作者：轩辕志远  
链接：https://www.zhihu.com/question/19786827/answer/28752144  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

1. 由于HTTP协议是无状态的协议，所以服务端需要记录用户的状态时，就需要用某种机制来识具体的用户，这个机制就是Session.典型的场景比如购物车，当你点击下单按钮时，由于HTTP协议无状态，所以并不知道是哪个用户操作的，所以服务端要为特定的用户创建了特定的Session，用用于标识这个用户，并且跟踪用户，这样才知道购物车里面有几本书。这个Session是保存在服务端的，有一个唯一标识。在服务端保存Session的方法很多，内存、数据库、文件都有。集群的时候也要考虑Session的转移，在大型的网站，一般会有专门的Session服务器集群，用来保存用户会话，这个时候 Session 信息都是放在内存的，使用一些缓存服务比如Memcached之类的来放 Session。  
2. 思考一下服务端如何识别特定的客户？这个时候Cookie就登场了。每次HTTP请求的时候，客户端都会发送相应的Cookie信息到服务端。实际上大多数的应用都是用 Cookie 来实现Session跟踪的，第一次创建Session的时候，服务端会在HTTP协议中告诉客户端，需要在 Cookie 里面记录一个Session ID，以后每次请求把这个会话ID发送到服务器，我就知道你是谁了。有人问，如果客户端的浏览器禁用了 Cookie 怎么办？一般这种情况下，会使用一种叫做URL重写的技术来进行会话跟踪，即每次HTTP交互，URL后面都会被附加上一个诸如 sid=xxxxx 这样的参数，服务端据此来识别用户。  
3. Cookie其实还可以用在一些方便用户的场景下，设想你某次登陆过一个网站，下次登录的时候不想再次输入账号了，怎么办？这个信息可以写到Cookie里面，访问网站的时候，网站页面的脚本可以读取这个信息，就自动帮你把用户名给填了，能够方便一下用户。这也是Cookie名称的由来，给用户的一点甜头。  
所以，总结一下：  
Session是在服务端保存的一个数据结构，用来跟踪用户的状态，这个数据可以保存在集群、数据库、文件中；  
Cookie是客户端保存用户信息的一种机制，用来记录用户的一些信息，也是实现Session的一种方式。

类似这种面试题，实际上都属于“开放性”问题，你扯到哪里都可以。不过如果我是面试官的话，我还是希望对方能做到一点——

不要混淆 session 和 session 实现。

本来 session 是一个抽象概念，开发者为了实现中断和继续等操作，将 user agent 和 server 之间一对一的交互，抽象为“会话”，进而衍生出“会话状态”，也就是 session 的概念。

而 cookie 是一个实际存在的东西，http 协议中定义在 header 中的字段。可以认为是 session 的一种后端无状态实现。

而我们今天常说的 “session”，是为了绕开 cookie 的各种限制，通常借助 cookie 本身和后端存储实现的，一种更高级的会话状态实现。

所以 cookie 和 session，你可以认为是同一层次的概念，也可以认为是不同层次的概念。具体到实现，session 因为 session id 的存在，通常要借助 cookie 实现，但这并非必要，只能说是通用性较好的一种实现方案。

作者：欲三更  
链接：https://www.zhihu.com/question/19786827/answer/84540780  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

1，session 在服务器端，cookie 在客户端（浏览器）  
2，session 默认被存在在服务器的一个文件里（不是内存）  
3，session 的运行依赖 session id，而 session id 是存在 cookie 中的，也就是说，如果浏览器禁用了 cookie ，同时 session 也会失效（但是可以通过其它方式实现，比如在 url 中传递 session\_id）  
4，session 可以放在 文件、数据库、或内存中都可以。  
5，用户验证这种场合一般会用 session

因此，维持一个会话的核心就是客户端的唯一标识，即 session id

作者：冯特罗  
链接：https://www.zhihu.com/question/19786827/answer/21643186  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

