VNC和TurboVNC 这四家提供VNC 产品的厂商。2019年，Kaspersky Lab 的研究人员对这四家公司进行了审计，以了解它们的安全性。他们的发现是令人失望的。总的来说，研究人员发现这四个程序的客户端和服务器部分共有37个严重缺陷。其中22个在 UltraVNC，另外10个在 LibVNC, 4个在 TightVNC，还有一个在 TurboVNC，但这是一个严重的漏洞，它会让攻击者在服务器端远程执行代码。

有人会建议通过 SSH 或 VPN 连接进行 VNC 的隧道化，通过这种方法增加一个具有更强加密功能的额外安全层。但是这种方法并不完美，除了增加了复杂性也容易引起其它的一些安全问题，例如中间人攻击等。

否定一个技术是简单的，但我们是否有替代技术呢？答案就是 Remote Desktop Protocol （RDP）。

那么，RDP 又是什么?

有过 Windows 使用经验的人对于远程桌面（Remote Desktop Protocol ，RDP）一定不会陌生。RDP 是由微软公司开发的一种专有协议，它为用户提供了通过网络连接到另一台计算机的图形界面。在使用上，用户需要使用 RDP 客户端软件，而在远程另一台计算机则需要运行 RDP 服务器软件。



微软的Windows、Linux、macOS、iOS、Android等操作系统都有客户端。Windows操作系统内置RDP服务器；Linux与macOS 可以安装一个 RDP 服务器。缺省配置下，服务器监听 TCP 端口 3389 和 UDP 端口 3389。

微软目前把他们的官方RDP客户端软件称为Remote Desktop Connection，以前叫做 “Terminal Services client”

与VNC 相比，RDP的安全性有很大的提升。主要的安全特性包括了：

- 128位加密，使用RC4加密算法（版本6加入）
- 提供了对TLS的支持（版本2加入）

此外，正如前面提到的VNC协议是基于像素的。尽管这带来了极大的灵活性，可以显示任何类型的桌面，但它的效率往往不如那些更好地理解底层图形布局(例 如： X11)或桌面(例如：RDP)的解决方案。这些协议以更简单的形式(例如：打开窗口)发送图形原语或高级命令，而 VNC 的 RFB 协议尽管支持压缩但只能是发送原始像素数据。

如何使用RDP?

在 Windows 环境下使用RDP是再简单不过的事情。我想谈的是在 Linux 环境下RDP 的安装部署与使用。虽然微软公司没有为 Linux 提供 RDP 的软件，但是我们可以使用开源的xRDP，这是RDP协议在Linux平台 的实现。

xRDP是一个开源的远程桌面协议服务器，它用来实现Linux接受来自 Windows、Mac 或者 Linux 远程桌面客户端或的连接。这意味着你不需要在我们所使用的 Windows 或 macOS 机器上安装额外的第三方应用程序。

Linux 安装 xRDP的方法如下。这里我以 Ubuntu 20.04 为例 –

- 安装Gnome

GNOME是一个Linux 操作系统下的桌面环境，完全由免费和开源软件组成。缺省情况下在EC2上安装的Linux 操作系统都不包含Gnome，需要额外安装。Ubuntu 缺省的桌面窗口管理器就是Gnome，用以下命令安装。

```
$ sudo apt update
$ sudo apt install ubuntu-desktop
```

除了Gnome 以外，我们还可以选择 LXDE、Xface 等等。相比之下，LXDE 是轻量级的窗口管理器，Xface 则具备类似 Windows 界面的风格。如果不在乎额外增加的大约 5GB 的磁盘存储的开销，我还是推荐使用Gnome。原因在于这与我们本地使用的 Ubuntu 具有一致性的体验。

- 安装 xRDP

```
$ sudo apt install -y xrdp
```

安装完成后，xRDP服务将自动启动。可以通过这个命令来检查其状态:

```
$ sudo systemctl status xrdp
```

输出结果如下:

```
lines 2-24/24 (END)
● xrdp.service - xrdp daemon
     Loaded: loaded (/lib/systemd/system/xrdp.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2020-06-15 19:24:04 CST; 1 day 23h ago
       Docs: man:xrdp(8)
             man:xrdp.ini(5)
    Process: 712 ExecStartPre=/bin/sh /usr/share/xrdp/socksetup (code=exited, status=0/SUCCESS)
    Process: 725 ExecStart=/usr/sbin/xrdp $XRDP_OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 734 (xrdp)
      Tasks: 2 (limit: 37755)
     Memory: 25.7M
     CGroup: /system.slice/xrdp.service
             ├─  734 /usr/sbin/xrdp
             └─14501 /usr/sbin/xrdp
```

- 接下来，要为Linux的用户（ubuntu）设置登录密码

```
$ sudo passwd ubuntu
$ sudo adduser ubuntu ssl-cert
```

