HTTPS建设使用的方案教程解析

时间：2018-02-01 文章来源：马海祥博客 访问次数：54 收藏到： 0

随着网络不断融入日常生活和工作当中，网络安全问题一直都是一个不能忽略的问题。据CNCERT监测发现，2015年网页仿冒、拒绝服务攻击等已经形成成熟地下产业链的威胁仍然呈现增长趋势，针对中国网站的仿冒页面（URL链接）191699个，较2014年增长85.7%，涉及IP地址20488个，较2014年增长199.4%。网页篡改、网站后门等攻击事件层出不穷，党政机关、科研机构、重要行业单位网站依然是黑客组织攻击特别是APT攻击的重点目标。2015年被植入后门的中国网站数量为75028个，较2014年增长86.7%，其中政府网站为3514个，较2014年增长130%。

2014年底，百度已对部分地区开放HTTPS加密搜索服务，随后，百度实行全站化HTTPS安全加密服务，百度HTTPS安全加密已覆盖主流浏览器，旨在用户打造了一个更隐私化的互联网空间、加速了国内互联网的HTTPS化。同时也希望更多网站加入到HTTPS的队伍中来，为网络安全贡献一份力量。在此，我向大家详细介绍一下HTTPS，后续还会有更详细深入的方案教程推出，各位敬请期待。

一、HTTPS是什么?

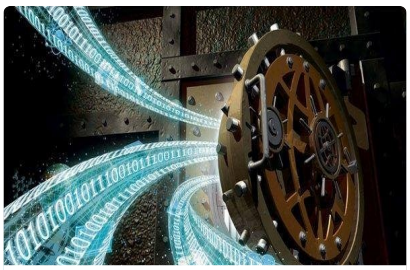
HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer），是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。

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。

分类目录

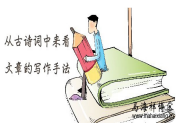
SEO新闻	SEO思维
移动端SEO	SEO问答
医疗SEO	淘宝SEO
企业SEO	站外SEO
网站设计	交互设计
网站策划	网页制作
营销策划	营销案例
竞价技巧	数据分析
写作技巧	微信微博
自媒体	新媒体
内容营销	网站运营
O2O模式	App运营
产品运营	网赚教程
创新思维	电子商务
名人访谈	创业故事

热点推荐


详解内存数据库中的索引技术




运营思维 更多>>

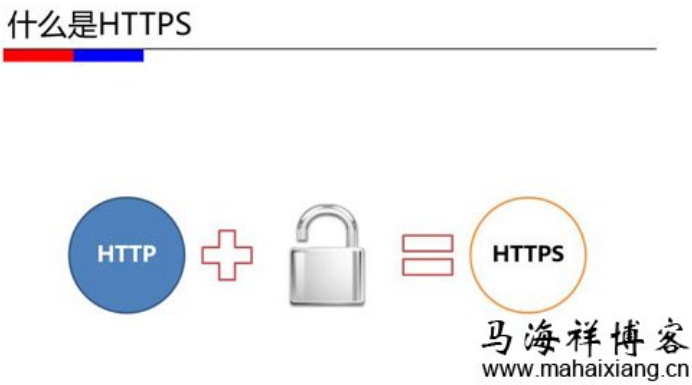


从古诗词中来看文章的写作手法

立即访问

教你写出提高客户转化率的6个文案策略

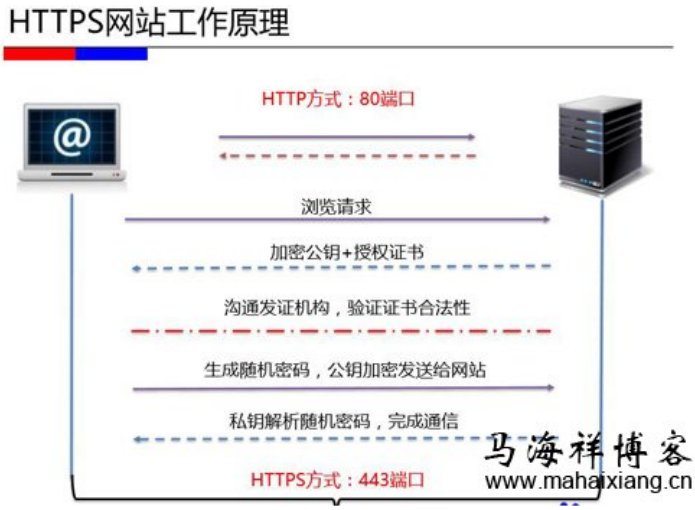
立即访问



传统的HTTP模式，存在着大量的灰色中间环节，相关信息很容易被窃取，但HTTPS却是通过认证用户与服务器，将数据准确地发送到客户机与服务器，并采用加密方式以防数据中途被盗取，大大降低了第三方窃取信息、篡改冒充身份的风险（具体可查看马海祥博客《HTTP与HTTPS的区别》的相关介绍）。