作者：郭无心  
链接：https://www.zhihu.com/question/19786827/answer/66706108  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

**COOKIE和SESSION有什么区别？**  
**cookie保存在客户端，session保存在服务器端，**  
**cookie**目的可以**跟踪会话，**也可以**保存用户喜好或者保存用户名密码**  
**session用来跟踪会话**  
  
**①**当我们登录网站勾选保存用户名和密码的时候，一般保存的都是cookie，将用户名和密码的cookie保存到硬盘中，这样再次登录的时候浏览器直接将cookie发送到服务端验证，直接username和password保存到客户端，当然这样不安全，浏览器也可以加密解密这样做，每个浏览器都可以有自己的加密解密方式，这样方便了用户，再比如用户喜欢的网页背景色，比如QQ空间的背景，这些信息也是可以通过cookie保存到客户端的，这样登录之后直接浏览器直接就可以拿到相应的偏好设置。  
  
②跟踪会话，比如某些网站中网页有不同的访问权限，有只能登录的用户访问的网页或者用户级别不同不能访问的，但是http请求是无状态的，每次访问服务端是不知道是否是登录用户，很自然的想到在http请求报文中加入登录标识就可以了，这个登录标识就可以是cookie，这样的cookie服务端要保存有所有登录用户的cookie，这样请求报文来了之后拿到登录标识cookie，在服务端进行比较久可以了。再比如购物网站，多次点击添加商品到购物车客户端很容易知道哪些物品在购物车中，但是服务端怎么知道每次添加的物品放到哪个登录用户的购物车中呢？也需要请求报文中带着cookie才行（在不登陆的情况下京东也是可以不断添加商品的，推测应该是登录的时候一并创建cookie并且发送物品信息），这些cookie都是为了跟踪会话用的，所以客户端有，服务端也有，并且服务端有全部的会话cookie。  
  
后面衍生出session技术,session技术是要使用到cookie的，之所以出现session技术，主要是为了安全。

http是无状态的协议，客户每次读取web页面时，服务器都打开新的会话，而且服务器也不会自动维护客户的上下文信息，那么要怎么才能实现网上商店中的购物车呢，session就是一种保存上下文信息的机制，它是针对每一个用户的，变量的值保存在服务器端，通过SessionID来区分不同的客户,session是以cookie或URL重写为基础的，默认使用cookie来实现，系统会创造一个名为JSESSIONID的输出cookie，我们叫做session cookie,以区别persistent cookies,也就是我们通常所说的cookie,注意session cookie是存储于浏览器内存中的，并不是写到硬盘上的，这也就是我们刚才看到的JSESSIONID，我们通常情是看不到JSESSIONID的，但是当我们把浏览器的cookie禁止后，web服务器会采用URL重写的方式传递Sessionid，我们就可以在地址栏看到 sessionid=KWJHUG6JJM65HS2K6之类的字符串。

<img src="https://pic1.zhimg.com/50/249c3f10f411af56640113b615c972be\_hd.jpg" data-rawwidth="897" data-rawheight="529" class="origin\_image zh-lightbox-thumb" width="897" data-original="https://pic1.zhimg.com/249c3f10f411af56640113b615c972be\_r.jpg">大家请看在HTTP请求报文头的最后一行有cookie，不过是JSessionID的cookie值

Cookie: $Version=1; Skin=new;jsessionid=5F4771183629C9834F8382E23BE13C4C

比如前两个值，应该属于偏好设置之类的。

服务端是怎么知道客户端的多个请求是隶属于一个Session呢？注意到后台的那个jsessionid=5F4771183629C9834F8382E23BE13C4C木有？原来就是通过HTTP请求报文头的Cookie属性的jsessionid的值关联起来的！（当然也可以通过重写URL的方式将会话ID附带在每个URL的后面哦）。  
明白了原理，我们就可以很容易的分辨出persistent cookies和session cookie的区别了，网上那些关于两者安全性的讨论也就一目了然了，session cookie针对某一次会话而言，会话结束session cookie也就随着消失了，而persistent cookie只是存在于客户端硬盘上的一段文本（通常是加密的），而且可能会遭到cookie欺骗以及针对cookie的跨站脚本攻击，自然不如 session cookie安全了。

