**Session和cookie**

当前问题现状：

想象一个包含“页面A”和“页面B”的网站，假设一个游客先看了A，然后在跳转到B。HTTP是无状态协议，因此，如果一个典型的web服务器正在管理这个站点，那么当访问者浏览到B时，在A上手机的任何知识都会丢失，换句话说，B不能利用访问者提供的任何信息。

为了绕过这个限制，应用服务器会检测访问者（即游客哈）何时首次进入网站。此时，应用服务器将启动此访问者的会话。在前面的示例中，当访问者请求A时，应用服务器将启动会话。网站设计人员可以使用A来收集访问者的信息，并将这些信息存储在会话变量中。会话变量中的信息对所有后续页面都可用。例如，如果路人甲向A提供他的年龄，A的设计人员将年龄写入一个session变量，那么B可以很容易地访问路人甲的年龄。

会话变量包含会话期间可用的值。当会话结束时，应用服务器将销毁与会话相关的会话变量。每个会话变量都消耗应用服务器上的内存，因此创建不必要的会话变量会影响性能。

Session:

由web站点创建/维护的会话变量

在创建会话时，WebCenter站点会自动创建以下会话变量:

|  |  |
| --- | --- |
| 会话变量 | 释义 |
| **SessionVariables.currentUser** | 游客登录的id |
| **SessionVariables.currentAcl** | 该游客所属的所有ACLs。如果游客没有显式登录，则默认ACL为浏览器。 |
| **SessionVariables.username** | 此游客登录的用户名。如果游客没有显式登录，默认用户名为DefaultReader。 |
| **SessionVariables.iniFile** | 包含web站点属性的文件的名称 |

举例“登录和退出”：

当游客第一次访问站点时，Web站点会创建一个会话，并在游客中隐式地将其日志记录为DefaultReader。在会话期间，如果游客显式地登录，Web站点会自动更新SessionVariables.currentUser,SessionVariables.currentAcl,SessionVariables.username。登录不会影响任何其他会话变量的值。换句话说，如果页面在登录之前创建会话变量，那么这些值在登录之后仍然有效。当一个游客显式地注销时，Web所生成的会话变量会自动恢复到在登录之前所持有的值。例如，考虑顺序如下:

1. 游客首先访问一个页面，SessionVariables.username的值是DefaultReader。
2. 游客登录为“路人甲”，那么SessionVariables.username的值就是“路人甲”。
3. 如果“路人甲”注销，则SessionVariables.username的值更新为DefaultReader。

会话的生命周期：

当访问者第一次访问您的网站时，会话就开始了。下列任何一项发生时，会议结束:

1、访问者关闭浏览器。

2、会话超时了。Web服务器站点使用timeout属性设置应用服务器中的会话超时值。如果将此属性设置为300，那么用户会话将在300秒或5分钟内无效。

3、系统管理员停止应用程序服务器。（也就是停掉服务）

Cookie:

cookie是应用程序（即web服务站点）写入游客浏览器的字符串。cookie存储会话之间的游客信息。游客的浏览器将该字符串写入游客磁盘上的一个特殊cookie文件。当游客返回到您的网站时，游客的浏览器将cookie的副本发送回设置它的web服务器。一旦创建了一个cookie，它就可以作为一个变量用于页面上。

例如，您的应用程序可能将游客最喜欢的运动队存储在一个cookie中。然后，当游客返回时，应用程序可以检索cookie并使用它的信息在横幅中显示这些信息。

Cookie属性：

|  |  |
| --- | --- |
| 属性 | 值 |
| **name** | cookie的名称。它还充当包含cookie值的传入变量的名称。  重要提示:Web站点页面上下文中的cookie被视为变量。因此，当cookie和资产属性共享相同的名称时，它们被视为相同的变量。 |
| **expiration** | 时间，以秒为单位，此后cookie不再被发送到web服务器。 |
| **security** | 可选地在cookie上设置安全性。 |
| **URL** | 限制仅在此URL上发送cookie |
| **Domain** | 限制只将cookie发送到指定域中的url。 |

因为cookie中的信息是关键的，cookie是一种安全威胁，一些游客设置浏览器来拒绝存储cookie。应用程序必须为此做好准备。

Cookie的生命生命周期：

1. 当不再需要cookie时，可以删除它们。
2. 过期

提示和技巧：

1. 在集群中，必须跨集群成员复制会话状态。在集群中，尽量将会话大小保持在最小;不要为每个客户端存储超过2千字节的会话数据。
2. 确定合理的会话超时值。设置太大的超时会占用系统资源。设置太小会迫使访问者以恼人的频率登录。
3. 客户端禁用cookie则可url访问地址后加上会话ID

例如：FlushServer?reset=true&username=username&password=password&

ssid=sessionID