# java基础

https://github.com/Snailclimb/JavaGuide/blob/master/Java%E7%9B%B8%E5%85%B3/Java%E5%9F%BA%E7%A1%80%E7%9F%A5%E8%AF%86.md

## **多态**

在Java中有两种形式可以实现多态：继承（多个子类对同一方法的重写）和接口（实现接口并覆盖接口中同一方法）。

## **重载和重写的区别**

****重载：**** 发生在同一个类中，方法名必须相同，参数类型不同、个数不同、顺序不同，方法返回值和访问修饰符可以不同，发生在编译时。

****重写：**** 发生在父子类中，方法名、参数列表必须相同，返回值范围小于等于父类，抛出的异常范围小于等于父类，访问修饰符范围大于等于父类；如果父类方法访问修饰符为 private 则子类就不能重写该方法。

## **接口和抽象类的区别是什么**

1. 接口的方法默认是 public，所有方法在接口中不能有实现(Java 8 开始接口方法可以有默认实现），抽象类可以有非抽象的方法
2. 接口中的实例变量默认是 final 类型的，而抽象类中则不一定
3. 一个类可以实现多个接口，但最多只能实现一个抽象类
4. 一个类实现接口的话要实现接口的所有方法，而抽象类不一定
5. 接口不能用 new 实例化，但可以声明，但是必须引用一个实现该接口的对象 从设计层面来说，抽象是对类的抽象，是一种模板设计，接口是行为的抽象，是一种行为的规范。

## **成员变量与局部变量的区别**

1. 从语法形式上，看成员变量是属于类的，而局部变量是在方法中定义的变量或是方法的参数；成员变量可以被 public,private,static 等修饰符所修饰，而局部变量不能被访问控制修饰符及 static 所修饰；但是，成员变量和局部变量都能被 final 所修饰；
2. 从变量在内存中的存储方式来看，成员变量是对象的一部分，而对象存在于堆内存，局部变量存在于栈内存
3. 从变量在内存中的生存时间上看，成员变量是对象的一部分，它随着对象的创建而存在，而局部变量随着方法的调用而自动消失。
4. 成员变量如果没有被赋初值，则会自动以类型的默认值而赋值（一种情况例外被 final 修饰的成员变量也必须显示地赋值）；而局部变量则不会自动赋值。

## 常用类及方法

### String 和 StringBuffer、StringBuilder 的区别是什么 String 为什么是不可变的

****可变性****

简单的来说：String 类中使用 final 关键字字符数组保存字符串，private　final　char　value[]，所以 String 对象是不可变的。而StringBuilder 与 StringBuffer 都继承自 AbstractStringBuilder 类，在 AbstractStringBuilder 中也是使用字符数组保存字符串char[]value 但是没有用 final 关键字修饰，所以这两种对象都是可变的。

StringBuilder 与 StringBuffer 的构造方法都是调用父类构造方法也就是 AbstractStringBuilder 实现的，大家可以自行查阅源码。

AbstractStringBuilder.java

abstract class AbstractStringBuilder implements Appendable, CharSequence {

char[] value;

int count;

AbstractStringBuilder() {

}

AbstractStringBuilder(int capacity) {

value = new char[capacity];

}

****线程安全性****

String 中的对象是不可变的，也就可以理解为常量，线程安全。AbstractStringBuilder 是 StringBuilder 与 StringBuffer 的公共父类，定义了一些字符串的基本操作，如 expandCapacity、append、insert、indexOf 等公共方法。StringBuffer 对方法加了同步锁或者对调用的方法加了同步锁，所以是线程安全的。StringBuilder 并没有对方法进行加同步锁，所以是非线程安全的。

****性能****

每次对 String 类型进行改变的时候，都会生成一个新的 String 对象，然后将指针指向新的 String 对象。StringBuffer 每次都会对 StringBuffer 对象本身进行操作，而不是生成新的对象并改变对象引用。相同情况下使用 StirngBuilder 相比使用 StringBuffer 仅能获得 10%~15% 左右的性能提升，但却要冒多线程不安全的风险。

****对于三者使用的总结：****

1. 操作少量的数据 = String
2. 单线程操作字符串缓冲区下操作大量数据 = StringBuilder
3. 多线程操作字符串缓冲区下操作大量数据 = StringBuffer

### Comparable和Comparator区别比较

　　Comparable是排序接口，若一个类实现了Comparable接口，就意味着“该类支持排序”。而Comparator是比较器，我们若需要控制某个类的次序，可以建立一个“该类的比较器”来进行排序。

　　Comparable相当于“内部比较器”，而Comparator相当于“外部比较器”。

　　两种方法各有优劣， 用Comparable 简单， 只要实现Comparable 接口的对象直接就成为一个可以比较的对象，但是需要修改源代码。 用Comparator 的好处是不需要修改源代码， 而是另外实现一个比较器， 当某个自定义的对象需要作比较的时候，把比较器和对象一起传递过去就可以比大小了， 并且在Comparator 里面用户可以自己实现复杂的可以通用的逻辑，使其可以匹配一些比较简单的对象，那样就可以节省很多重复劳动了。

### hashCode:

会返回每个对象特有的序号（java是依据对象的内存地址计算出的此序号）

如果想要让两个不同的对象视为相等的，就必须覆盖Object继下来的hashCode方法和equals方法，因为Object hashCode方法返回的是该对象的内存地址，所以必须重写hashCode方法，才能保证两个不同的对象具有相同的hashCode，同时也需要两个不同对象比较equals方法会返回true

### final关键字

final可以修饰变量，方法和类，用于表示所修饰的内容一旦赋值之后就不会再被改变，比如String类就是一个final类型的类

下面总结了一些使用final关键字的好处

final关键字提高了性能。JVM和Java应用都会缓存final变量。

final变量可以安全的在多线程环境下进行共享，而不需要额外的同步开销。

使用final关键字，JVM会对方法、变量及类进行优化。

### volatile

### ThreadLocal

### java序列化和反序列化

## 序列化和反序列化的概念

序列化：把对象转换为字节序列的过程称为对象的序列化。  
反序列化：把字节序列恢复为对象的过程称为对象的反序列化。

序列化

 ObjectOutputStream oos = new ObjectOutputStream(new FileOutputStream(new File("d:/flyPig.txt")));

 oos.writeObject(flyPig);

 System.out.println("FlyPig 对象序列化成功！");

反序列化

 ObjectInputStream ois = new ObjectInputStream(new FileInputStream(new File("d:/flyPig.txt")));

 FlyPig person = (FlyPig) ois.readObject();

 System.out.println("FlyPig 对象反序列化成功！");

## 集合容器

### 数组

默认排序：需要元素实现Comparable接口，重写compareTo方法

### List主要分为3类

ArrayList， LinkedList和Vector（父类Collection）

List是一个有序的集合，和set不同的是，List允许存储项的值为空，也允许存储相等值的存储项

### ArrayList

是一个数组实现的列表，由于数据是存入数组中的，所以它的特点也和数组一样，查询很快，但是中间部分的插入和删除很慢

### Vector

Vector就是ArrayList的线程安全版，它的方法前都加了synchronized锁，其他实现逻辑都相同。   
如果对线程安全要求不高的话，可以选择ArrayList，毕竟synchronized也很耗性能

### ****LinkedList****

LinkedList是一个双向链表,

链表的数据结构：一个是当前链表的头节点，一个是尾部节点，还有是链表长度。

由于查询时候需要移动指针，所以性能偏低。但在插入删除方面只需要移动指针操作优于

ArrayList。因为ArrayList需要进行循环遍历，特别是插入到某一个位置时候需要将当前位置

以后的数据循环遍历下标+1，并且存放到新的数组里面。完成插入的操作。

### ArrayList和LinkedList的分析

可以理解List的3个特性   
1.是按顺序查找   
2.允许存储项为空   
3.允许多个存储项的值相等   
可以知其然知其所以然

然后对比LinkedList和ArrayList的实现方式不同，可以在不同的场景下使用不同的List   
ArrayList是由数组实现的，方便查找，返回数组下标对应的值即可，适用于多查找的场景   
LinkedList由链表实现，插入和删除方便，适用于多次数据替换的场景

### HashMap源码分析

<https://www.jianshu.com/p/b40fd341711e>

http://www.importnew.com/28263.html

散列表（Hash table，也叫哈希表），是根据关键码值(Key value)而直接进行访问的数据结构。也就是说，它通过把关键码值映射到表中一个位置来访问记录，以加快查找的速度。这个映射函数叫做散列函数，存放记录的数组叫做散列表。

HashMap 是一个散列表，它存储的内容是键值对 (key-value) 映射。

HashMap的键不重复：如果hashCode相同的话， 再去比较 equals()方法，如果也相同的话，JVM就认为数据已经存在了，就不会添加数据！

HashMap 实现原理：jdk1.7版本之前(包括1.7) 数组 + 链表

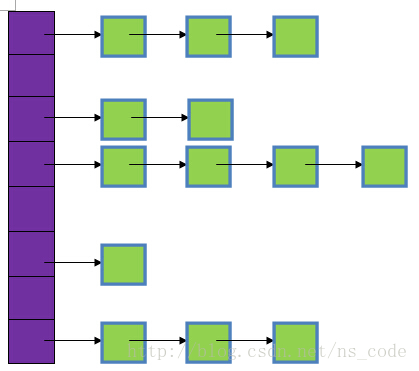
HashMap 里面是一个数组，然后数组中每个元素是一个单向链表。

HashMap的底层主要是基于数组和链表实现的，它之所以有相当快的查询速度主要是因为它是通过计算散列码来决定存储位置的。HashMap中主要是通过key的hashCode来计算hash值，然后通过hash值选择不同的数组来存储。