通常session cookie是不能跨窗口使用的，当你新开了一个浏览器窗口进入相同页面时，系统会赋予你一个新的sessionid，这样我们信息共享的目的就达不到了，此时我们可以先把sessionid保存在persistent cookie中，然后在新窗口中读出来，就可以得到上一个窗口SessionID了，这样通过session cookie和persistent cookie的结合我们就实现了跨窗口的session tracking（会话跟踪）。  
在一些web开发的书中，往往只是简单的把Session和cookie作为两种并列的http传送信息的方式，session cookies位于服务器端，persistent cookie位于客户端，可是session又是以cookie为基础的，明白的两者之间的联系和区别，我们就不难选择合适的技术来开发web service了。

部分参考自：[session与cookie的区别](https://link.zhihu.com/?target=http%3A//www.cnblogs.com/xulb597/archive/2012/07/02/2573252.html)  
  
===================分割线==============  
举个QQ空间的例子：  
① 当我们登录QQ空间的时候，可以选择保存用户名和密码，这样下次登录的时候浏览器可以自动填充或者自动登陆，此时使用的是cookie技术，将于

http://qzone.qq.com/

域名对应的cookie保存到硬盘中，下次访问的时候浏览器查找保存在硬盘中的与该域名对应的cookie填充。  
  
②登录之后，我们可能做些操作，比如删除日志，发表说说，这些只有登录用户才能做的事情可以使用cookie也可以使用session进行会话跟踪  
  
③空间的喜好设置可以保存到硬盘cookie当中。  
  
-------------------------------------------------------------------------------------------------------------------------  
其实说白了session就是用来保存会话的cookie。  
下面介绍下Java中Servlet的session管理

http://lavasoft.blog.51cto.com/62575/275589 深入理解HTTP Session

session在web开发中是一个非常重要的概念，这个概念很抽象，很难定义，也是最让人迷惑的一个名词，也是最多被滥用的名字之一，在不同的场合，session一次的含义也很不相同。这里只探讨HTTP Session。  
  
为了说明问题，这里基于Java Servlet理解Session的概念与原理，这里所说Servlet已经涵盖了JSP技术，因为JSP最终也会被编译为Servlet，两者有着相同的本质。  
  
在Java中，HTTP的Session对象用javax.servlet.http.HttpSession来表示。  
  
1、概念：Session代表服务器与浏览器的一次会话过程，这个过程是连续的，也可以时断时续的。在Servlet中，session指的是HttpSession类的对象，这个概念到此结束了，也许会很模糊，但只有看完本文，才能真正有个深刻理解。  
  
2、Session创建的时间是：  
一个常见的误解是以为session在有客户端访问时就被创建，然而事实是直到某server端程序调用 HttpServletRequest.getSession(true)这样的语句时才被创建，注意如果JSP没有显示的使用 <% @page session="false"%> 关闭session，则JSP文件在编译成Servlet时将会自动加上这样一条语句 HttpSession session = HttpServletRequest.getSession(true);这也是JSP中隐含的 session对象的来历。  
由于session会消耗内存资源，因此，如果不打算使用session，应该在所有的JSP中关闭它。  
  
引申：  
**1）、访问\*.html的静态资源因为不会被编译为Servlet，也就不涉及session的问题。**  
2）、当JSP页面没有显式禁止session的时候，在打开浏览器第一次请求该jsp的时候，服务器会自动为其创建一个session，并赋予其一个sessionID，发送给客户端的浏览器。**以后客户端接着请求本应用中其他资源的时候，会自动在请求头上添加：**  
**Cookie:JSESSIONID=客户端第一次拿到的session ID**  
这样，**服务器端在接到请求时候，就会收到session ID，**并根据ID在内存中找到之前创建的session对象，提供给请求使用。这也是session使用的基本原理----搞不懂这个，就永远不明白session的原理。  
下面是两次请求同一个jsp，请求头信息：  
  
