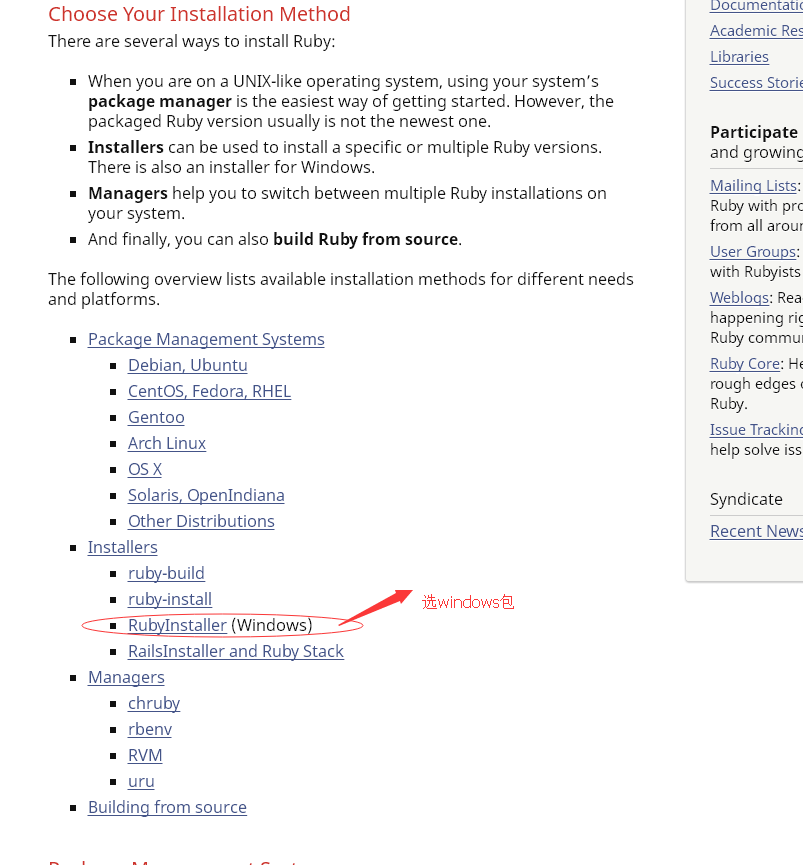
# Windows 快速搭建ruby环境

## 下载ruby软件

（1）下载软件

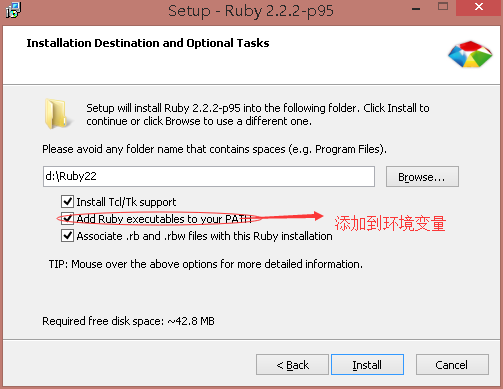
下载地址：<http://www.ruby-lang.org/en/documentation/installation/#rubyinstaller>