HashMap 采用一种所谓的“Hash 算法”来决定每个元素的存储位置

只要hashCode相同，计算出来的hash值就一样，如果存储对象多了，就有可能不同的对象计算出来的hash值是相同的，这就出现了所谓的hash冲突。

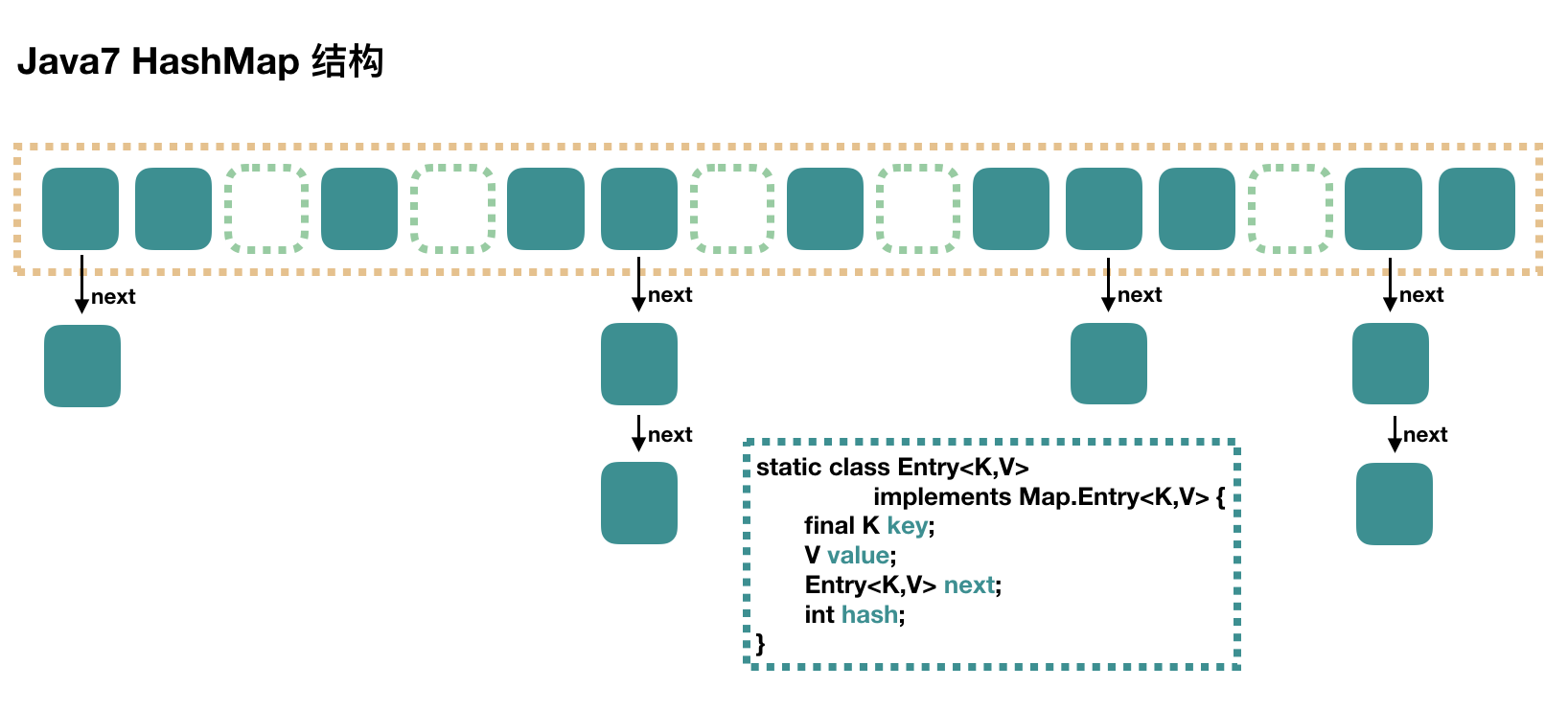
解决hash冲突：HashMap底层是通过链表来解决hash冲突的。



 图中，紫色部分即代表哈希表，也称为哈希数组，数组的每个元素都是一个单链表的头节

点，链表是用来解决冲突的，如果不同的key映射到了数组的同一位置处，就将其放入单链

表中。



这个仅仅是示意图，因为没有考虑到数组要扩容的情况，具体的后面再说。

大方向上，HashMap 里面是一个数组，然后数组中每个元素是一个单向链表。

上图中，每个绿色的实体是嵌套类 Entry 的实例，Entry 包含四个属性：key, value, hash 值和用于单向链表的 next。

capacity：当前数组容量，始终保持 2^n，可以扩容，扩容后数组大小为当前的 2 倍。

loadFactor：负载因子，默认为 0.75。

threshold：扩容的阈值，等于 capacity \* loadFactor

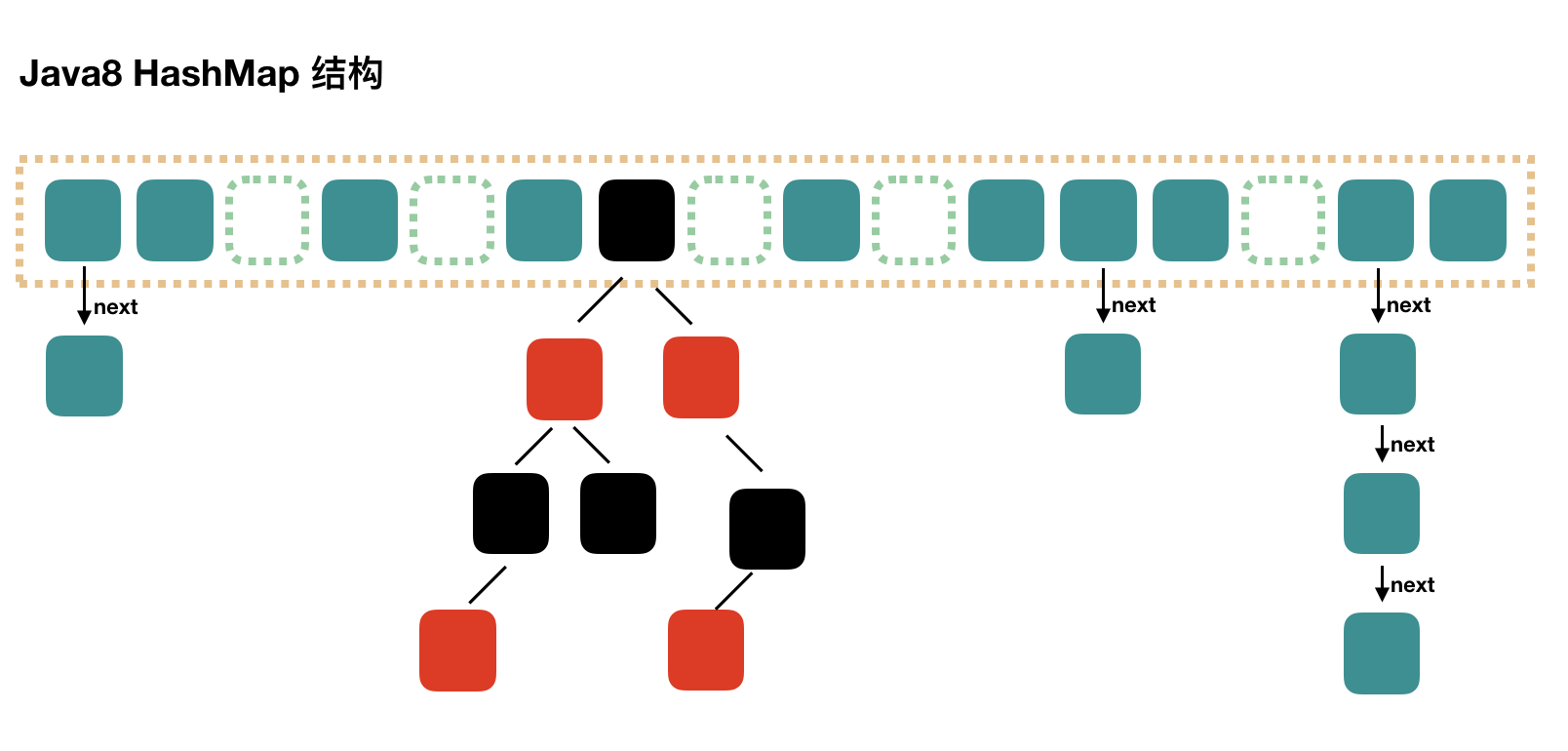
和 Java7 稍微有点不一样的地方就是，Java7 是先扩容后插入新值的，Java8 先插值再扩容，不过这个不重要。