**通过图可以清晰发现，第二次请求的时候，已经添加session ID的信息。**  
3、Session删除的时间是：  
1）Session超时：超时指的是连续一定时间服务器没有收到该Session所对应客户端的请求，并且这个时间超过了服务器设置的Session超时的最大时间。  
2）程序调用HttpSession.invalidate()  
3）服务器关闭或服务停止  
  
4、session存放在哪里：服务器端的内存中。**不过session可以通过特殊的方式做持久化管理。**  
  
5、session的id是从哪里来的，sessionID是如何使用的：当客户端第一次请求session对象时候，服务器会为客户端创建一个session，并将通过特殊算法算出一个session的ID，用来标识该session对象，当浏览器下次（session继续有效时）请求别的资源的时候，浏览器会偷偷地将sessionID放置到请求头中，服务器接收到请求后就得到该请求的sessionID，服务器找到该id的session返还给请求者（Servlet）使用。一个会话只能有一个session对象，对session来说是只认id不认人。  
  
6、session会因为浏览器的关闭而删除吗？  
不会，session只会通过上面提到的方式去关闭。  
  
7、同一客户端机器多次请求同一个资源，session一样吗？  
一般来说，每次请求都会新创建一个session。  
  
  
其实，这个也不一定的，总结下：对于多标签的浏览器（比如360浏览器）来说，在一个浏览器窗口中，多个标签同时访问一个页面，session是一个。对于多个浏览器窗口之间，同时或者相隔很短时间访问一个页面，session是多个的，**和浏览器的进程有关**。对于一个同一个浏览器窗口，直接录入url访问同一应用的不同资源，session是一样的。  
  
8、session是一个容器，可以存放会话过程中的任何对象。  
  
9、session因为请求（request对象）而产生，同一个会话中多个request共享了一session对象，可以直接从请求中获取到session对象。  
  
10、其实，session的创建和使用总在服务端，而浏览器从来都没得到过session对象。但浏览器可以请求Servlet（jsp也是Servlet）来获取session的信息。客户端浏览器真正紧紧拿到的是session ID，而这个对于浏览器操作的人来说，是不可见的，并且用户也无需关心自己处于哪个会话过程中。  
---------------------------------------------------------------------------------------------------  
比如下面一段使用session的代码

public void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException

{

response.setContentType("text/html");

response.setCharacterEncoding("utf-8");

PrintWriter out = response.getWriter();

// 得到用户名和密码，验证

String u = request.getParameter("username");

String p = request.getParameter("password");

UserBeanBO ubb = new UserBeanBO();

if (ubb.checkUser(u, p))

{

// 1.把成功登陆的用户所有信息放入session

UserBean ub = ubb.getUserBean(u);

request.getSession().setAttribute("userInfo", ub);

// 2.把购物车的信息取出

MyCartBO mcb = (MyCartBO)request.getSession().getAttribute("mycart");

ArrayList al = mcb.showMyCart();

// 把al放入request

request.setAttribute("mycartInfo", al);

// 用户合法

request.getRequestDispatcher("success.jsp").forward(request,response);

} else

{

// 用户不合法

request.getRequestDispatcher("error.jsp").forward(request, response);

}

}

HttpSession javax.servlet.http.HttpServletRequest.getSession()

Returns the current session associated with this request, or if the request

does not have a session, creates one.