二、HTTPS安全原理解析

HTTPS主要由有两部分组成：HTTP + SSL / TLS，也就是在HTTP上又加了一层处理加密信息的模块。服务端和客户端的信息传输都会通过TLS进行加密，所以传输的数据都是加密后的数据。HTTPS与HTTP的原理区别可以观察下图：



HTTP工作原理：

①、客户端的浏览器首先要通过网络与服务器建立连接，该连接是通过TCP来完成的，一般TCP连接的端口号是80。 建立连接后，客户机发送一个请求给服务器，请求方式的格式为：统一资源标识符（URL）、协议版本号，后边是MIME信息包括请求修饰符、客户机信息和许可内容。

②、服务器接到请求后，给予相应的响应信息，其格式为一个状态行，包括信息的协议版本号、一个成功或错误的代码，后边是MIME信息包括服务器信息、实体信息和可能的内容。

HTTPS的工作原理：

①、客户端将它所支持的算法列表和一个用作产生密钥的随机数发送给服务器；

②、服务器从算法列表中选择一种加密算法，并将它和一份包含服务器公用密钥的证书发送给客户端；该证书还包含了用于认证目的的服务器标识，服务器同时还提供了一个用作产生密钥的随机数；

③、客户端对服务器的证书进行验证(有关验证证书，可以参考数字签名)，并抽取服务器的公用密钥；然后，再产生一个称作pre_master_secret的随机密码串，并使用服务器的公用密钥对其进行加密(参考非对称加/解密)，并将加密后的信息发送给服务器；

④、客户端与服务器端根据pre_master_secret以及客户端与服务器的随机数值独立计算出加密和MAC密钥(参考DH密钥交换算法)。

⑤、客户端将所有握手消息的MAC值发送给服务器；

⑥、服务器将所有握手消息的MAC值发送给客户端。

HTTPS的数据加密性：

HTTPS中数据的保密性主要是通过加密完成的。加密算法一般分为两种，一种是非对称加密（也叫公钥加密），另外一种是对称加密（也叫密钥加密）。

HTTPS使用非对称加解密主要有两个作用，一个是密钥协商，另外可以用来做数字签名。所谓密钥协商简单说就是根据双方各自的信息计算得出双方传输内容时对称加解密需要使用的密钥。如下图：

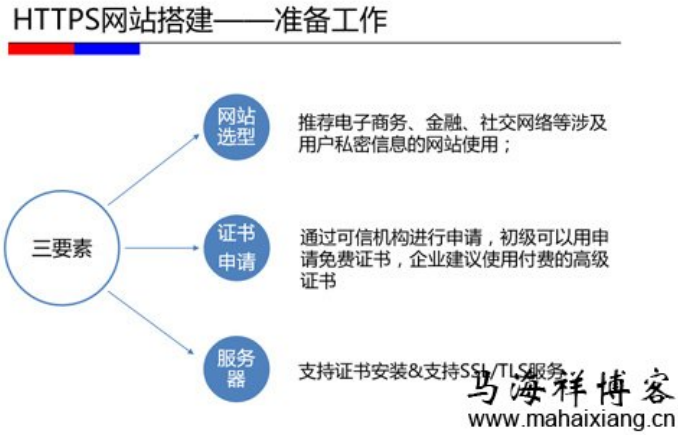
对称加密就是加密和解密都使用的是同一个密钥。如下图：

HTTS多次握手和复杂的加密机制有效的加大了网站的安全性，加密机制与认证机制可以减少网站被劫持和假冒的风险！

三、搭建HTTPS网站的准备工作

简单来说，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，所以HTTPS网站搭建中比较重要的内容都是围绕着SSL证书进行的。