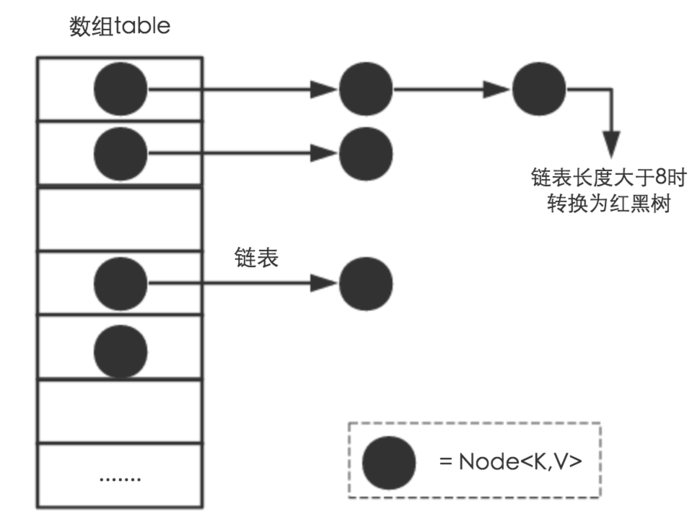
HashMap （JDK1.8 增加了红黑树部分）是数组 + 链表 + 红黑树实现的。

Java8 对 HashMap 进行了一些修改，最大的不同就是利用了红黑树，所以其由 数组+链表+红黑树 组成。

根据 Java7 HashMap 的介绍，我们知道，查找的时候，根据 hash 值我们能够快速定位到数组的具体下标，但是之后的话，需要顺着链表一个个比较下去才能找到我们需要的，时间复杂度取决于链表的长度，为 O(n)。

为了降低这部分的开销，在 Java8 中，当链表中的元素超过了 8 个以后，会将链表转换为红黑树，在这些位置进行查找的时候可以降低时间复杂度为 O(logN)。





### HashMap 特性

* Hash 相关的数据结构本质上就是键值对
* Hash 中不能存在重复的键
* HashMap 提供非常快速查找时间复杂度
* HashMap 具体实现中，null 可以作为 key 或者 value 存在
* HashMap 不是线程安全
* HashMap 非线程安全，即任一时刻可以有多个线程同时写 HashMap，可能会导致数据的不一致。如果需要满足线程安全，可以用 Collections 的 synchronizedMap 方法使 HashMap 具有线程安全的能力，或者使用 ConcurrentHashMap。
* Collections.synchronizedMap

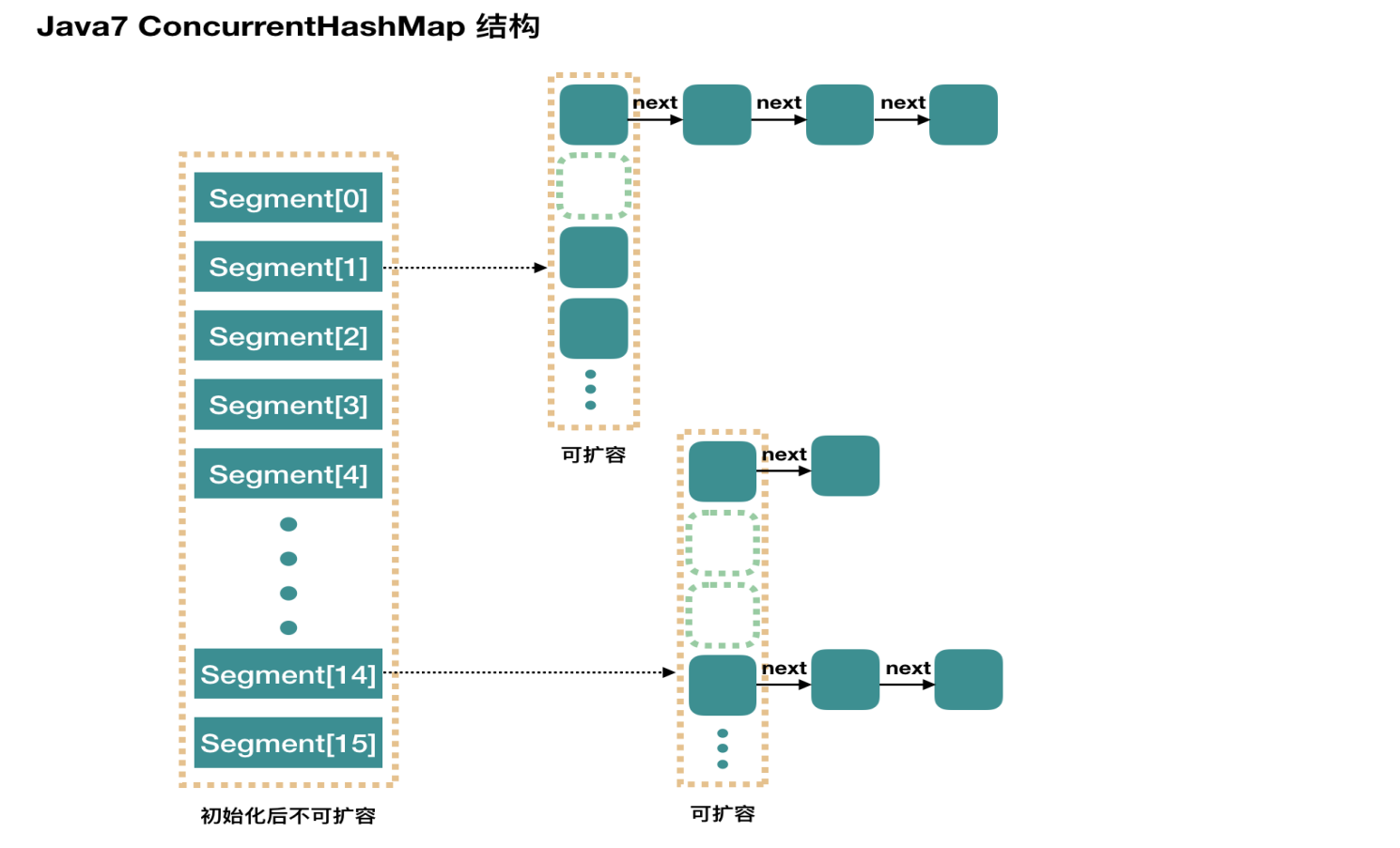
### ConcurrentHashMap

http://www.importnew.com/28263.html

ConcurrentHashMap 和 HashMap 思路是差不多的，但是因为它支持并发操作，所以要复杂一些。

整个 ConcurrentHashMap 由一个个 Segment 组成，Segment 代表”部分“或”一段“的意思，所以很多地方都会将其描述为分段锁。注意，行文中，我很多地方用了“槽”来代表一个 segment。

简单理解就是，ConcurrentHashMap 是一个 Segment 数组，Segment 通过继承 ReentrantLock 来进行加锁，所以每次需要加锁的操作锁住的是一个 segment，这样只要保证每个 Segment 是线程安全的，也就实现了全局的线程安全。



concurrencyLevel：并行级别、并发数、Segment 数，怎么翻译不重要，理解它。默认是 16，也就是说 ConcurrentHashMap 有 16 个 Segments，所以理论上，这个时候，最多可以同时支持 16 个线程并发写，只要它们的操作分别分布在不同的 Segment 上。这个值可以在初始化的时候设置为其他值，但是一旦初始化以后，它是不可以扩容的。

再具体到每个 Segment 内部，其实每个 Segment 很像之前介绍的 HashMap，不过它要保证线程安全，所以处理起来要麻烦些。

### TreeMap

### Set: 继承自Collection

非线程安全

用于存储无序(存入和取出的顺序不一定相同)元素，值不能重复

TreeMap 是一个**有序的key-value集合**，它是通过[红黑树](http://www.cnblogs.com/skywang12345/p/3245399.html)实现的。

TreeMap基于**红黑树（Red-Black tree）实现**。该映射根据**其键的自然顺序进行排序**，或者根据**创建映射时提供的 Comparator 进行排序**，具体取决于使用的构造方法。  
TreeMap的基本操作 containsKey、get、put 和 remove 的时间复杂度是 log(n) 。O(n)

### HashSet

HashSet实现了Set接口，它不允许集合中有重复的值，当我们提到HashSet时，第一件事情就是在将对象存储在HashSet之前，要先确保对象重写equals()和hashCode()方法，这样才能比较对象的值是否相等，以确保set中没有储存相等的对象。如果我们没有重写这两个方法，将会使用这个方法的默认实现。

public boolean add(Object o)方法用来在Set中添加元素，当元素值重复时则会立即返回false，如果成功添加的话会返回true

hashSet会通过元素的hashcode（）和equals方法进行判断元素师否重复。

HashSet到底是如何判断两个元素重复。

通过hashCode方法和equals方法来保证元素的唯一性，add()返回的是boolean类型

判断两个元素是否相同，先要判断元素的hashCode值是否一致，只有在该值一致的情况下，才会判断equals方法，如果存储在HashSet中的两个对象hashCode方法的值相同equals方法返回的结果是true，那么HashSet认为这两个元素是相同元素，只存储一个（重复元素无法存入）。