Returns: the HttpSession associated with this request

See Also:

getSession(boolean)

javax.servlet.http.HttpServletRequest.getSession() 将会返回当前request相关联的HttpSession对象，如果不存在，将会创建一个。  
  
翻译一下，当一个浏览器请求来到之后，Servlet处理程序（Servlet容器内部实现）将会主动检查请求信息Cookie当中是否有JSESSIONID，若有，找到对应JSESSION的HttpSession对象，如果没有，创建一个，具体的机制在Servlet容器的实现当中。

**session management会话管理的原理**

web请求与响应基于http，而http是无状态协议。所以我们为了跨越多个请求保留用户的状态，需要利用某种工具帮助我们记录与识别每一次请求及请求的其他信息。举个栗子，我们在淘宝购物的时候，首先添加了一本《C++ primer》进入购物车，然后我们又继续去搜索《thinking in java》，继续添加购物车，这时购物车应该有两本书。但如果我们不采取session management会话管理的话，基于http无状态协议，我们在第二次向购物车发出添加请求时，他是无法知道我们第一次添加请求的信息的。所以，我们就需要session management会话管理！

**会话管理的基本方式**

会话管理的基本主要有隐藏域，cookies，与URL重写这几种实现方式。用得较多的是后两种。

**隐藏域实现会话管理**

以一个网络注册信息填写为例。  
我们在填注册信息的时候，经常遇到填完一个页面的内容之后，还要继续填写下一个页面的内容。但由于http的无状态，那么容易造成的后果，当进入第二页填写的时候，服务器已经不记得我们上一页填写了什么。  
怎么利用隐藏域解决这个问题呢？  
顾名思义，其实就是既然服务器不会记得两次请求间的关系，那就由浏览器在每次请求时主动告诉服务器多次请求间的必要信息，但是上一页的信息并不显示在第二页中，而是采用隐藏域的方式。  
然而显然这种方式是存在各种问题的。  
比如关掉网页之后，就会遗失信息，而且查看网页源代码时，容易暴露信息，安全性不高。隐藏域并不是servlet/jsp实际会话管理的机制。

**cookie实现会话管理**

cookie是什么？举个简单的例子，现在当我们浏览网站的时候，经常会自动保存账号与密码，这样下次访问的时候，就可以直接登录了。这种技术的实现就是利用了cookie技术。 **cookie是存储key-value对的一个文件，务必记住，它是由服务器将cookie添加到response里一并返回给客户端，然后客户端会自动把response里的cookie接收下来，并且保存到本地，下次发出请求的时候，就会把cookie附加在request里，服务器在根据request里的cookie遍历搜索是否有与之符合的信息**  
具体cookie的实现我们会在后面详细讲到

**URL重写实现会话管理**

URL重写就是将需要记录的信息附加在请求的链接背后，以链接参数的形式发送给服务器识别。具体实现的过程会在后文结合cookie详解。

**servlet&jsp中的session会话管理机制**

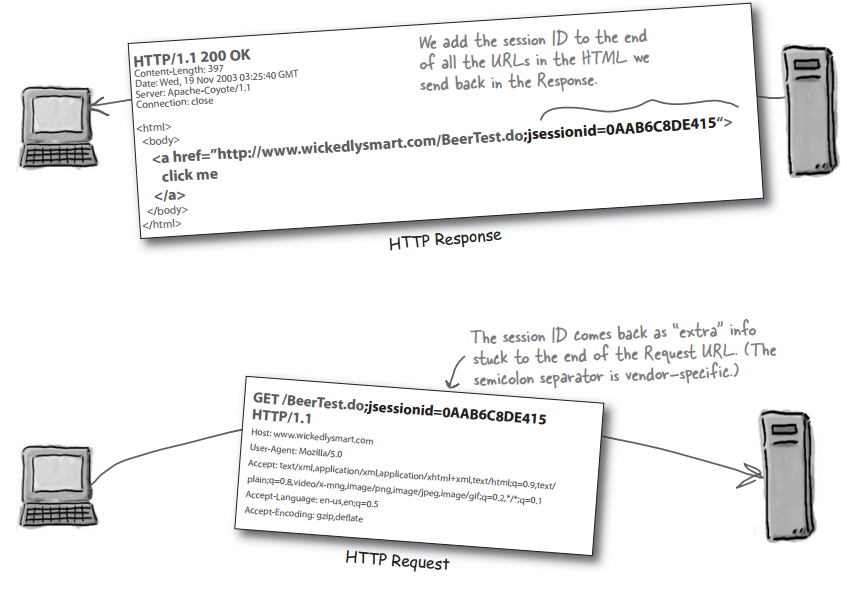
**利用httpsession对象进行会话管理。httpsession对象可以保存跨同一个客户多个请求的会话状态。**