那我们应该做什么准备工作，如下图：



网站选型：

HTTPS会提升网站安全性，同样也拉高技术成本，所以我们建议一些涉及到用户隐私信息的网站进行HTTPS建设，公开性的内容是根据网站自身情况进行选择；

证书申请：

①、CSR文件制作：申请SSL证书之前，需要制作CSR文件，CSR，Certificate Signing Request，是制作SSL 证书的必要步骤。一个 CSR 文件中描述了 SSL 证书持有人的信息（如个人姓名或公司名称）、联系地址等，用于验证 SSL 证书和域名是同一个人持有，以确保网站的合法性。制作完成后向 SSL 证书提供商上传这个文件，以获得最终的 SSL 证书。

在申请服务器证书时，不要出现某些特殊字符，否则在您提交CSR后，会出现"105"的错误代码。这个错误是由于在您生成CSR时，输入的信息中包含一些特殊字符，如：(@,#,&,!,等等，例如：您可以将"&"用"and"代替)。

在您生成CSR时，公用名（Common Name）是必须填写的，但许多客户填写这一项时，经常填错或不符合标准。

公用名（Common Name） 是您的主机名+域名，比如：www.mahaixiang.cn的服务器证书是颁发给某一台主机的，而不是一个域，您的公用名（Common Name）必须与您要使用服务器证书的主机的全名完全相同，因为www.domain.com与domain.com是不同的。

要生成CSR文件，你必须为服务器创建一对密钥对。密钥对和证书是不可分开的，一旦您遗失了公钥、私钥或密码，重新生成密钥对后，和原来的证书就不匹配了。如果您申请的是全球信SSL证书，可以重新提交CSR免费重发证书；如果您申请的是闪快SSL证书，就必须重新付费申请证书（具体可查看马海祥博客《HTTP、SSL/TLS和HTTPS协议的区别与联系》的相关介绍）。

②、CA认证证书申请：将CSR提交给CA，CA一般有2种认证方式：

a、域名认证：一般通过对管理员邮箱认证的方式，这种方式认证速度快，但是签发的证书中没有企业的名称;

b、企业文档认证：需要提供企业的营业执照。

也有需要同时认证以上2种方式的证书，叫EV ssl证书，这种证书可以使IE7以上的浏览器地址栏变成绿色，所以认证也最严格。

③、证书安装：

在收到CA的证书后，可以将证书部署上服务器，一般APACHE文件直接将KEY+CER复制到文件上，然后修改httpD.CONF文件;TOMCAT等，需要将CA签发的证书CER文件导入JKS文件后，复制上服务器，然后修改SERVER.XML;IIS需要处理挂起的请求，将CER文件导入。

鉴于对建站成本的考虑，需要高级别ssl 证书的往往是大中型网站，如网上银行、购物网站、金融证券、政府机构等，诸如个人博客之类的小型站点完全可以先尝试免费ssl证书。

服务器选购：

考虑到CSR和SSL证书与服务器的环境配置及功能支持有必不可分的联系，建议在再选购服务器之前做好充分的考虑。尤其是对服务器是否支持SSL功能，是否与证书匹配等

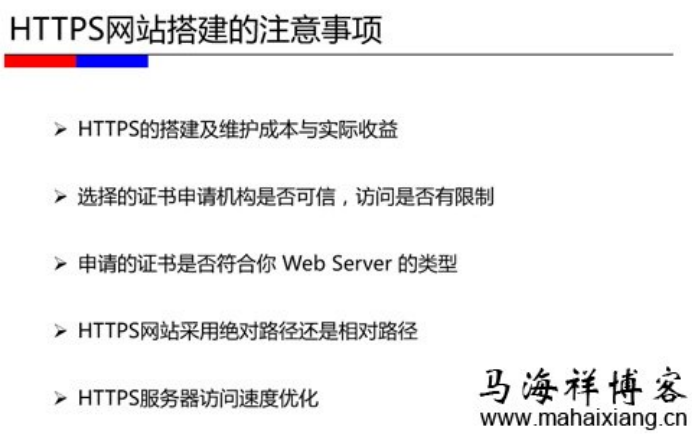
功能需要重视；

网站开发：

由于网站功能与开发语言各不相同，在这就不详细说明网站开发的准备工作了，HTTPS网站与HTTP网站在开发期间基本是一致的，只是使用协议不同。

四、HTTPS网站搭建中的注意事项

HTTPS网站的加密功能决定了在搭建过程中一定要注意一些问题：



1、衡量投入与产出：无论是做一个新的HTTPS站还是从HTTP转成HTTPS的网站，都需要投入硬件、软件、人力等新的成本，所以在未评估之前建议不要做；一旦做好，轻易不要关闭HTTPS网站倒退回HTTP，这种倒退行为很容易造成不利影响；