### TreeSet

通过compareTo或者compare方法中的来保证元素的唯一性。

添加的元素必须要实现Comparable接口。当compareTo()函数返回值为0时，说明两个对象相等，此时该对象不会添加进来。

### LinkedHashSet

会保存插入的顺序。

### HashTable

HashTable产生于JDK 1.1，而HashMap产生于JDK 1.2。从时间的维度上来看，HashMap要比HashTable出现得晚一些。

HashTable是同步的，HashMap不是，也就是说HashTable在多线程使用的情况下，不需要做额外的同步，而HashMap则不行。

HashMap是支持null键和null值的，而HashTable在遇到null时，会抛出NullPointerException异常。这并不是因为HashTable有什么特殊的实现层面的原因导致不能支持null键和null值，这仅仅是因为HashMap在实现时对null做了特殊处理，将null的hashCode值定为了0，从而将其存放在哈希表的第0个bucket中。

HashMap和HashTable都使用哈希表来存储键值对。在数据结构上是基本相同的，都创建了一个继承自Map.Entry的私有的内部类Entry，每一个Entry对象表示存储在哈希表中的一个键值对。

就是公开的方法比如get都使用了synchronized描述符。而遍历视图比如keySet都使用了Collections.synchronizedXXX进行了同步包装。

HashTable已经被淘汰了，不要在代码中再使用它。

简单来说就是，如果你不需要线程安全，那么使用HashMap，如果需要线程安全，那么使用ConcurrentHashMap。HashTable已经被淘汰了，不要在新的代码中再使用它。

## 多线程

### 线程创建方式

 通过继承Thread类，重写run方法；

 通过实现runable接口；

 通过实现callable接口这三种方式

public class CreateThreadDemo {

public static void main(String[] args) {

//1.继承Thread

Thread thread = new Thread() {

@Override

public void run() {

System.out.println("继承Thread");

super.run();

}

};

thread.start();

//2.实现runable接口

Thread thread1 = new Thread(new Runnable() {

@Override

public void run() {

System.out.println("实现runable接口");

}

});

thread1.start();

//3.实现callable接口

ExecutorService service = Executors.newSingleThreadExecutor();

Future<String> future = service.submit(new Callable() {

@Override

public String call() throws Exception {

return "通过实现Callable接口";

}

});

try {

String result = future.get();

System.out.println(result);

} catch (InterruptedException e) {

e.printStackTrace();

} catch (ExecutionException e) {

e.printStackTrace();

}

}

}

### 线程的状态

新建、运行、阻塞、等待、带超时的等待、终止

### 彻底理解synchronized

synchronized可以用在**方法**上也可以使用在**代码块**中

它最大的特征就是在同一时刻只有一个线程能够获得对象的监视器（monitor），从而进入到同步代码块或者同步方法之中，即表现为**互斥性（排它性）**。

### 什么是CAS

使用锁时，线程获取锁是一种**悲观锁策略**，即假设每一次执行临界区代码都会产生冲突，所以当前线程获取到锁的时候同时也会阻塞其他线程获取该锁。而CAS操作（又称为无锁操作）是一种**乐观锁策略**，它假设所有线程访问共享资源的时候不会出现冲突，既然不会出现冲突自然而然就不会阻塞其他线程的操作。因此，线程就不会出现阻塞停顿的状态。那么，如果出现冲突了怎么办？无锁操作是使用\*\*CAS(compare and swap)\*\*又叫做比较交换来鉴别线程是否出现冲突，出现冲突就重试当前操作直到没有冲突为止。

### 多线程join

多线程Join方法的作用就是把指定的线程加入到当前线程，让主线程等待子线程结束之后才能继续运行，从而完成同步操作。

join方法是先将线程池中的其它线程wait状态，join执行完毕，又调用了notifyAll()唤醒所有线程中的线程。

强行进入使用join方法的线程，其他线程等待该线程完全执行完后才会进来

### sleep

线程按照指定的时间休眠, sleep方法并不会失去锁。

### sleep() VS wait()

两者主要的区别：

1. sleep()方法是Thread的静态方法，而wait是Object实例方法
2. wait()方法必须要在同步方法或者同步块中调用，也就是必须已经获得对象锁。而sleep()方法没有这个限制可以在任何地方种使用。另外，wait()方法会释放占有的对象锁，使得该线程进入等待池中，等待下一次获取资源。而sleep()方法只是会让出CPU并不会释放掉对象锁；
3. sleep()方法在休眠时间达到后如果再次获得CPU时间片就会继续执行，而wait()方法必须等待Object.notift/Object.notifyAll通知后，才会离开等待池，并且再次获得CPU时间片才会继续执行。

### 守护线程

守护线程是一种特殊的线程，就和它的名字一样，它是系统的守护者，在后台默默地守护一些系统服务，比如垃圾回收线程，JIT线程就可以理解守护线程。与之对应的就是用户线程，用户线程就可以认为是系统的工作线程，它会完成整个系统的业务操作。用户线程完全结束后就意味着整个系统的业务任务全部结束了，因此系统就没有对象需要守护的了，守护线程自然而然就会退。当一个Java应用，只有守护线程的时候，虚拟机就会自然退出。

### 避免死锁

避免一个线程同时获得多个锁；互相竞争资源，并且不释放。

避免一个线程在锁内部占有多个资源，尽量保证每个锁只占用一个资源；

尝试使用定时锁，使用lock.tryLock(timeOut)，当超时等待时当前线程不会阻塞；

对于数据库锁，加锁和解锁必须在一个数据库连接里，否则会出现解锁失败的情况

### 同步VS异步

同步和异步通常用来形容一次方法调用。同步方法调用一开始，调用者必须等待被调用的方法结束后，调用者后面的代码才能执行。而异步调用，指的是，调用者不用管被调用方法是否完成，都会继续执行后面的代码，当被调用的方法完成后会通知调用者。比如，在超时购物，如果一件物品没了，你得等仓库人员跟你调货，直到仓库人员跟你把货物送过来，你才能继续去收银台付款，这就类似同步调用。而异步调用了，就像网购，你在网上付款下单后，什么事就不用管了，该干嘛就干嘛去了，当货物到达后你收到通知去取就好。

### 并发与并行

并发和并行是十分容易混淆的概念。并发指的是多个任务交替进行，而并行则是指真正意义上的“同时进行”。实际上，如果系统内只有一个CPU，而使用多线程时，那么真实系统环境下不能并行，只能通过切换时间片的方式交替进行，而成为并发执行任务。真正的并行也只能出现在拥有多个CPU的系统中。

## 常用设计模式

23种常见设计模式

### 工厂模式

我们没有创建逻辑暴露给客户端创建对象，并使用一个通用的接口引用新创建的对象。

### 抽象工厂模式

是一个超级工厂，用来创建其他工厂。 这个工厂也被称为工厂的工厂。 这种类型的设计模式属于创建模式，因为此模式提供了创建对象的最佳方法之一。

在抽象工厂模式中，接口负责创建相关对象的工厂，而不明确指定它们的类。 每个生成的工厂可以按照工厂模式提供对象。

### 单例（Singleton）模式

是Java中最简单的设计模式之一。这种类型的设计模式属于创建模式，因为此模式提供了创建对象的最佳方法之一。

这种模式涉及一个类，它负责创建一个对象，同时确保只创建一个对象。这个类提供了一种方法来访问它的唯一对象，可以直接访问，而不需要实例化类的对象。

### 适配器模式

作为两个不兼容接口之间的桥梁。 这种类型的设计模式属于结构模式，因为该模式组合了两个独立接口。

在这其中InputStreamReader和OutputStreamWriter就在字节流与字符流中起到了桥梁作用， 如：

BufferedReader reader = new BufferedReader(new InputStreamReader(new FileInputStream(new File("text.txt"))));

### Java mvc模式

如框架ssh、ssm

* **模型（Model）** - 模型表示携带数据的对象或JAVA POJO。如果其数据改变它也可以具有逻辑来更新控制器。
* **视图（View）** - 视图表示模型包含的数据的可视化层。
* **控制器（Controller）** - 控制器对模型和视图都有起作用。它控制数据流进入模型对象，并在数据更改时更新视图。它保持视图和模型分开，也是视图和模型的中间层。

**Java观察者模式**

activeMQ消息队列

观察者模式在对象之间存在一对多关系时使用，例如，如果一个对象被修改，它的依赖对象将被自动通知。 观察者模式属于行为模式类别。

### 责任链模式：

通过把请求从一个对象传递到链条中下一个对象的方式，直到请求被处理完毕，以实现对象间的解耦。如 javax.servlet.Filter#doFilter()。

### 代理模式（Proxy）

为其他对象提供一种代理以控制对这个对象的访问。

ActiveMQ 是Apache出品，最流行的，能力强劲的开源消息总线。ActiveMQ 是一个完全支持JMS1.1和J2EE 1.4规范的JMS Provider实现,尽管JMS规范出台已经是很久的事情了,但是JMS在当今的J2EE应用中间仍然扮演着特殊的地位。