换句话说，与一个特定客户的整个会话期间看，httpsession会持久储存。

**对于会话期间客户做的所有请求，从中得到的所有信息都可以用httpsession对象保存。**

**httpsession的工作机制**

* 以之前的问卷调查为例，当一个新客户小明填写问卷时，服务器会生成一个httpsession对象，用于保存会话期间小明所选择的信息，服务器会以setAttribute的方式将其保存到httpsession对象中。  
  每个客户会有一个独立的httpsession对象，保存这个客户所有请求所需要保存的信息。
* 服务器如何识别所有的请求是否来自同一个客户？  
  客户需要一个会话ID来标识自己。就跟我们每个人的身份证号一样。对于客户的第一个请求，容器会生成一个唯一的会话ID，并通过相应把它返回给用户，客户在以后发回一个请求中发回这个会话ID，容器看到ID之后，就会找到匹配的会话，并把这个会话与请求关联。
* **实现存储会话ID的就是通过cookie！**

[](http://upload-images.jianshu.io/upload_images/1234352-474c42b13e2d470d.png?imageMogr2/auto-orient/strip%7CimageView2/2/w/1240)

cookie存储在客户端，是被服务器放在response里发回客户端的，以后每次request时，都会把cookie加入到request里。  
而session是存在服务器的，以属性的形式将会话中的信息存到httpsession对象中。调用时，只要通过httpsession对象调用相应attribute即可。

* 很多地方总是把session与cookie分开单独讲。但我们通过前面的介绍，不难知道，session实现其会话管理机制时，在如何确定所有请求是否来自同一个客户时，是利用了cookie技术的。所以不应该将cookie与session完全分开讲。
* 这里产生这个误解的原因。是因为我们对session的会话管理机制不够了解。因为容器在创建session对象时，会帮我们实现所有cookie相关的工作，而我们只需要实现这一句：

|  |  |
| --- | --- |
| 1 | HttpSession session = request.getSession(); |

记住： **这个方法不只是创建一个会话，而是会完成所有与cookie相关的工作，只是容器都自动帮我们实现了。**我们来看看容器在背后默默为我们做了什么：

* 建立新的httpsession对象
* 生成唯一的会话ID
* 建立新的会话对象
* 把会话ID与cookie关联
* 在响应中设置cookie

cookie所有的工作都在后台进行。  
看到这里，是不是很爽？容器几乎帮我们实现了所有cookie工作。  
从请求中得到会话ID  
只需一行代码：

|  |  |
| --- | --- |
| 1 | HttpSession session = request.getSession(); |

与上一部分为响应生成会话ID是一致的  
其中也在后台实现了一些步骤：  
if（请求包含一个会话ID）  
找到与该ID匹配的会话  
else if（没有会话ID或者没有匹配的ID）  
创建一个新的会话。  
还是那句话： **cookie所有工作都在后台自动进行**

**cookie的更多用处**

cookie原先设计的初衷就是为了帮助支持会话状态。但是因为cookie的简便性，容器为我们封装了大量操作。现在cookie已经被越来越运用到各个方面。  
首先， **我们明确cookie是存在客户端的，实际上就是在客户端与服务端交换的一小段数据（一个name/string对）。**  
由于session在用户关闭浏览器后，会话结束，就会消失，cookie随之应该也会消失。但servlet的API中提供了一些方法，可以让客户端的cookie存活的时间更久一点。这就是cookie相对于session的一大优势所在。我们目前常用的记住用户名和密码，下次登录就是利用cookie在session消失后，还能存活实现的。  
所以，我们可以定制cookie为我们实现各种功能。