地址2：<http://rj.baidu.com/soft/detail/22711.html?ald>



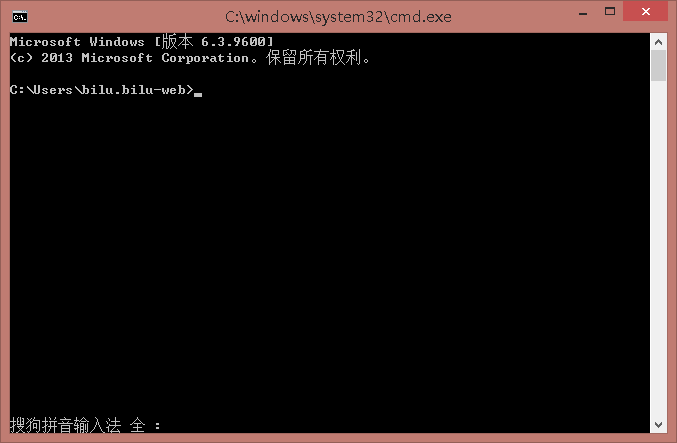
1. 安装时注意添加到环境变量



其他步骤next

## 关键步骤到了，gem换源

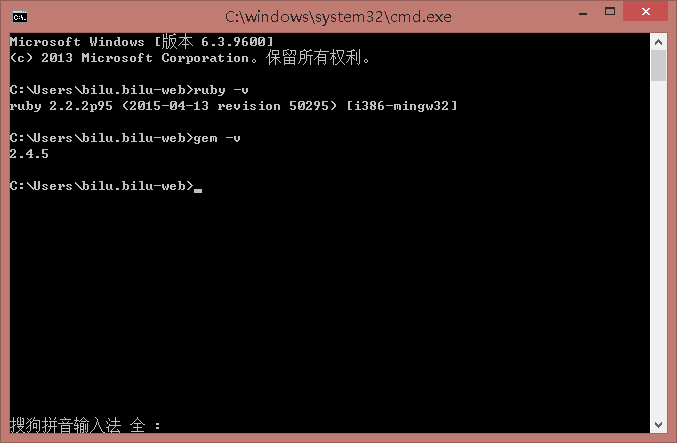
1.win+r 快捷键，输入cmd 调出命令提示符



1. 输入命令

ruby -v 回车

gem -v 回车



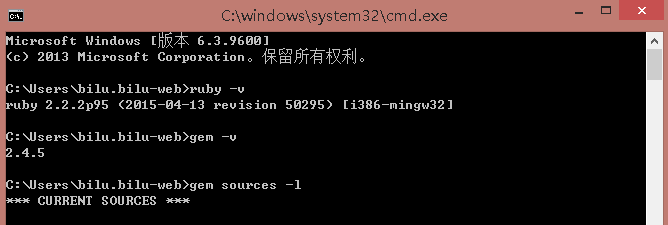
如果你的ruby环境安装正常，就会显示如上图的版本号，

1. gem的镜像源配置，或者换镜像源

输入命令：

gem sources -l

检查gem的来源，会出现如图信息



我这里sources目录下面没有镜像源

所以我需要添加镜像源，目前国内知名的镜像源有

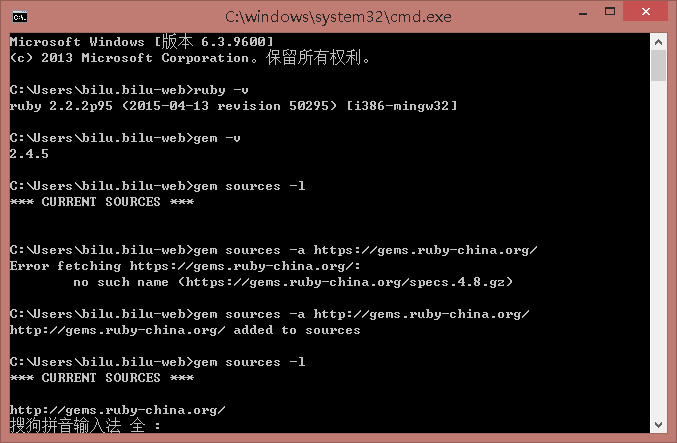
1.<https://gems.ruby-china.org>/

2.<https://ruby.taobao.org/>

这里我以第一个镜像源为例

执行命令

gem sources -a http://gems.ruby-china.org/



大家可能有个疑问，为什么用的http://而不是https://

其实就是因为这个原因我才写下此文档的，

当我用gem sources -a https://gems.ruby-china.org/去安装镜像源时，无数次的报错，然我束手无策，

查找无数百度，都是用的https,在我不断死磕到底的精神下，总算把问题的原因，查找出来了，

真是我被ta虐千百遍，依然待他如初恋啊！

这里又涉及到http协议的知识了，在下方有详细的解释

## http协议知识

HTTPS和HTTP的概念和区别

浏览：19002|更新：2013-11-20 23:05

一键约师傅

百度师傅高质屏和好师傅，拯救你的碎屏机

HTPPS和HTTP的概念

HTTPS（全称：Hypertext Transfer Protocol over Secure Socket Layer），是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。 它是一个URI scheme（抽象标识符体系），句法类同http:体系。用于安全的HTTP数据传输。https:URL表明它使用了HTTP，但HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层（在HTTP与TCP之间）。这个系统的最初研发由网景公司进行，提供了身份验证与加密通讯方法，现在它被广泛用于万维网上安全敏感的通讯，例如交易支付方面。

