Single Sign-On

Mateus Nicolas
Mathov Camila
Tisera Lucas

¿SSO qué es y para qué sirve?

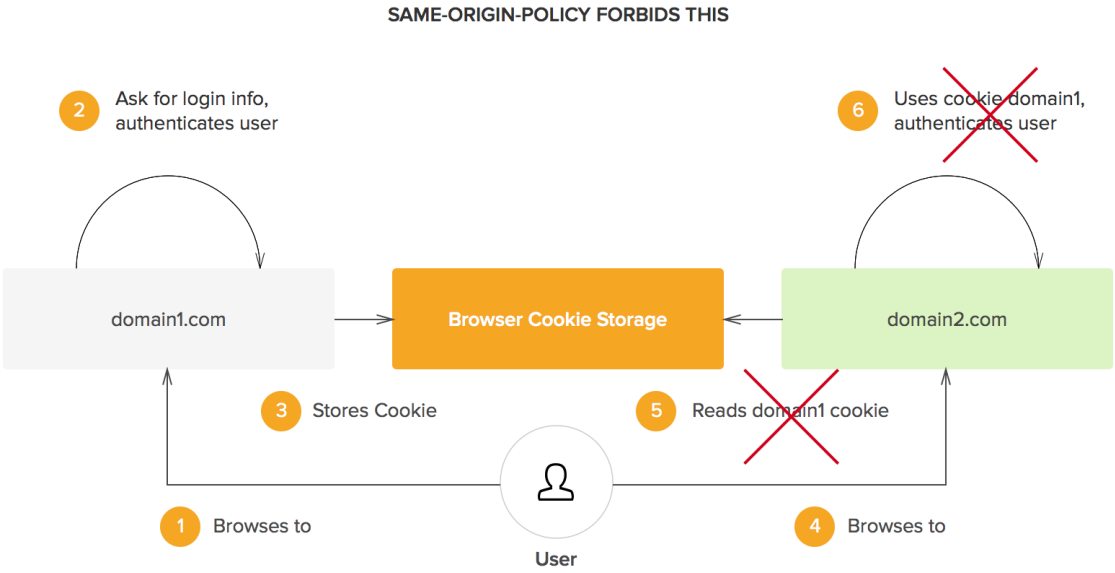
Single Sign On conocido también como SSO por sus siglas en inglés permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos. El SSO es de gran utilidad cuando existen diferentes sistemas a los que es posible acceder mediante una única contraseña y se desea evitar el ingreso repetitivo de estas cada vez que el usuario se desconecte del servicio. Para los usuarios supone una gran comodidad ya que identificándose solo una vez es posible mantener la sesión válida para el resto de las aplicaciones que hacen uso del SSO.

Ventajas	Desventajas
Acelera el acceso de los usuarios a sus aplicaciones	Utilizar una única combinación aumenta las probabilidades de vulnerabilidad de contraseñas
Reduce la carga de memorizar diversas contraseñas	Al fallar SSO se pierde acceso a todos los sistemas relacionados
Fácil de implementar y conectar a nuevas fuentes de datos	Suplantación de identidades en los accesos externos de los usuarios