### 观察者模式

<https://www.cnblogs.com/luohanguo/p/7825656.html>

观察者模式的定义：

在对象之间定义了一对多的依赖，这样一来，当一个对象改变状态，依赖它的对象会收到通知并自动更新。

大白话：

　　其实就是发布订阅模式，发布者发布信息，订阅者获取信息，订阅了就能收到信息，没订阅就收不到信息。

### 事件驱动模型简介

事件驱动模型也就是我们常说的观察者，或者发布-订阅模型；理解它的几个关键点：

1. 首先是一种对象间的一对多的关系；最简单的如交通信号灯，信号灯是目标（一方），行人注视着信号灯（多方）；
2. 当目标发送改变（发布），观察者（订阅者）就可以接收到改变；
3. 观察者如何处理（如行人如何走，是快走/慢走/不走，目标不会管的），目标无需干涉；所以就松散耦合了它们之间的关系。

## 加解密

### 参考资料

该文中的内容来源于 Oracle 的官方文档 [Java SE Tools Reference](http://docs.oracle.com/javase/8/docs/technotes/tools/unix/index.html" \t "_blank) 。Oracle 在 Java 方面的文档是非常完善的。对 Java 8 感兴趣的朋友，可以直接找到这个总入口 [Java SE 8 Documentation](http://docs.oracle.com/javase/8/" \t "_blank) ，想阅读什么就点什么。本博客不定期从 Oracle 官网搬砖。这里介绍的工具是 [keytool](http://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html" \t "_blank) 。

### 网络安全概论

在 Web 世界里，安全是一个重之又重的课题，甚至是美国政府都禁止某些加密解密算法的出口。 Java 和 Linux 都是 Web 领域的领头羊，各种加解密的算法和管理工具一应俱全，例如 GnuPG 就是一个不错的安全套件。但是在这里，只展示一下 JDK 中的 keytool 工具的使用方法。

先来说一下加解密算法的分类。基本上可以分为三类，它们分别是对称性解密算法、非对称性加密算法和消息摘要算法。每一类算法中又有多个不同的具体算法。对于这些算法，我们不要求完全掌握，但是对于各类算法的特点和用途是一定要了解的，对于一些常见的名字，如 DES、AES、RSA、DSA、MD5、SHA1 等，一定要熟悉，至少要知道它们分别属于哪类算法。

### 对称加密

对称性加密算法使用同一个密钥对信息进行加密和解密，其信息的安全性一部分取决于加密算法和密钥的长度，另一部分取决于密钥在传递过程中是否会被截获或盗取。

常用的对称性加密算法有DES算法、AES算法、3DES算法、TDEA算法、Blowfish算法、RC5算法、IDEA算法。常用的非对称性加密算法有DSA算法、RSA算法、Elgamal算法、背包算法、Rabin算法、D-H算法、ECC算法（椭圆曲线加密算法）。

### 非对称加密

非对称性加密算法使用两个密钥分别对信息进行加密和解密，这两个密钥称为私钥/公钥对。使用私钥加密的信息必须使用公钥解密，反之亦然。公钥可以公开发布，私钥由加密方保存，绝对不公开，将私钥被截获或窃取的可能性降到最低，因此非对称性加密算法的安全性比对称性加密算法的安全性更高。既然非对称性加密算法比对称性加密算法安全性更高，那对称性加密算法有什么存在的必要呢？这是因为对称性加密算法的运算速度更快。

现实中，往往将对称性加密算法和非对称性加密算法结合使用，对于要传输的大块数据使用对称性加密算法加密，然后对加密使用的密钥使用非对称性加密算法进行加密，这样既可以获得更高的安全性，又可以获得更高的加解密运算速度。

### (消息摘要)散列型加密

消息摘要算法的主要目的是对数据生成摘要。消息摘要算法不需要密钥，只有输入相同的数据才能得到相同的摘要，而且不可能从摘要反过来推算出数据。常用的消息摘要算法有MD5算法和SHA-1算法及其大量的变体。它们可以用来保证数据的完整性，在网络上发布文件时，常同时提供该文件的MD5值就是利用的消息摘要算法的这个特点，一旦该文件被篡改或者在网络传输中出现数据错误，再对其进行摘要运算就得不到相同的MD5值。

# jvm虚拟机

## Java 主流的虚拟机

JRockit VM和HotSpot

## Java内存模型：

程序计数器：是一块较小的内存空间，是当前线程所执行字节码的行号的指示器，通过改变这个计数器的值来选取需要执行的字节码指令。比如多线程的数据状态，且该区域为线程私有。Java多线程通过空间切换时间，分配处理器时间。为了线程切换后能回复到正确的位置，每条线程都需要独立的程序计数器。

java虚拟机栈：

本地方法 栈：

java虚拟机堆：

常量池：

## Jvm参数：

**-vmargs -Xms128M -Xmx512M -XX:PermSize=64M -XX:MaxPermSize=128M  
-vmargs 说明后面是VM的参数，所以后面的其实都是JVM的参数了  
-Xms128m JVM初始分配的堆内存  
-Xmx512m JVM最大允许分配的堆内存，按需分配  
-XX:PermSize=64M JVM初始分配的非堆内存  
-XX:MaxPermSize=128M JVM最大允许分配的非堆内存，按需分配**

# 计算机网络模型

## http

## https

## tcp

## udp

## socket

## cookie

cookie的内容主要包括：名字，值，过期时间，路径和域。路径与域一起构成cookie的作用范围。若不设置过期时间，则表示这

个cookie的生命期为浏览器会话期间，关闭浏览器窗口，cookie就消失。这种生命期为浏览器会话期的cookie被称为会话cookie。

会话cookie一般不存储在硬盘上而是保存在内存里，当然这种行为并不是规范规定的。若设置了过期时间，浏览器就会把cookie

保存到硬盘上，关闭后再次打开浏览器，这些cookie仍然有效直到超过设定的过期时间。存储在硬盘上的cookie可以在不同的浏

览器进程间共享，比如两个IE窗口。而对于保存在内存里的cookie，不同的浏览器有不同的处理方式

## session

session机制。session机制是一种服务器端的机制，服务器使用一种类似于散列表的结构（也可能就是使用散列表）来保存信息。

          当程序需要为某个客户端的请求创建一个session时，服务器首先检查这个客户端的请求里是否已包含了一个session标识

（称为session id），如果已包含则说明以前已经为此客户端创建过session，服务器就按照session id把这个session检索出来

使用（检索不到，会新建一个），如果客户端请求不包含session id，则为此客户端创建一个session并且生成一个与此session相

关联的session id，session id的值应该是一个既不会重复，又不容易被找到规律以仿造的字符串，这个session id将被在本次响应

中返回给客户端保存。保存这个session id的方式可以采用cookie，这样在交互过程中浏览器可以自动的按照规则把这个标识发送给

服务器。一般这个cookie的名字都是类似于SEEESIONID。但cookie可以被人为的禁止，则必须有其他机制以便在cookie被禁止时

仍然能够把session id传递回服务器。

## cookie和session的区别

cookie机制采用的是在客户端保持状态的方案，而session机制采用的是在服务器端保持状态的方案。

1、cookie数据存放在客户的浏览器上，session数据放在服务器上。

2、cookie不是很安全，别人可以分析存放在本地的COOKIE并进行COOKIE欺骗  
   考虑到安全应当使用session。

3、session会在一定时间内保存在服务器上。当访问增多，会比较占用你服务器的性能  
   考虑到减轻服务器性能方面，应当使用COOKIE。

4、单个cookie保存的数据不能超过4K，很多浏览器都限制一个站点最多保存20个cookie。

5、所以个人建议：  
   将登陆信息等重要信息存放为SESSION  
   其他信息如果需要保留，可以放在COOKIE中

## get请求

## post请求

## BIO与NIO、AIO的区别

**https://www.jianshu.com/p/ef418ccf2f7d**

一、BIO

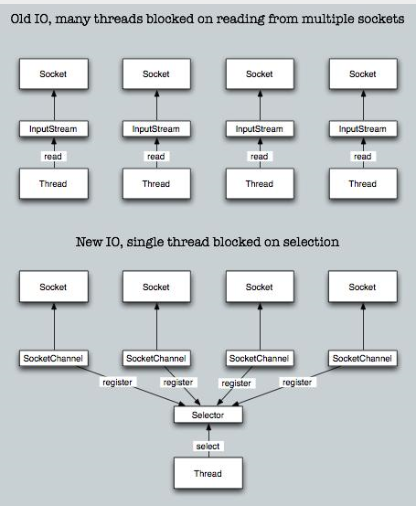
     在JDK1.4出来之前，我们建立网络连接的时候采用BIO模式，需要先在服务端启动一个ServerSocket，然后在客户端启动Socket来对服务端进行通信，默认情况下服务端需要对每个请求建立一堆线程等待请求，而客户端发送请求后，先咨询服务端是否有线程相应，如果没有则会一直等待或者遭到拒绝请求，如果有的话，客户端会线程会等待请求结束后才继续执行。

二、NIO

    NIO本身是基于事件驱动思想来完成的，其主要想解决的是BIO的大并发问题： 在使用同步I/O的网络应用中，如果要同时处理多个客户端请求，或是在客户端要同时和多个服务器进行通讯，就必须使用多线程来处理。也就是说，将每一个客户端请求分配给一个线程来单独处理。这样做虽然可以达到我们的要求，但同时又会带来另外一个问题。由于每创建一个线程，就要为这个线程分配一定的内存空间（也叫工作存储器），而且操作系统本身也对线程的总数有一定的限制。如果客户端的请求过多，服务端程序可能会因为不堪重负而拒绝客户端的请求，甚至服务器可能会因此而瘫痪。

