基于 SUN AM 的 Domino 系统单点登录设计与实现①

朱吉军[1] 王志敏[2]

（1. 大庆油田有限责任公司 勘探开发研究院 黑龙江 大庆 163712；2. 大庆油田有限责任公司 化工集团甲醇分公司 黑龙江 大庆 163712）

摘 要：基于 SUN AM 的 Domino 单点登录解决方案目前 SUN、IBM 公司都没有一个企业级的解决方案，而目前的解决方案是通过代填口令实现的，这样一旦截获用户口令，将有可能造成不可估量的损失。在深入分析 Domino 的 DSAPI 技术、Domino Session 产生机制，依据 SUN AM 流程，设计了出了基于 SUN AM 的 Domino 单点登录流程并进行了实现，解决了基于 SUN AM 的 Domino 单点登录技术瓶颈，为企业业务整合提供了企业级的解决方案。

关键词：单点登录 SSO;SUN AM;Domino;DSAPI

Design and Implementation of Single Sign-On Solution for System Domino Based on SUN AM

ZHU Ji-Jun[1], WANG Zhi-Min[2] (1. Daqing Oilfield Company E&D Research Institute,Daqing,163712, China; 2. Methanol Branch of Daqing Oilfield Chemical Industry Company, Daqing 163712, China)

Abstract: The company of SUN and IBM do not have a good enterprise solution for SSO based on sun am for Domino system. The solution is currently achieved through the password. So, if intercepted by a user's password, it will result in incalculable damage, and will not conform to the concept of SSO. The AM SSO solution for Domino is designed after analyzing the technology of domino's DSAPI, the generation mechanism of domino session, and the AM SSO process. It has solved the technology bottlenecks of SSO based on SUN for domino system, and provided a enterprise solution for enterprise business Integration

Keywords: SSO; SUN AM; Domino; DSAPI

企业业务整合解决方案之一就是单点登录[1](Single Sign On)技术，简称为 SSO。使用“单点登录”整合后[2]，只需要登录一次就可以进入多个系统，而不需要重新登录，这不仅仅带来了更好的用户体验，更重要的是降低了安全的风险和管理的消耗；“单点登录”还是 SOA 时代的需求之一，在面向服务的架构中，服务和服务之间，程序和程序之间的通讯大量存在，服务之间的安全认证是 SOA 应用的难点之一，因此建立“单点登录”的系统体系能够大大简化 SOA 的安全问题，提高服务之间的合作效率。通过实施单点登录功能，使用户只需一次登录就可以根据相关的规则去访问不同的应用系统，提高信息系统的易用性、安全性、稳定性；在此基础上进一步实现企业用户高速协同办公和企业知识管理功能。

① 收稿时间:2009-11-25;收到修改稿时间:2010-01-08

但是在基于SUN AM的单点登录解决方案中，很难将Domino系统整合起来，而企业由于历史原因又很多Domino系统，鉴于此，本文在深入分析Domino的DSAPI技术和SUN AM的单点登录流程的基础上，设计并实现了基于SUN AM的Domino单点登录技术，解决了基于SUN AM的Domino系统的单点登录技术瓶颈。

1　现有解决方案分析

(1)SUN公司解决方案　在AM6.5中SUN提供了一个Domino Agent，但是在实施过程中发现这个Agent加入Domino之后，系统非常慢，而且安全性也不好控制；AM 8.0中(现在叫OpenSSO)已经不提供Domino的解决方案，彻底放弃了这种Agent思路。

(2)IBM Domino解决方案　IBM Domino有自己的一整套单点登录解决方案，不可能开发这个Agent来推动竞争伙伴产品发展。

(3)代填口令　代填口令也是一种单点登录技术解决方案，但安全性(用户口令可以通过http截获；Domino管理员也可以在Domino日志中看见用户口令)、集成性不好，并对Domino Server产生额外的压力(同一个用户产生多个Session)；这样一旦用户口令泄密，将有可能给企业造成不可估量的损失，以在企业解决方案不到万不得已的时候不建议采用。

2　SUN AM登录原理

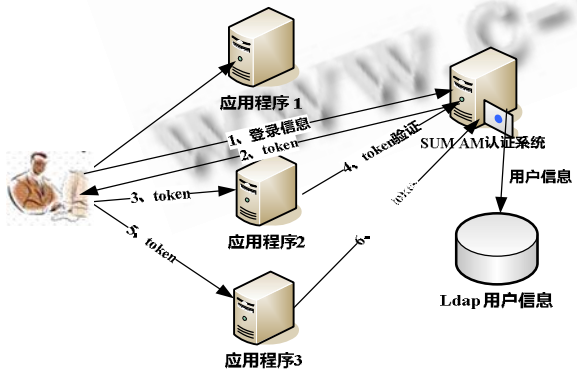

图1　SUN AM登录原理

用户通过AM的认证页面进行认证，认证通过之后，平台为该用户创建一个单点登录令牌[3]，并将该令牌的ID通过cookie返回至用户浏览器；当用户访问WEB应用系统时，单点登录令牌ID自动通过cookie传递至WEB应用系统,WEB应用系统可以通过单点登录令牌ID还原单点登录令牌，并向Access Manager验证单点登录令牌是否有效。如果有效，则应用系统可以从单点登录令牌获取用户身份信息，而不再需要用户进行再次认证。