2、证书申请机构：在选择申请机构之前一定要考察核对该机构是否有可信资质，有些机构没有被国际机构认可（浏览器上会没有小绿锁），也有些机构在访问地域上有所限制，还有的机构出现过公钥泄露的情况，所以请慎重选择；

3、证书的选择：因为网站的开发语言、使用功能和服务器环境不同，证书的选择也不同，所以在选择时要考虑好需要什么证书，避免浪费成本；

4、网站路径方式：在HTTP网站上绝对路径和相对路径并没有明显的区别，但是在HTTPS和HTTP共存的情况如果使用绝对路径容易出现协议混淆的情况，如果混淆后可能会出现链接打不开，或者蜘蛛抓取失败等现象，这个应该十分注意！

5、服务器的访问速度：由于HTTPS多次握手的特性，网站速度是一定会受到影响的，所以在搭建网站的同时要注意网站速度的优惠，可以适当考虑使用CDN等产品。

五、网站要不要做HTTPS?

百度站长社区对于做不做HTTPS网站的问题进行了相关调研，如下图：

调研中发现，大多数人对HTTPS持观望态度，他们对HTTPS安全性是认可的，但是从各个层面进行考虑后，做出了目前不做HTTPS网站的决定，主要有以下两种观点：

正方观点

1、HTTPS具有更好的加密性能，避免用户信息泄露；

2、HTTPS复杂的传输方式，降低网站被劫持的风险；

3、搜索引擎已经全面支持HTTPS抓取、收录，并且会优先展示HTTPS结果；

4、从安全角度来说个人觉得要做HTTPS，不过HTTPS可以采用登录后展示；

5、HTTPS绿锁表示可以提升用户对网站信任程度；

6、基础成本可控，证书及服务器已经有了成型的支持方案；

7、网站加载速度可以通过cdn等方式进行弥补，但是安全不能忽略；

8、HTTPS是网络的发展趋势，早晚都要做；

9、可以有效防止山寨、镜像网站；

反方观点

1、HTTPS会降低用户访问速度，增加网站服务器的计算资源消耗；

2、目前搜索引擎只是收录了小部分HTTPS内容，应该保持观望制度；

3、HTTPS需要申请加密协议，增加了运营成本；

4、百度目前对HTTPS的优先展现效果不明显，谷歌较为明显；

5、技术门槛较高，无从下手；

6、目前站点不涉及私密信息，无需HTTPS；

7、兼容性有待提升，如robots不支持/联盟广告不支持等；

8、HTTPS网站的安全程度有限，该被黑还是被黑；

9、HTTPS维护比较麻烦，在搜索引擎支持HTTP的情况，没必要做HTTPS（具体可查看马海祥博客《从SEO的角度来分析网站是否该采用HTTPS协议》的相关介绍）。

六、HTTPS的优点与缺点

根据案例反馈，目前HTTPS的优缺点主要分布在三方面：

1、HTTPS的优点

安全性方面

在目前的技术背景下，HTTPS是现行架构下最安全的解决方案，主要有以下几个好处：

（1）、使用HTTPS协议可认证用户和服务器，确保数据发送到正确的客户机和服务器；

（2）、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，可防止数据在传输过程中不被窃取、改变，确保数据的完整性。

