24/09/11 - Migració de les aplicacions de FB a OAuth 2.0 l'1 d'Octubre

El proper 1 d'Octubre Facebook realitzarà uns canvis dràstics en la seva política d'aplicacions.

A partir que es va descobrir un problema de seguretat, Facebook va anunciar que caldria implementar un nou sistema més segur per a les aplicacions.

Al seu bloc per a desenvolupadors, anuncien com a partir d'aquest primer d'Octubre deixaran de funcionar les aplicacions que no utilitzin oAuth 2.0, el que entre d'altres implica:

? Actualitzar codi si utilitzes versions anteriors

? Comprar i implantar un certificat SSL per als servidors Web o els Balanjedors de càrrega (load balancers)

? Reescriure el codi que correspongui per a que es comuniqui amb FB emprant SSL

? Implementar sessions de PHP (si la teva aplicació és en PHP). El que té més complexitat del que sembla quan treballem en un entorn webfarm (granja de servidors)

Cito de la seva web:

Reminder: Breaking Changes coming on Oct 1st

The following breaking changes are slated to go into effect on the 1st of October:

1. **OAuth 2.0 Migration**All apps must migrate to OAuth 2.0 for authentication. The old SDKs, including the old JavaScript SDK (FeatureLoader.js) and old iOS SDK (facebook-iphone-sdk) will no longer work.
2. **Apps on Facebook authentication and security migration**All Canvas and Page tab apps must convert to process signed_request (fb_sig will be removed) and obtain an SSL certificate for use in `Secur`

	e Canvas URL
and	Secure Page Tab URL

(unless you are in Sandbox mode).

3. **Auth 1.0 deprecation**Auth.promotesession, auth.createtoken, auth.expiresession, auth.getsession will be removed on Oct 1st. Details on support for OAuth 2.0.

4. **manage_pages permission required to access user accounts (/me/accounts)**We are modifying access to the FQL page_admin table and the graph.facebook.com/me/accounts endpoint. Previously, with basic permissions granted, an app could go to this endpoint or the FQL table to access the list of a users' apps and Pages. We are going to require that apps have the manage_pages permission in order to obtain access to this information.

Jo m'he encarregat d'assegurar-me que la migració de les aplicacions de l'empresa on treballo fos un èxit.

Aquestes són les dificultats que m'he trobar:

Certificats SSL:

A l'empresa volien contractar un certificat del tipus wildcard multi-domain.

Aquests certificats no existeixen, si compres un certificat SSL senzill et permet protegir un sol nom de domini, per exemple www.codic.cat.

Si compres un certificat SSL del tipus wildcard et permet protegir el teu domini:

Un wildcard per a codic.cat et permet protegir tots els subdominis de primer nivell per a codic.cat.

Per exemple: dns.codic.cat o www.codic.cat

Però és important saber que només per al primer nivell.

No pots protegir www1.servidors.codic.cat.

Aquests dominis addicionals els pots protegir mitjançant d'adició de SANs ? Secure Alternative Names al certificat. Això s'ha de fer al moment d'encarregar-lo. Es pot fer després mitjançant la creació de duplicats, però no us ho recomano i us pot donar problemes si feu servir CDN (Content Delivery Network).

Els SAN també són importants perquè alguns dispositius mòbils no suporten els certificats wildcard (per exemple l'infame windows mobile 5) i haureu de crear entrades SAN fins i tot per als dominis de primer nivell si voleu que funcioni en aquests dispositius.

Arribats a aquest punt us explico que els wildcard multidomini no existeien, per tant si teniu dos dominis per als que voleu wildcard, haureu de comprar dos certificats diferents.

A més del certificat wildcard, heu de demanar que estigui llicenciat per a usar-lo en múltiples servidors si empreu un CDN.

Hi ha diversos CDN d'abast mundial como akamai, el més conegut i probablement el més car, amazon, o més modestos i econòmics com cotendo.

Després instal·leu el certificat als servidors web o als balancejadors de càrrega i al CDN, segons les vostres configuracions i a funcionar.

Per a triar certificat vaig contactar amb diverses entitats certificadores.

Verisign ? Reconeguda mundialment com la número 1, va ser de les pioneres. Però són poc flexibles i cars. Els vaig contactar per email en anglès i em va trucar una comercial que parlava castellà. Se li escapaven els detalls tècnics i em va remetre a suport tècnic, també en castellà. Conclusió: no emeten certificats wildcard per a usar en múltiples servidors (CDN), i el preu que em feien per a tenir unes 25 SAN era de vora els $6,000.00 sis mil dòlars americans. Tenen fama de trigar fins a dues setmanes a enviar el certificat. Una utilitat interessant és que et permeten generar un certificat de proves auto-signat gratuïtament des de la seva web però el cap de sistemes no va aconseguir fer-lo funcionar en un lamp de proves per a les provatures prèvies a la implantació.

Digicert ? El que utilitza Facebook a part d'akamai i el que vaig comprar. Vaig poder plantejar tots els dubtes a través d'un xat web disponible a la seva plana. El certificat wildcard amb 10 SANs màxim va costar $475 quatre cents setanta cinc dòlars americans. En una hora teníem el certificat i l'instal·làrem als balancejadors de càrrega.Thawte ? Els vaig contactar a través d'un formulari web i vaig rebre un mail tipus al cap d'unes hores, i un altre al dia següent.

godaddy ? Els més barats, generosos i flexibles. Per $219 teníem un wildcard al que podíem afegir 100 SANs. Malauradament internet explorer 9 no el llistava a la llista d'entitats certificadores que reconeixia. Això és important perquè si no li apareixen als visitants missatges de que aquell certificat no pot ser validat i molts es fan enrera, o els crea molèsties en navegar. Molts usuaris utilitzen internet explorer de microsoft així que descartat.

No vaig poder aclarir, cap persona de suport m'ho va poder contestar, si el fet d'afegir moltes adreces SAN (per tant generant un arxiu de ertificat més gran) pot fer que les comunicacions amb els visitants siguin més lentes.

Cal considerar que les comunicacions SSL sempre són més lentes i tenen un cert impacte en consum de CPU dels servidor web o balancejadors, pel que els proveïdors ens cobraran més per usar SSL.

Calculo que el 90% de les aplicacions l'1 d'Octubre quedaran desactivades, si més no parcialment per als usuaris de FB que usen SSL.

Adreça curta per a Twitter d'aquest article: http://wp.me/pzeab-1Sq

Traduir a l'Anglès. Translate to English	Compartir: ||