    NIO基于Reactor，当socket有流可读或可写入socket时，操作系统会相应的通知引用程序进行处理，应用再将流读取到缓冲区或写入操作系统。  也就是说，这个时候，已经不是一个连接就要对应一个处理线程了，而是有效的请求，对应一个线程，当连接没有数据时，是没有工作线程来处理的。

   BIO与NIO一个比较重要的不同，是我们使用BIO的时候往往会引入多线程，每个连接一个单独的线程；而NIO则是使用单线程或者只使用少量的多线程，每个连接共用一个线程。



      NIO的最重要的地方是当一个连接创建后，不需要对应一个线程，这个连接会被注册到多路复用器上面，所以所有的连接只需要一个线程就可以搞定，当这个线程中的多路复用器进行轮询的时候，发现连接上有请求的话，才开启一个线程进行处理，也就是一个请求一个线程模式。

      在NIO的处理方式中，当一个请求来的话，开启线程进行处理，可能会等待后端应用的资源(JDBC连接等)，其实这个线程就被阻塞了，当并发上来的话，还是会有BIO一样的问题。

　　HTTP/1.1出现后，有了Http长连接，这样除了超时和指明特定关闭的http header外，这个链接是一直打开的状态的，这样在NIO处理中可以进一步的进化，在后端资源中可以实现资源池或者队列，当请求来的话，开启的线程把请求和请求数据传送给后端资源池或者队列里面就返回，并且在全局的地方保持住这个现场(哪个连接的哪个请求等)，这样前面的线程还是可以去接受其他的请求，而后端的应用的处理只需要执行队列里面的就可以了，这样请求处理和后端应用是异步的.当后端处理完，到全局地方得到现场，产生响应，这个就实现了异步处理。

三、AIO

     与NIO不同，当进行读写操作时，只须直接调用API的read或write方法即可。这两种方法均为异步的，对于读操作而言，当有流可读取时，操作系统会将可读的流传入read方法的缓冲区，并通知应用程序；对于写操作而言，当操作系统将write方法传递的流写入完毕时，操作系统主动通知应用程序。  即可以理解为，read/write方法都是异步的，完成后会主动调用回调函数。  在JDK1.7中，这部分内容被称作NIO.2，主要在java.nio.channels包下增加了下面四个异步通道：

* AsynchronousSocketChannel
* AsynchronousServerSocketChannel
* AsynchronousFileChannel
* AsynchronousDatagramChannel

其中的read/write方法，会返回一个带回调函数的对象，当执行完读取/写入操作后，直接调用回调函数。

BIO是一个连接一个线程。

NIO是一个请求一个线程。

AIO是一个有效请求一个线程。

Java对BIO、NIO、AIO的支持：

Java BIO ： 同步并阻塞，服务器实现模式为一个连接一个线程，即客户端有连接请求时服务器端就需要启动一个线程进行处理，如果这个连接不做任何事情会造成不必要的线程开销，当然可以通过线程池机制改善。

Java NIO ： 同步非阻塞，服务器实现模式为一个请求一个线程，即客户端发送的连接请求都会注册到多路复用器上，多路复用器轮询到连接有I/O请求时才启动一个线程进行处理。

Java AIO(NIO.2) ： 异步非阻塞，服务器实现模式为一个有效请求一个线程，客户端的I/O请求都是由OS先完成了再通知服务器应用去启动线程进行处理，

BIO、NIO、AIO适用场景分析:

BIO方式适用于连接数目比较小且固定的架构，这种方式对服务器资源要求比较高，并发局限于应用中，JDK1.4以前的唯一选择，但程序直观简单易理解。

NIO方式适用于连接数目多且连接比较短（轻操作）的架构，比如聊天服务器，并发局限于应用中，编程比较复杂，JDK1.4开始支持。

AIO方式使用于连接数目多且连接比较长（重操作）的架构，比如相册服务器，充分调用OS参与并发操作，编程比较复杂，JDK7开始支持。

## 跨域

[探讨跨域请求资源的几种方式](https://www.cnblogs.com/dojo-lzz/p/4265637.html)

什么是跨域

JSONP

proxy代理

cors

xdr

　　由于浏览器同源策略，凡是发送请求url的协议、域名、端口三者之间任意一与当前页面地址不同即为跨域。

# javaEE框架

## Spring

### IOC控制反转 DI

### AOP面向切面编程

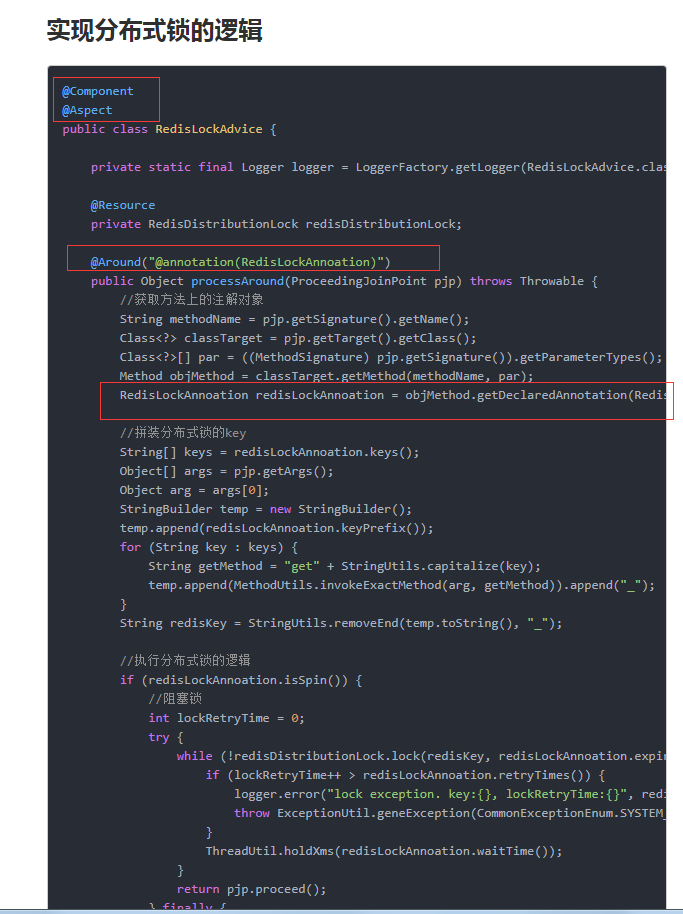
### spring注解@CrossOrigin解决跨域

### 注解

<https://www.jianshu.com/p/e72baf5e5617>



注解的实现类



## SpringMvc

## SpringBoot

## MyBatis

# 数据库

## mysql的常用引擎

在MySQL数据库中，常用的引擎主要就是2个：Innodb和MyIASM。

首先：

1.简单介绍这两种引擎，以及该如何去选择。

2.这两种引擎所使用的数据结构是什么。

a.Innodb引擎，Innodb引擎提供了对数据库ACID事务的支持。并且还提供了行级锁和外键的约束。它的设计的目标就是处理大数据容量的数据库系统。它本身实际上是基于Mysql后台的完整的系统。Mysql运行的时候，Innodb会在内存中建立缓冲池，用于缓冲数据和索引。但是，该引擎是不支持全文搜索的。同时，启动也比较的慢，它是不会保存表的行数的。当进行Select count(\*) from table指令的时候，需要进行扫描全表。所以当需要使用数据库的事务时，该引擎就是首选。由于锁的粒度小，写操作是不会锁定全表的。所以在并发度较高的场景下使用会提升效率的。

b.MyIASM引擎，它是MySql的默认引擎，但不提供事务的支持，也不支持行级锁和外键。因此当执行Insert插入和Update更新语句时，即执行写操作的时候需要锁定这个表。所以会导致效率会降低。不过和Innodb不同的是，MyIASM引擎是保存了表的行数，于是当进行Select count(\*) from table语句时，可以直接的读取已经保存的值而不需要进行扫描全表。所以，如果表的读操作远远多于写操作时，并且不需要事务的支持的。可以将MyIASM作为数据库引擎的首先。

补充2点：

c.大容量的数据集时趋向于选择Innodb。因为它支持事务处理和故障的恢复。Innodb可以利用数据日志来进行数据的恢复。主键的查询在Innodb也是比较快的。

d.大批量的插入语句时（这里是INSERT语句）在MyIASM引擎中执行的比较的快，但是UPDATE语句在Innodb下执行的会比较的快，尤其是在并发量大的时候。

2.两种引擎所使用的索引的数据结构是什么？

答案:都是B+树!