（3）、HTTPS是现行架构下最安全的解决方案，虽然不是绝对安全，但它大幅增加了中间人攻击的成本。

2、HTTPS的缺点

技术方面

（1）、相同网络环境下，HTTPS协议会使页面的加载时间延长近50%，增加10%到20%的耗电。此外，HTTPS协议还会影响缓存，增加数据开销和功耗。

（2）、HTTPS协议的安全是有范围的，在黑客攻击、拒绝服务攻击、服务器劫持等方面几乎起不到什么作用。

（3）、最关键的，SSL 证书的信用链体系并不安全。特别是在某些国家可以控制 CA 根证书的情况下，中间人攻击一样可行。

成本方面

（1）、SSL的专业证书需要购买，功能越强大的证书费用越高。个人网站、小网站可以选择入门级免费证书。

（2）、SSL 证书通常需要绑定 固定IP，为服务器增加固定IP会增加一定费用；

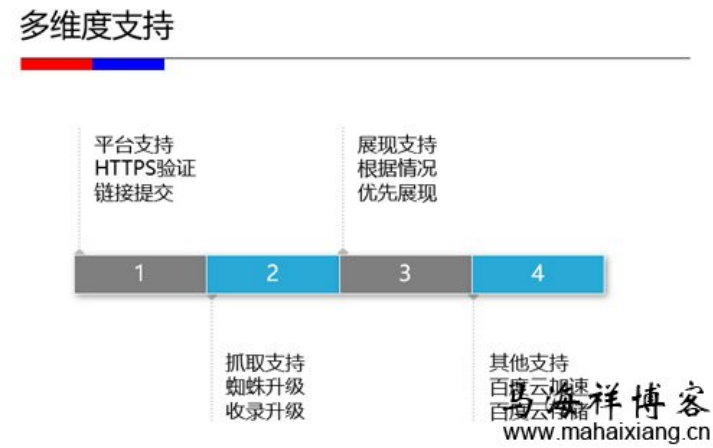
（3）、HTTPS 连接服务器端资源占用高较高多，相同负载下会增加带宽和服务器投入成本；

既然HTTPS有这么多缺点，那是不是就不该做呢，当然不是的，随着技术的发展很多缺点是可以优化和弥补的。比如：

打开速度问题完全可以通过CDN加速解决，很多IDC也在着手推出免费证书和一站式HTTPS搭建服务，HTTPS成本在未来将会大大缩小！

七、百度对HTTPS的支持

2015年5月25日，百度站长平台发布公告，宣布全面放开对https站点的收录，https站点不再需要做任何额外工作即可被百度抓收。处于HTTPS的安全性，百度对HTTPS一直持支持态度，为了提升百度搜索对HTTPS网站的友好度，特别进行了一系列升级。



站长平台：百度平台目前已经完美支持HTTPS验证,并为HTTPS准备了相应的数据提交接口，第一时间对HTTPS进行数据接收。

HTTPS站点如何在平台的验证

在平台添加HTTPS站点时，一定要带上https://进行验证，否则默认为http的站点；

百度搜索：目前Baidu Spider3.0已经顺利升级，可以正常抓取HTTPS内容，并进行正常的收录和索引，根据HTTPS网站的普及情况，还将会进行优先展示HTTPS结果等策略升级（具体可查看马海祥博客《百度升级HTTPS认证工具：优先抓取和展现HTTPS的链接》的相关介绍）。

其他支持：目前百度各方面也在全力支持HTTPS，已经推出HTTPS服务有百度开放云的CDN和云主机。

HTTS多次握手和复杂的加密机制有效的加大了网站的安全性，加密机制与认证机制可以减少网站被劫持和假冒的风险!

马海祥博客点评：

网站使用HTTPS需要申请安全证书，目前来说还是比较繁琐的，对小公司来说成本有些高。不过以后会越来门槛越低，可以申请一些免费的证书来部署，或者使用已经部署了HTTPS服务的建站工具来搭建网站，省去自己申请安全证书的麻烦。

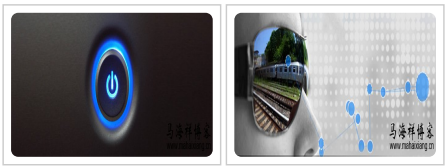
打赏

相关标签搜索： seo https

上一篇：基于眼球追踪技术对用户调研的探讨研究
下一篇：百亿级规模的日志系统架构设计及优化

相关文章推荐：

1 今日头条的个性化推荐算法
2 如何开启苹果系统的两步验证机制，避免
3 基于眼球追踪技术对用户调研的探讨研究
4 HTTP与HTTPS的区别
5 HTTPS建设使用的方案教程解析
6 HTTP服务的七层架构技术解析及运用
7 HTTP、SSL/TLS和HTTPS协议的区别与联系
8 自然语言处理的单词嵌入及表征方法



9 关于大型网站架构的负载均衡技术详解
10 深入解析互联网协议的原理


您可能还会对以下这些文章感兴趣！

详解大型网站系统的特点和架构演化发展历程

大型网站的挑战主要来自庞大的用户，高并发的访问和海量数据，任何简单的业务一旦需要处理数以P计的数据和面对数以亿计的用户，问题就会变得棘手，大型网站架构主要就是解决这类问题。大型网站不是从无到有一步就搭建好一个大型网站，而是能够伴随小型网站业务的渐进发……【查看全文】