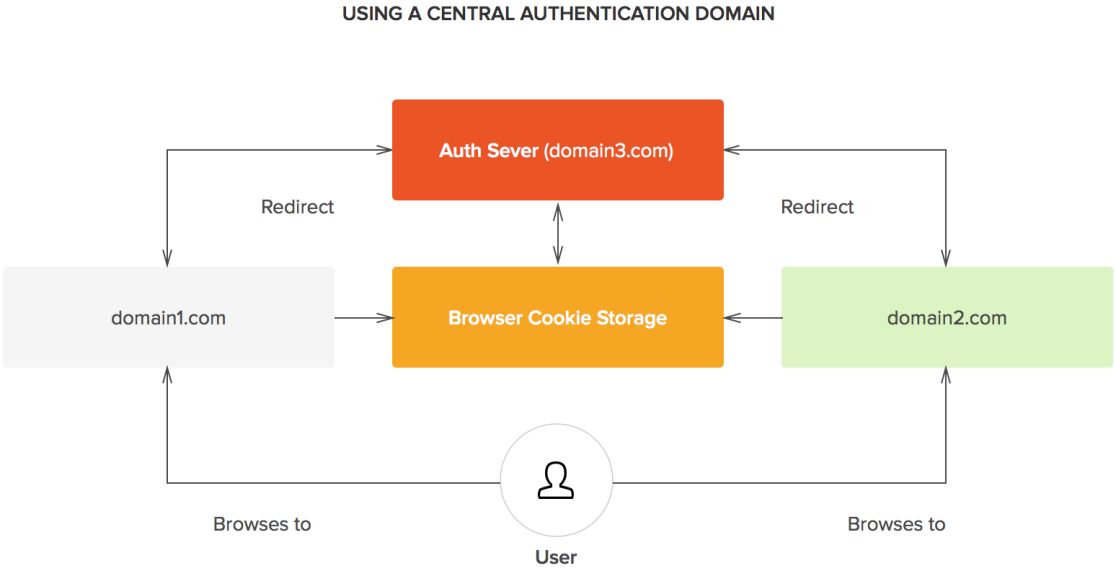
Funcionamiento basico

Eventualmente los desarrolladores web se enfrentan a un problema: ya han creado una aplicación en el dominio X y ahora quieren que su nuevo desarrollo en el dominio Y use la mima información para el inicio de sesion que el otro dominio. De hecho quieren aun mas, quieren que los usuarios que ya están conectados en el dominio X estén también conectados al dominio Y.

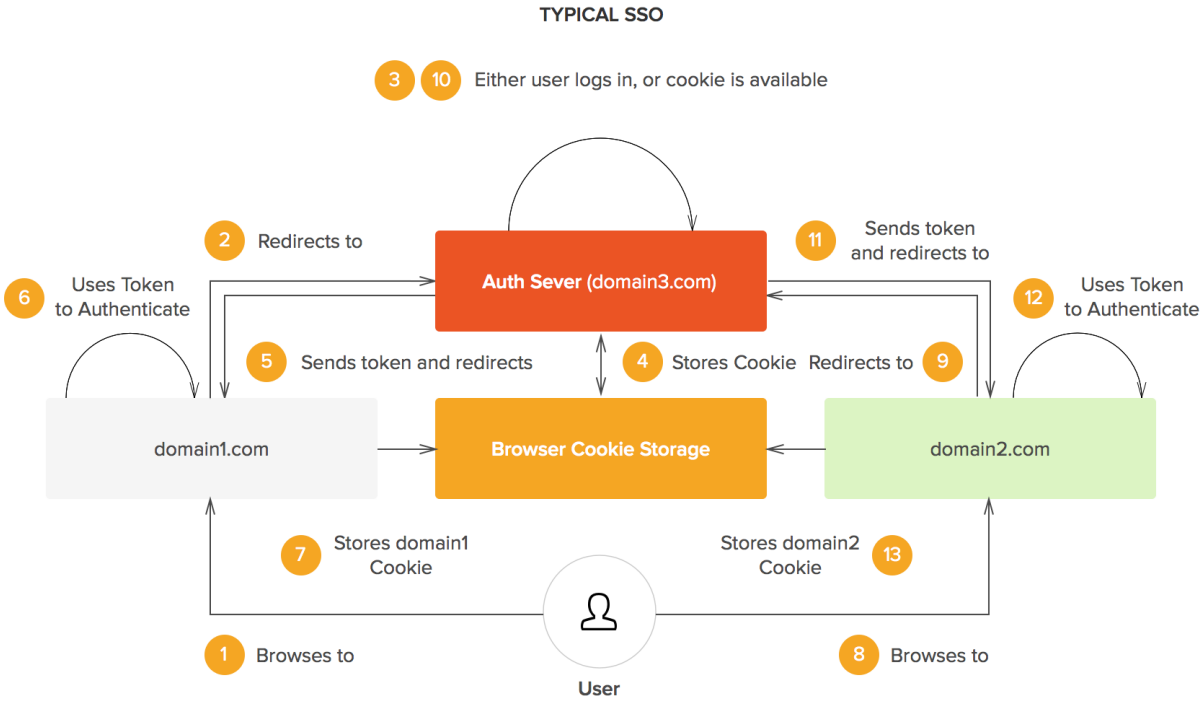
La solución obvia es compartir información de sesion entre los diferentes dominios. Sin embargo, por razones de seguridad, los navegadores adoptan una política conocida como “política de mismo origen”. Esta política dicta que las cookies (y otros datos guardados localmente) solo pueden ser accedidos por su creador (es decir el dominio que pidió que se guardara la información en primer lugar). En otras palabras, dominio X no puede acceder a las cookies del dominio Y o viceversa. Esto es lo que las soluciones SSO intentan resolver de una manera u otra: compartir información de sesion entre diferentes dominios.