MyIASM引擎，B+树的数据结构中存储的内容实际上是实际数据的地址值。也就是说它的索引和实际数据是分开的，只不过使用索引指向了实际数据。这种索引的模式被称为非聚集索引。

Innodb引擎的索引的数据结构也是B+树，只不过数据结构中存储的都是实际的数据，这种索引有被称为聚集索引。

三、 关于Mysql数据库默认的存储引擎：

MyISAM和InnoDB是MySQL的两种存储引擎。从MySQL5.5.5以后，InnoDB是默认引擎。

如果是默认安装，那就应该是InnoDB，你可以在my.cnf文件中找到default-storage-engine=INNODB；

InnoDB优点：支持事务，支持外键，并发量较大，适合大量update。

缺点：查询数据相对较快，不适合大量的select。

## 事务

### 3.1、原子性（A）

所谓的原子性就是说，在整个事务中的所有操作，要么全部完成，要么全部不做，没有中间状态。对于事务在执行中发生错误，所有的操作都会被回滚，整个事务就像从没被执行过一样。

### 3.2、一致性（C）

事务的执行必须保证系统的一致性，就拿转账为例，A有500元，B有300元，如果在一个事务里A成功转给B50元，那么不管并发多少，不管发生什么，只要事务执行成功了，那么最后A账户一定是450元，B账户一定是350元。

### 3.3、隔离性（I）

所谓的隔离性就是说，事务与事务之间不会互相影响，一个事务的中间状态不会被其他事务感知。

### 3.4、持久性（D）

所谓的持久性，就是说一单事务完成了，那么事务对数据所做的变更就完全保存在了数据库中，即使发生停电，系统宕机也是如此。

## 数据库性能优化

# 分布式

## 分布式原理

https://juejin.im/entry/59b9e125f265da064703d1da

相对于单体系统，分布式是指将一个业务拆分不同的子业务，分布在不同的服务器上执行，不同服务器之间可以互相通信和协调。

## 集群

* 是指多台服务器集中在一起，实现同一业务（同一个业务代码部署多套到不同机子上），集合起来提供服务的（一般会配上负载均衡）。理论上，分布式的系统一般都是带集群的。

## 负载均衡

* 高效分发请求

Nginx

## 微服务

* 作者有关 Microservice 的原文：<https://martinfowler.com/articles/microservices.html>
* 中文翻译：<http://insights.thoughtworks.cn/microservices-2/>
* 它不是框架，也不是系统，只是一种架构风格。所以我们用的 dubbo [‘dʌbəu]、Spring Cloud 等框架，都是分布式服务框架。只是这种分布式服务框架都是微服务架构必不可少的基础能力，微服务一定是分布式的。分布式服务的概念比较模糊，只是解决了网站的高并发问题，很多细节问题是微服务帮其明确的。微服务更加强调敏捷和健壮，强调服务的粒度，一个服务只需完成一个单一的、独立的功能，多个微服务组合完成相对复杂的业务系统，以满足需求。而且微服务注重借助于各种中间件进行业务解耦和提高性能，以及提高服务的容错性。
* 所以，理论上：微服务的架构都是带：模块拆分、服务拆分、分布式、集群。
* 微服务其实在很早以前就有人/公司在做，只是过去没人去给它做总结和思考它本身，然后 Martin Fowler 就帮我们帮我们做了。
* 单体系统在早期也没啥不好，但是随着 AWS 这种可弹性扩展的云诞生之后，这种单体架构就显得不够时尚了，只有微服务的架构才能合理榨干这些各种类型的云服务。  
  微服务的目的是有效的拆分应用，实现敏捷开发和部署 。

### 引入微服务带来的技术问题

* 既然微服务的目的是有效的拆分应用，实现敏捷开发和部署，那拆分后的新模式肯定会带来新的问题。
  + 客户端怎么访问 N 个服务？
  + N 个服务怎么管理？
  + N 个服务如何通信？
  + 服务挂了怎么处理？
  + 服务变成无状态？
  + 网络开销？

### RPC原理

### dubbo

### springCloud

## 中间件

### 缓存

**redis**

https://blog.csdn.net/u013256816/article/details/51146314

### 搜索引擎

MQ消息队列

### JMS介绍

JMS的全称是Java Message Service，即Java消息服务。用于在两个应用程序之间，或分布式系统中发送消息，进行异步通信。

它主要用于在生产者和消费者之间进行消息传递，生产者负责产生消息，而消费者负责接收消息。把它应用到实际的业务需求中的话我们可以在特定的时候利用生产者生成一消息，并进行发送，对应的消费者在接收到对应的消息后去完成对应的业务逻辑。

对于消息的传递有两种类型：

**一种是点对点的**，即一个生产者和一个消费者一一对应；

**另一种是发布/订阅模式**，即一个生产者产生消息并进行发送后，可以由多个消费者进行接收。

## 分布式锁

https://github.com/yujiasun/Distributed-Kit

[http://www.importnew.com/27477.html#comment-662045](http://www.importnew.com/27477.html" \l "comment-662045)

### 前言

分布式锁一般有三种实现方式：1. 数据库乐观锁；2. 基于Redis的分布式锁；3. 基于ZooKeeper的分布式锁。本篇博客将介绍第二种方式，基于Redis实现分布式锁。虽然网上已经有各种介绍Redis分布式锁实现的博客，然而他们的实现却有着各种各样的问题，为了避免误人子弟，本篇博客将详细介绍如何正确地实现Redis分布式锁。

### 可靠性

首先，为了确保分布式锁可用，我们至少要确保锁的实现同时满足以下四个条件：

1. 互斥性。在任意时刻，只有一个客户端能持有锁。
2. 不会发生死锁。即使有一个客户端在持有锁的期间崩溃而没有主动解锁，也能保证后续其他客户端能加锁。
3. 具有容错性。只要大部分的Redis节点正常运行，客户端就可以加锁和解锁。
4. 解铃还须系铃人。加锁和解锁必须是同一个客户端，客户端自己不能把别人加的锁给解了。

### 代码实现

### 组件依赖

首先我们要通过Maven引入Jedis开源组件，在pom.xml文件加入下面的代码：

|  |  |
| --- | --- |
| 1  2  3  4  5 | <dependency>      <groupId>redis.clients</groupId>      <artifactId>jedis</artifactId>      <version>2.9.0</version>  </dependency> |

### 加锁代码

**正确姿势**

Talk is cheap, show me the code。先展示代码，再带大家慢慢解释为什么这样实现：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26 | public class RedisTool {        private static final String LOCK\_SUCCESS = "OK";      private static final String SET\_IF\_NOT\_EXIST = "NX";      private static final String SET\_WITH\_EXPIRE\_TIME = "PX";        /\*\*       \* 尝试获取分布式锁       \* @param jedis Redis客户端       \* @param lockKey 锁       \* @param requestId 请求标识       \* @param expireTime 超期时间       \* @return 是否获取成功       \*/      public static boolean tryGetDistributedLock(Jedis jedis, String lockKey, String requestId, int expireTime) {            String result = jedis.set(lockKey, requestId, SET\_IF\_NOT\_EXIST, SET\_WITH\_EXPIRE\_TIME, expireTime);            if (LOCK\_SUCCESS.equals(result)) {              return true;          }          return false;        }    } |

可以看到，我们加锁就一行代码：jedis.set(String key, String value, String nxxx, String expx, int time)，这个set()方法一共有五个形参：

* 第一个为key，我们使用key来当锁，因为key是唯一的。
* 第二个为value，我们传的是requestId，很多童鞋可能不明白，有key作为锁不就够了吗，为什么还要用到value？原因就是我们在上面讲到可靠性时，分布式锁要满足第四个条件解铃还须系铃人，通过给value赋值为requestId，我们就知道这把锁是哪个请求加的了，在解锁的时候就可以有依据。requestId可以使用UUID.randomUUID().toString()方法生成。
* 第三个为nxxx，这个参数我们填的是NX，意思是SET IF NOT EXIST，即当key不存在时，我们进行set操作；若key已经存在，则不做任何操作；
* 第四个为expx，这个参数我们传的是PX，意思是我们要给这个key加一个过期的设置，具体时间由第五个参数决定。
* 第五个为time，与第四个参数相呼应，代表key的过期时间。

总的来说，执行上面的set()方法就只会导致两种结果：1. 当前没有锁（key不存在），那么就进行加锁操作，并对锁设置个有效期，同时value表示加锁的客户端。2. 已有锁存在，不做任何操作。

心细的童鞋就会发现了，我们的加锁代码满足我们可靠性里描述的三个条件。首先，set()加入了NX参数，可以保证如果已有key存在，则函数不会调用成功，也就是只有一个客户端能持有锁，满足互斥性。其次，由于我们对锁设置了过期时间，即使锁的持有者后续发生崩溃而没有解锁，锁也会因为到了过期时间而自动解锁（即key被删除），不会发生死锁。最后，因为我们将value赋值为requestId，代表加锁的客户端请求标识，那么在客户端在解锁的时候就可以进行校验是否是同一个客户端。由于我们只考虑Redis单机部署的场景，所以容错性我们暂不考虑。

### Redis 分布式锁的正确实现方式（ Java 版 ）

2017/12/02 | 分类： [基础技术](http://www.importnew.com/cat/basic" \o "查看 基础技术 中的全部文章) | [11 条评论](http://www.importnew.com/27477.html" \l "comments" \o "《Redis 分布式锁的正确实现方式（ Java 版 ）》上的评论) | 标签： [redis](http://www.importnew.com/tag/redis), [分布式](http://www.importnew.com/tag/%e5%88%86%e5%b8%83%e5%bc%8f)