3　Domino的DSAPI技术原理

Domino网络服务器应用程序编程接口(Domino Web Server Application Programming Interface, DSAPI)为Web用户定制用户名和口令认证。DSAPI是一个C语言的应用程序编程接口，它可以为Domino服务器编写自己的扩展（extensions）。在处理HTTP请求过程中，每当一个特殊事件发生时，DSAPI过滤器(filter)就会被触发。一个DSAPI过滤器的运行过程如图2所示。

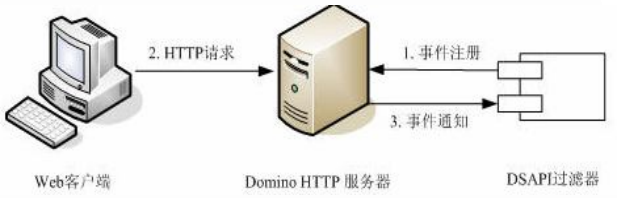

图2　Domino中DSAPI过滤器运行流程

具体流程为：

① 事件注册　一个DSAPI过滤器允许你定制HTTP请求的处理过程。但是只有DSAPI过滤器已经声明支持这个事件，服务器才会把该事件交给DSAPI过滤器处理。所以，DSAPI过滤器首先要注册自己声明的事件。目前一共有13种事件可以被DSAPI过滤器所捕捉到。一个DSAPI过滤器所能支持的事件数目取决于你的设计和具体实现，理论上它可以支持任意多个事件。DSAPI接口的实现依赖于过滤器声明它所支持的事件。

② HTTP请求　Web客户端发起一个HTTP请求给Domino HTTP服务器。

③ 事件通知　当Domino服务器在接收到一个HTTP请求时，它会判断这个请求事件的类型。如果某个DSAPI过滤器已经声明支持这个事件，服务器就会把这个HTTP事件交给这个DSAPI过滤器处理。这样，当一个用户访问服务器上的某个资源时，

就可以使用自定义的认证过程来代替正常的 Domino Web 认证过程。

3.1 DSAPI 实现

在 Windows 平台上进行开发，并使用 Microsoft Visual C++ 6.0 作为开发工具。整个过程包括四个步骤：

(1)DSAPI 过滤器的实现 Windows 环境下，它被编译成一个动态连接库。首先我们使用 Visual C++ 创建一个工程，并完成相关的配置：

• 使用 Visual C++，创建一个 Win32 动态连接库的工程

• 设定相应的路径，主要包括 Lotus C API 的头文件路径和 Lib 文件路径，可以在下载的 Lotus C API Toolkits 中找到相应的路径。

然后需要实现最基本的两个入口函数。

①初始 unsigned int FilterInit(FilterInitData* filterInitData){…},注册事件，具体事件类型见 DSAPI 手册。

② 事件通知 unsignedint HttpFilterProc (FilterContext*pContext, unsigned int event-Type, void* pEventData) {…}，注册事件处理。

(2) Domino 服务器的配置 把代码编译，链接成功后得到的 DLL 文件拷贝到 domino 服务器的程序目录中，然后在 Domino 服务器上注册 DSAPI 过滤器。配置如图 3。