这里设置的密码将被用来登录到目标的 EC2 实例，出于安全的理由务必使其符合密码安全的策略。第二条命令是将 用户 ubuntu 加入到 ssl-cert 用户组中。这是因为默认情况下，xRDP 使用的是自签发的证书，这个证书保存在 /etc/ssl/private/ssl-cert-snakeoil目录下。证书的密钥文件只能由 “ssl-cert” 用户组的成员读取。

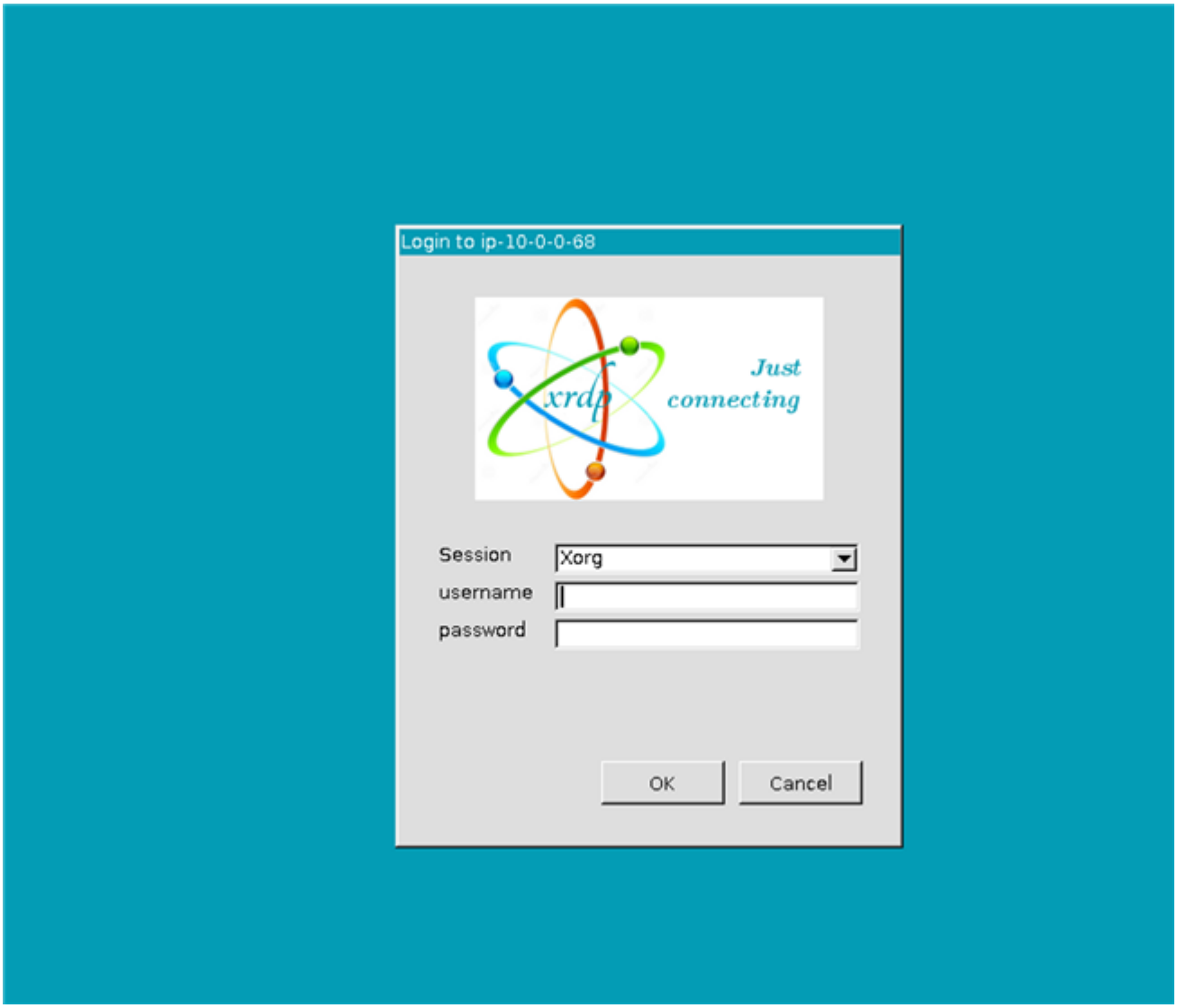
此外，如果我们的 EC2 实例绑定了Elastics IP 并且拥有自己的域名，我推荐使用Let’s Encrypt 发出的免费SSL证书替换缺省的自签发的证书。需要注意的一点，Let’s Encrypt 证书的有效期是90天。可以考虑配置crontab 使用cerbot 自动更新证书。