超文本传输协议 (HTTP-Hypertext transfer protocol) 是一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。

HTTPS和HTTP的区别：

https协议需要到ca申请证书，一般免费证书很少，需要交费。http是超文本传输协议，信息是明文传输，https 则是具有安全性的ssl加密传输协议http和https使用的是完全不同的连接方式用的端口也不一样,前者是80,后者是443。http的连接很简单,是无状态的HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议 要比http协议安全HTTPS解决的问题：1 . 信任主机的问题. 采用https 的server 必须从CA 申请一个用于证明服务器用途类型的证书. 改证书只有用于对应的server 的时候,客户度才信任次主机. 所以目前所有的银行系统网站,关键部分应用都是https 的. 客户通过信任该证书,从而信任了该主机. 其实这样做效率很低,但是银行更侧重安全. 这一点对我们没有任何意义,我们的server ,采用的证书不管自己issue 还是从公众的地方issue, 客户端都是自己人,所以我们也就肯定信任该server.2 . 通讯过程中的数据的泄密和被窜改1. 一般意义上的https, 就是 server 有一个证书.a) 主要目的是保证server 就是他声称的server. 这个跟第一点一样.b) 服务端和客户端之间的所有通讯,都是加密的.i. 具体讲,是客户端产生一个对称的密钥,通过server 的证书来交换密钥. 一般意义上的握手过程.ii. 加下来所有的信息往来就都是加密的. 第三方即使截获,也没有任何意义.因为他没有密钥. 当然窜改也就没有什么意义了.2. 少许对客户端有要求的情况下,会要求客户端也必须有一个证书.a) 这里客户端证书,其实就类似表示个人信息的时候,除了用户名/密码, 还有一个CA 认证过的身份. 应为个人证书一般来说上别人无法模拟的,所有这样能够更深的确认自己的身份.b) 目前少数个人银行的专业版是这种做法,具体证书可能是拿U盘作为一个备份的载体.HTTPS 一定是繁琐的.a) 本来简单的http协议,一个get一个response. 由于https 要还密钥和确认加密算法的需要.单握手就需要6/7 个往返.i. 任何应用中,过多的round trip 肯定影响性能.b) 接下来才是具体的http协议,每一次响应或者请求, 都要求客户端和服务端对会话的内容做加密/解密.i. 尽管对称加密/解密效率比较高,可是仍然要消耗过多的CPU,为此有专门的SSL 芯片. 如果CPU 信能比较低的话,肯定会降低性能,从而不能serve 更多的请求.ii. 加密后数据量的影响. 所以，才会出现那么多的安全认证提示

HTTPS网站对百度和谷歌SEO有什么影响？

从“site”中我们可以看见百度只收录http，尽管做了301跳转；谷歌方面则收录了2个不同版本的页面，很明确的指明了我的主域名是哪个版本。另外收录情况也是大大不用。再看看它们在搜索结果里面的情况。

google SERP 28

baidu SERP 500…

现在就可以清楚的知道：https对google是没有丝毫影响的，不管是排名或者是收录。但是在baidu就明显行不通了，完全不收录https的站点，更别说排名。假如baidu没有发现你的http版本，那就是：抱歉，没有找到与“XX”相关的网页，就算是做了301，但是一个做了301的页面拿什么跟做了优化的对手网站竞争？

有时候一个网站因商业要求等先天条件必须要用到加密协议怎么办?

你主要市场的SE不支持https那一切都等于白搭了。所以最好清楚目标SE是什么态度，比如google那么你就可以不用理会了。

但是对于百度呢？

怎么处理或者避免这种情况发生置之不理。

一、直接复制一个http版本，https首页301到http

如一些特殊的网站，登陆后显示加密内容假如引用首页的话，可以在目录下复制一个首页，全部调用此目录，有需要可以在robots文件屏蔽掉。

二、站内外的链接一致采用http，有需要可以将之前的链接进行修改。

三、SE重新识别