分享到：

原文出处： [吴兆锋](http://wudashan.cn/2017/10/23/Redis-Distributed-Lock-Implement/" \t "_blank)

### 前言

分布式锁一般有三种实现方式：1. 数据库乐观锁；2. 基于Redis的分布式锁；3. 基于ZooKeeper的分布式锁。本篇博客将介绍第二种方式，基于Redis实现分布式锁。虽然网上已经有各种介绍Redis分布式锁实现的博客，然而他们的实现却有着各种各样的问题，为了避免误人子弟，本篇博客将详细介绍如何正确地实现Redis分布式锁。

### 可靠性

首先，为了确保分布式锁可用，我们至少要确保锁的实现同时满足以下四个条件：

1. 互斥性。在任意时刻，只有一个客户端能持有锁。
2. 不会发生死锁。即使有一个客户端在持有锁的期间崩溃而没有主动解锁，也能保证后续其他客户端能加锁。
3. 具有容错性。只要大部分的Redis节点正常运行，客户端就可以加锁和解锁。
4. 解铃还须系铃人。加锁和解锁必须是同一个客户端，客户端自己不能把别人加的锁给解了。

### 代码实现

### 组件依赖

首先我们要通过Maven引入Jedis开源组件，在pom.xml文件加入下面的代码：

|  |  |
| --- | --- |
| 1  2  3  4  5 | <dependency>      <groupId>redis.clients</groupId>      <artifactId>jedis</artifactId>      <version>2.9.0</version>  </dependency> |

### 加锁代码

**正确姿势**

Talk is cheap, show me the code。先展示代码，再带大家慢慢解释为什么这样实现：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26 | public class RedisTool {        private static final String LOCK\_SUCCESS = "OK";      private static final String SET\_IF\_NOT\_EXIST = "NX";      private static final String SET\_WITH\_EXPIRE\_TIME = "PX";        /\*\*       \* 尝试获取分布式锁       \* @param jedis Redis客户端       \* @param lockKey 锁       \* @param requestId 请求标识       \* @param expireTime 超期时间       \* @return 是否获取成功       \*/      public static boolean tryGetDistributedLock(Jedis jedis, String lockKey, String requestId, int expireTime) {            String result = jedis.set(lockKey, requestId, SET\_IF\_NOT\_EXIST, SET\_WITH\_EXPIRE\_TIME, expireTime);            if (LOCK\_SUCCESS.equals(result)) {              return true;          }          return false;        }    } |

可以看到，我们加锁就一行代码：jedis.set(String key, String value, String nxxx, String expx, int time)，这个set()方法一共有五个形参：

* 第一个为key，我们使用key来当锁，因为key是唯一的。
* 第二个为value，我们传的是requestId，很多童鞋可能不明白，有key作为锁不就够了吗，为什么还要用到value？原因就是我们在上面讲到可靠性时，分布式锁要满足第四个条件解铃还须系铃人，通过给value赋值为requestId，我们就知道这把锁是哪个请求加的了，在解锁的时候就可以有依据。requestId可以使用UUID.randomUUID().toString()方法生成。
* 第三个为nxxx，这个参数我们填的是NX，意思是SET IF NOT EXIST，即当key不存在时，我们进行set操作；若key已经存在，则不做任何操作；
* 第四个为expx，这个参数我们传的是PX，意思是我们要给这个key加一个过期的设置，具体时间由第五个参数决定。
* 第五个为time，与第四个参数相呼应，代表key的过期时间。

总的来说，执行上面的set()方法就只会导致两种结果：1. 当前没有锁（key不存在），那么就进行加锁操作，并对锁设置个有效期，同时value表示加锁的客户端。2. 已有锁存在，不做任何操作。

心细的童鞋就会发现了，我们的加锁代码满足我们可靠性里描述的三个条件。首先，set()加入了NX参数，可以保证如果已有key存在，则函数不会调用成功，也就是只有一个客户端能持有锁，满足互斥性。其次，由于我们对锁设置了过期时间，即使锁的持有者后续发生崩溃而没有解锁，锁也会因为到了过期时间而自动解锁（即key被删除），不会发生死锁。最后，因为我们将value赋值为requestId，代表加锁的客户端请求标识，那么在客户端在解锁的时候就可以进行校验是否是同一个客户端。由于我们只考虑Redis单机部署的场景，所以容错性我们暂不考虑。

**错误示例1**

比较常见的错误示例就是使用jedis.setnx()和jedis.expire()组合实现加锁，代码如下：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | public static void wrongGetLock1(Jedis jedis, String lockKey, String requestId, int expireTime) {        Long result = jedis.setnx(lockKey, requestId);      if (result == 1) {          // 若在这里程序突然崩溃，则无法设置过期时间，将发生死锁          jedis.expire(lockKey, expireTime);      }    } |

setnx()方法作用就是SET IF NOT EXIST，expire()方法就是给锁加一个过期时间。乍一看好像和前面的set()方法结果一样，然而由于这是两条Redis命令，不具有原子性，如果程序在执行完setnx()之后突然崩溃，导致锁没有设置过期时间。那么将会发生死锁。网上之所以有人这样实现，是因为低版本的jedis并不支持多参数的set()方法。

**错误示例2**

这一种错误示例就比较难以发现问题，而且实现也比较复杂。实现思路：使用jedis.setnx()命令实现加锁，其中key是锁，value是锁的过期时间。执行过程：1. 通过setnx()方法尝试加锁，如果当前锁不存在，返回加锁成功。2. 如果锁已经存在则获取锁的过期时间，和当前时间比较，如果锁已经过期，则设置新的过期时间，返回加锁成功。代码如下：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25 | public static boolean wrongGetLock2(Jedis jedis, String lockKey, int expireTime) {        long expires = System.currentTimeMillis() + expireTime;      String expiresStr = String.valueOf(expires);        // 如果当前锁不存在，返回加锁成功      if (jedis.setnx(lockKey, expiresStr) == 1) {          return true;      }        // 如果锁存在，获取锁的过期时间      String currentValueStr = jedis.get(lockKey);      if (currentValueStr != null && Long.parseLong(currentValueStr) < System.currentTimeMillis()) {          // 锁已过期，获取上一个锁的过期时间，并设置现在锁的过期时间          String oldValueStr = jedis.getSet(lockKey, expiresStr);          if (oldValueStr != null && oldValueStr.equals(currentValueStr)) {              // 考虑多线程并发的情况，只有一个线程的设置值和当前值相同，它才有权利加锁              return true;          }      }        // 其他情况，一律返回加锁失败      return false;    } |

那么这段代码问题在哪里？1. 由于是客户端自己生成过期时间，所以需要强制要求分布式下每个客户端的时间必须同步。 2. 当锁过期的时候，如果多个客户端同时执行jedis.getSet()方法，那么虽然最终只有一个客户端可以加锁，但是这个客户端的锁的过期时间可能被其他客户端覆盖。3. 锁不具备拥有者标识，即任何客户端都可以解锁。

### 解锁代码

**正确姿势**

还是先展示代码，再带大家慢慢解释为什么这样实现：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24 | public class RedisTool {        private static final Long RELEASE\_SUCCESS = 1L;        /\*\*       \* 释放分布式锁       \* @param jedis Redis客户端       \* @param lockKey 锁       \* @param requestId 请求标识       \* @return 是否释放成功       \*/      public static boolean releaseDistributedLock(Jedis jedis, String lockKey, String requestId) {            String script = "if redis.call('get', KEYS[1]) == ARGV[1] then return redis.call('del', KEYS[1]) else return 0 end";          Object result = jedis.eval(script, Collections.singletonList(lockKey), Collections.singletonList(requestId));            if (RELEASE\_SUCCESS.equals(result)) {              return true;          }          return false;        }    } |

可以看到，我们解锁只需要两行代码就搞定了！第一行代码，我们写了一个简单的Lua脚本代码，上一次见到这个编程语言还是在《[黑客与画家](http://www.amazon.cn/gp/product/B004WHZGZQ/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&tag=importnew-23&linkCode=as2&camp=536&creative=3200&creativeASIN=B004WHZGZQ" \t "_blank" \o "黑客与画家:硅谷创业之父Paul Graham文集)》里，没想到这次居然用上了。第二行代码，我们将Lua代码传到jedis.eval()方法里，并使参数KEYS[1]赋值为lockKey，ARGV[1]赋值为requestId。eval()方法是将Lua代码交给Redis服务端执行。

那么这段Lua代码的功能是什么呢？其实很简单，首先获取锁对应的value值，检查是否与requestId相等，如果相等则删除锁（解锁）。那么为什么要使用Lua语言来实现呢？因为要确保上述操作是原子性的。关于非原子性会带来什么问题，可以阅读【[解锁代码-错误示例2](http://wudashan.cn/2017/10/23/Redis-Distributed-Lock-Implement/" \l "releaseLock-wrongDemo2" \t "_blank)】 。那么为什么执行eval()方法可以确保原子性，源于Redis的特性，下面是官网对eval命令的部分解释：

## 单点登录

https://www.cnblogs.com/ywlaker/p/6113927.html

# 性能优化

# 安全攻防

# 需要看的相关书籍

jvm、多线程、redis、mq