阅读：853 关键词： 大型网站 网站架构 网站系

今日头条的个性化推荐算法

互联网给用户带来了大量的信息，满足了用户在信息时代对信息的需求，但也使得用户在面对大量信息时无法从中获得对自己真正有用的那部分信息，对信息的使用效率反而降低了，而通常解决这个问题最常规的办法是推荐系统。推荐系统能有效帮助用户快速发现感兴趣和高质量的信……【查看全文】

阅读：12908 关键词： 今日头条 日期：2016

HTTP服务的七层架构技术解析及运用

一般来说，计算机领域的体系结构普遍采用了分层的方式，从最底层的硬件往高层依次有：操作系统->驱动程序->运行库->系统程序->应用程序等等。从网络分层模型OSI来讲，由上至下为：应用层->表示层->会话层->传输层->网络层->数据链路层->物理层。当然实际应用的TCP/IP协……【查看全文】

阅读：4386 关键词： 七层架构解析 七层架构运用

HTTPS建设使用的方案教程解析

百度已对部分地区开放HTTPS加密搜索服务，随后，百度实行全站化HTTPS安全加密服务，百度HTTPS安全加密已覆盖主流浏览器，旨在用户打造了一个更隐私化的互联网空间、加速了国内互联网的HTTPS化。同时也希望更多网站加入到HTTPS的队伍中来，为网络安……【查看全文】

阅读：42 关键词： seo https 日期：2018-

HTTP、SSL/TLS和HTTPS协议的区别与联系

HTTPS是为了安全性而设置的，要验证很多的信息，相对应http请求的速度肯定有点慢，如果使用HTTPS的话很麻烦的，无意给服务器和客户端增加了很大的压力，所以平时最好不要使用HTTPS，如果牵扯到个人隐私或者是其他的什么重要信息就一定要这么做了，很多的时候你感觉有点问题，……【查看全文】

阅读：14035 关键词： http ssl https httpsh

计算机的开机启动原理

计算机从打开电源到开始操作，整个启动可以说是一个非常复杂的过程。总体来说，计算机的整个启动过程分成四个阶段：第一阶段：BIOS；第二阶段：主引导记录；第三阶段：硬盘启动；第四阶段：操作系统；直至执行/bin/login程序，跳出登录界面，等待用户输入用户名和密码。……【查看全文】

阅读：3039 关键词： 计算机 计算机启动 计算机

如何开启苹果系统的两步验证机制，避免iCloud帐号遭到攻击

首先，你需要登录至苹果的网页版Apple ID管理系统，你需要点击“管理你的Apple ID”，随后输入帐号密码信息。在登录之后，你需要从左侧导航栏中选择“密码和安全”选项，在这里，你将需要验证安全问题，随后下拉至“两步验证”区域，点击蓝色的“开始”链接并阅读其中的……【查看全文】

阅读：1407 关键词： 苹果系统 验证机制 icloud

关于大型网站架构的负载均衡技术详解

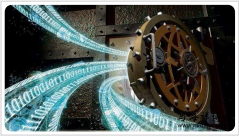
负载均衡是将负载（工作任务，访问请求）进行平衡、分摊到多个操作单元（服务器，组件）上进行执行，是解决高性能，单点故障（高可用），扩展性（水平伸缩）的终极解决方案。面对大量用户访问、高并发请求，海量数据，可以使用高性能的服务器、大型数据库，存储设备，高性能W……【查看全文】

阅读：809 关键词： 大型网站 网站架构 负载均

基于贝叶斯推断应用原理的过滤垃圾邮件研究

随着电子邮件的应用与普及，垃圾邮件的泛滥也越来越多地受到人们的关注。而目前正确识别垃圾邮件的技术难度非常大。传统的垃圾邮件过滤方法，主要有关键词法和校验码法等。前者的过滤依据是特定的词语；后者则是计算邮件文本的校验码，再与已知的垃圾邮件进行对比。它们……【查看全文】

阅读：855 关键词： 贝叶斯推断 贝叶斯应用 贝



详解内存数据库中的索引技术

传统的数据库管理系统把所有数据都放在磁盘上进行管理，所以称作磁盘数据库（DRDB:Disk-Resident Database），磁盘数据库需要频繁地访问磁盘来进行数据的操作，磁盘的读写速度远远小于CPU处理数据的速度，所以磁盘数据库的瓶颈出现在磁盘读写上，基于此，内存数据库的概……【查看全文】

阅读：3257 关键词： 内存数据库 索引技术 数据

↓ 点击查看更多 ↓