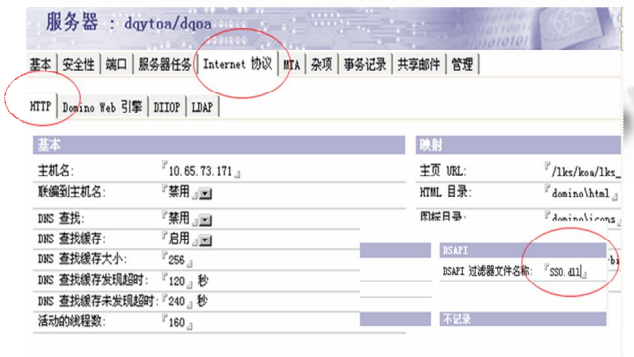

图 3 Domino DSAPI 配置

4 认证方式设计实现及应用案例

4.1 认证方式设计实现

通过分析 SUM AM 的单点登录流程，结合 Domino DSAPI 技术，设计出单点登录流程[4,5]。如图 4。

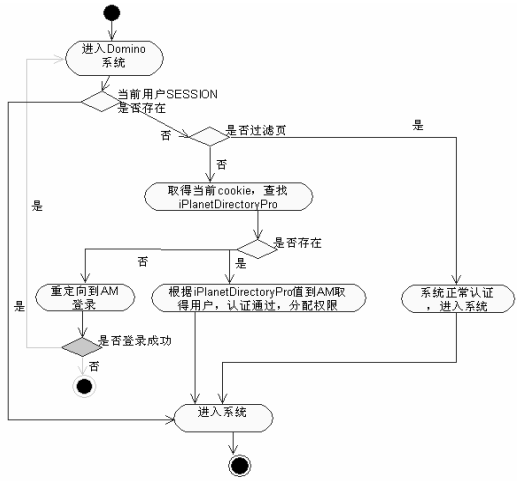

图 4 基于 AM 的 Domino SSO 流程

其中 iPlanetDirectoryPro 为 AM 为当前用户产生的令牌。要实现上述流程，关键要实现如何通过 DSAPI 取得 cookie，如何建立 Domino Session，因为如果不建立 session，用户信息将不能进入 cache，导致对页面的每一种资源都要重复认证，严重影响系统性能。

① cookie 取得

在 DSAPI 中 cookie 取得如下：

pAuthenticateData->GetHeader(pContext, "Cookie", cookieBuf, sizeof(cookieBuf)-1, &dwError);

其中 pContext：FilterContext；

pAuthenticateData：FilterAuthenticate 事件所对应的结构类型为

② Domino Session 建立

按照 DSAPI 的官方资料设计之后，当认证一次之后，认证信息无法进入 Cache，也就是这个用户的 session 没有建立起来；通过分析 Domino Web 流程知道，session 是通过用户进入 names.nsf 登录之后建立起来，那么我可以通过 DSAPI 中重定向假登录来触发 session 的建立，如下：

```
sprintf(redirectURL,"%s/names.nsf?login&username=%s&Password=123&redirectto=%s",serverPath,user,serverPath);//password 可以随便给目的只是触发 Domino Session 产生
sprintf(redirectURL,"Location: %s\r\n\r\n\r\n",url);
customHeaders.responseCode=301;
// 重定向代码
```

```
customHeaders.reasonText="Moved Permanently";
customHeaders.headerText=redirectURL;
context->ServerSupport(context,kWriteResponseHeaders,&customHeaders,0,0,&errid);
authData->authType=kAuthenticBasic;
return kFilterHandledEvent;
```

其中 serverPath 为服务器地址。这样以来通过重定向，就可以让 Domino 系统建立 user 这个从 AM 中取得用户的 Domino Session，将当前用户加入 cache 中，可以避免重复授权，提高了系统性能。

4.2 实际应用案例

将编译好的动态库配置入 Domino 的 DSAPI 项之后，启动浏览器输入某企业 Domino 系统 URL，这时当用户还没有登录其它的单点登录系统，由于浏览器没有 SUN AM 产生的令牌 Token，这时会定位到 SUN AM 登录界面进行，登录如图 5 所示。

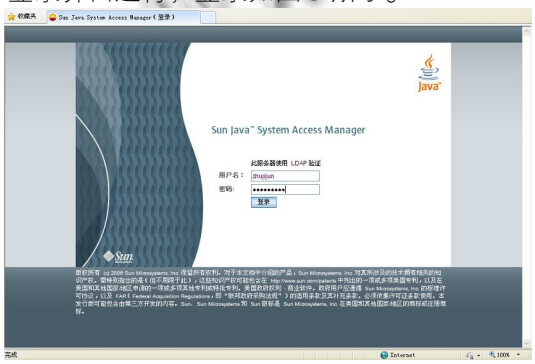

图 5　浏览器不存在 Token，登录 Domino 系统

当输入合法用户，浏览器会直接跳转进入 Domino 系统，不需要重新输入用户名和口令。

当用户已经登录了其它单点登录系统，然后登录 Domino 系统，系统直接进入不需要输入口令，如图 6 所示。

图 6　浏览器存在 Token，登录 Domino 系统

5　结语

通过分析 SUN AM 的单点登录原理、Domino DSAPI 开发接口、Domino Session 产生机制，在技术上实现了基于 SUN AM 的 Domino 单点登录解决方案，避免了使用代填口令方式，解决了基于 SUN AM 的 Domino 单点登录技术瓶颈，为企业业务整合提供更高的安全性并提供了真正的单点登录流程。

参考文献

1 陈观林,张泳. 企业信息门户单点登录系统的设计与实现.计算机系统应用. 2008,17(8):2－5.
2 皮晓东.单点登录的研究与实现. 计算机应用与软件. 2007,24(6):156－158.
3 李蔷,陈钢.基于 AM 的单点登录(SSO)解决方案.电脑知识与技术. 2008,(5):871－874.
4 刘润达,诸云强,宋佳等.一种简单跨域单点登录系统的实现.计算机应用, 2007,27(2):288－291.
5 谭立球,费耀平，李建华.企业信息门户单点登录系统的实现.计算机工程, 2005,31(17):102－104.