Diferentes protocolos SSO comparten informacion de seccion de diferentes maneras, pero el concepto esencial es el mismo: hay un dominio centran mediante el cual se realiza la autentificacion, y luego la sesion es compartida por los demas dominios de alguna manera.



Siempre que el usuario va a un dominio que requiere autentificación es redireccionado al dominio de autentificación. Luego cuando el usuario haya iniciado sesion en este dominio podrá ser inmediatamente redireccionado al dominio original con el token necesario de autentificación.



Tipos

Hay cinco tipos principales de SSO, también se les llama reduced sign on systems (en inglés, sistemas de autenticación reducida).

- Enterprise single sign-on (E-SSO), también llamado legacy single sign-on, funciona para una autenticación primaria, interceptando los requisitos de login presentados por las aplicaciones secundarias para completar los mismos con el usuario y contraseña. Los sistemas E-SSO permiten interactuar con sistemas que pueden deshabilitar la presentación de la pantalla de login.
- **Web single sign-on (Web-SSO)**, también llamado Web access management (Web-AM) trabaja sólo con aplicaciones y recursos accedidos vía web. El objetivo es permitir autenticar a los usuarios en diversas aplicaciones, sin necesidad de volver a autenticar. Los accesos son interceptados con la ayuda de un servidor proxy o de un componente instalado en el servidor web o en la aplicación web destino. Los usuarios no autenticados que tratan de acceder son redirigidos a un servidor o servicio web de autenticación y regresan solo después de haber logrado un acceso exitoso o con un TOKEN de autenticación para la aplicación destino. Se utilizan cookies, parámetros por GET (más inseguro) o POST para reconocer aquellos usuarios que acceden y su estado de autenticación.
- Kerberos es un método popular de externalizar la autenticación de los usuarios.

Los usuarios se registran en el servidor Kerberos y reciben un "ticket", luego las aplicaciones-cliente lo presentan para obtener acceso.

- Identidad federada es una nueva manera de concebir este tema, también para aplicaciones Web. Utiliza protocolos basados en estándares para habilitar que las aplicaciones puedan identificar los clientes sin necesidad de autenticación redundante.
- OpenID es un proceso de SSO distribuido y descentralizado donde la identidad se compila en una url que cualquier aplicación o servidor puede verificar.

¿Cómo implementarlo?

Hay diferentes aproximaciones para implementar un SSO, dependiendo del ambiente en el que se requiera. Es diferente hacer un SSO para dos sitios que están en el mismo servidor que para sitios que estén en distintos servidores o que tengan distintos dominios.

SSO en el mismo servidor

La base del SSO es lograr compartir la información que identifica a cada usuario en la sesión. Si los sitios están en el mismo servidor y comparten el mismo dominio (es decir, existe un dominio principal abc.com y varios subdomios xyz.abc.com o def.abc.com) lo que debe hacerse es configurar las siguientes directivas:

Debe modificarse el dominio de las cookies de modo que cada cookie sea creado con el dominio.*abc.com*.
Debe asegurarse que todas las cookies se almacenen en el mismo lugar del servidor.
El nombre de la sesión debe ser el mismo en todos los sitios.
Es posible que se tengan que desactivar algunas directivas de seguridad como el session referer check, que verifica que los cookies hayan sido creados en el mismo sitio. Por ello, es importante que el sitio tome en cuenta otras validaciones de seguridad

SSO entre distintos servidores

El problema al intentar establecer una arquitectura SSO en servidores distintos es, por supuesto, que las Cookies no pueden almacenarse en la misma ubicación y por lo tanto, no pueden ser leídas por los sitios. Lo que necesitamos, entonces, es crear un espacio compartido en donde puedan alamcenarse estas Cookies. Sólo uno de los servidores proveerá el servicio de almacenaje de las cookies de la sesión, los otros servidores se comunicarán con este para alamcenar sus sesiones.

SSO entre distintos dominios

Si los sitios tienen distintos dominios, lo mejor es guardar las sesiones en bases de datos, de modo que cada sitio tome la información de los usuarios registrados desde allí. Claro que hay que tomar en cuenta que el costo de traer información desde una base de datos es mayor que el de obtenerla desde la memoria o el disco, como en el caso de las cookies. Hay que analizar el impacto que tendrá en el rendimiento del sitio y buscar métodos de caché de sesiones en caso de optar por el uso de bases de datos. Tanto la configuración de cookies como guardar las sesiones en bases de datos permiten no solo guardar la información de los usuarios registrados, si no cualquier otra información que se almacene en la sesión.