- 修改安全组 RDP 协议缺省使用3389端口。务必记得在EC2的安全组中打开TCP与UDP在这个端口上的访问许可。

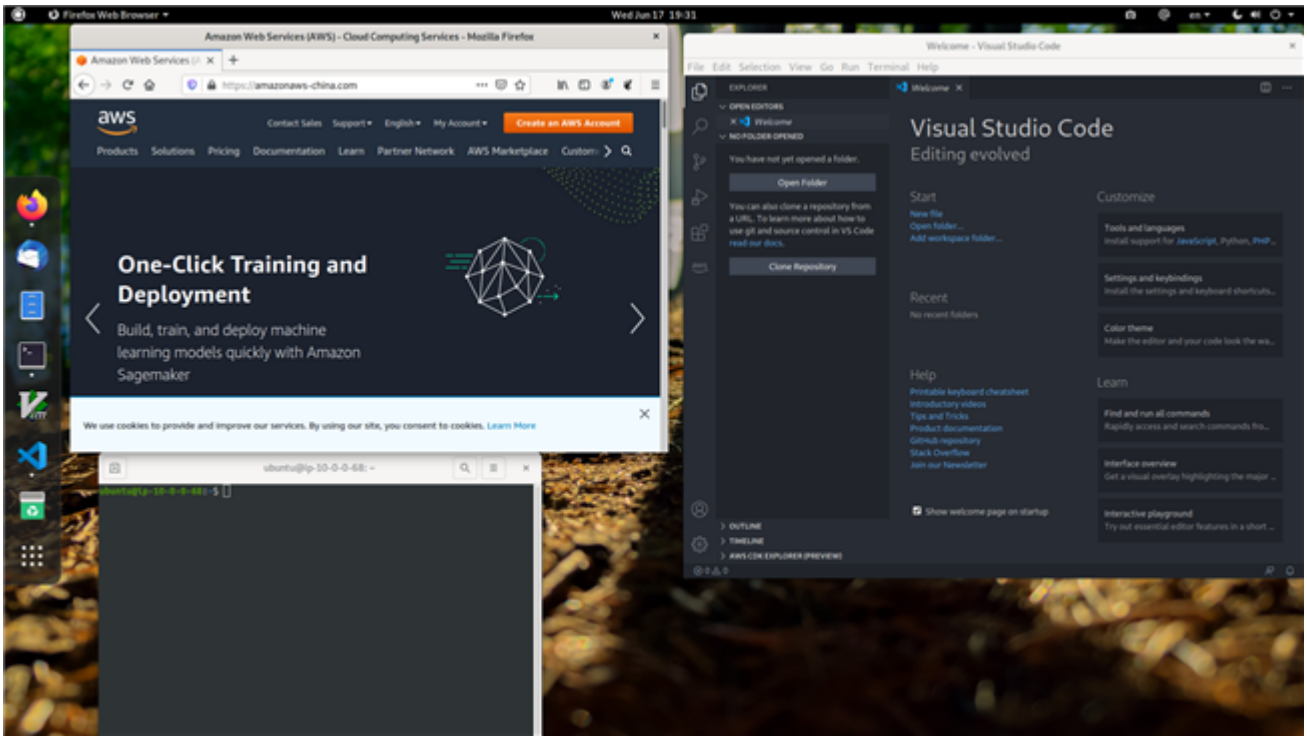
Inbound rules Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-
SSH	TCP	22	::/0	-
Custom UDP	UDP	3389	0.0.0.0/0	-
Custom UDP	UDP	3389	::/0	-
RDP	TCP	3389	0.0.0.0/0	-
RDP	TCP	3389	::/0	-

- 登录



在这里，username 输入ubuntu，password 输入刚刚修改过的用户密码。成功登录之后熟悉的Ubuntu 桌面就会立刻出现在眼前。



按照我的体验，网络延迟在35ms以内xRDP 的与本地Linux 桌面的操作体验几乎没有差别。实测之下，通过我所使用的100M联通宽带访问AWS 中国（北京）区域的EC2 实例，网络延迟大约在5ms左右。

```
lianghon@f01898507da0:[~]: ping 52.81.64.173 -c5
PING 52.81.64.173 (52.81.64.173): 56 data bytes
64 bytes from 52.81.64.173: icmp_seq=0 ttl=49 time=4.812 ms
64 bytes from 52.81.64.173: icmp_seq=1 ttl=49 time=4.912 ms
64 bytes from 52.81.64.173: icmp_seq=2 ttl=49 time=4.587 ms
64 bytes from 52.81.64.173: icmp_seq=3 ttl=49 time=5.558 ms
64 bytes from 52.81.64.173: icmp_seq=4 ttl=49 time=5.124 ms

--- 52.81.64.173 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.587/4.999/5.558/0.329 ms
```

单以鼠标、键盘的使用体验而论，本地桌面与远程桌面的差别已经微乎其微了，我终于可以放心的将许多工作移到云端。无论是通过我的笔记本电脑、iPad 甚至是一台树莓派都能够让我接入顺利的接入远程桌面。如此一来，开发在云端岂不是再简单不过的事情了。

最近有很多朋友在读过文章以后愿意与我进行进一步的讨论。如果你们有这样的想法不妨发邮件给我，我的邮箱是 lianghon@amazon.com。

本篇作者