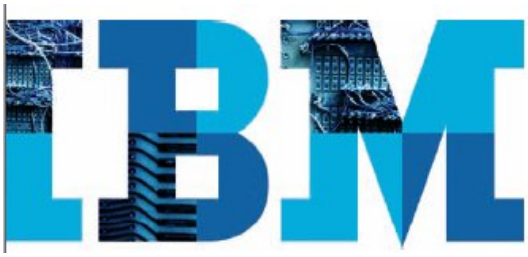
WebSphere DataPower SOA Appliances in Mobile Environments

Contents

Executive Summary
There is a lot of attention being paid to mobile applications and how businesses can use the mobility of its employees and its customers to be more successful. Like any new technology trends there are some new things to think about but also there is much that will need to work with your existing business investments.

This white paper will provide some considerations to think about either before or soon after you have your first mobile app is development.



Introduction

Everyone is talking about mobile applications, but what exactly is a mobile app? And how does is relate to my current application development process? Mobile apps generally fall into one of 3 types:

- native applications
  - is built using a device specific SDK (i.e Apple's iPhone/tablet, Google's android platform
  - is built to run on a specific platform operating system using the capabilities of the device
- an HTML5 web app
  - has provided some enhancements for web applications that are of particular use to developers of mobile applications because they optimize the exchange of information via the browser (webkit) capabilities found on all mobile devices
- a hybrid app
  - has emerged to work around limitations of the other two
    - native apps, if changed need to be versioned, redistributed and might require supporting multiple versions
    - browser apps, may not take advantage of all the features of the platform.
  - provides a library that allows coding for a "generic" mobile function without having to build different applications for each platform—a javascript library generally provides the mapping between the specific platform and the "abstracted" function.

What does that mean to a business owner/influencer of application content? If you already have web application development in your business, you may already be writing apps that can be accessed by a mobile browser. This was the first wave of the mobile application development and it continues to evolve with the new HTML, JSON and REST trends. For many of these browser apps (HTTP/JSON/REST), WebSphere DataPower can and is being used to optimize and secure access to backend services.

1. Success. Build for it. Prepare for it.

We are all tuned to be prepared for threats these days, and we have backups and disaster plans…… but what about the "threat" of success? One of the most important things to consider with mobile apps is that they may go "viral" and this can be a really good thing ……if you have prepared for success. This means when the entry-point hosting the server side of the app hits its simultaneous 1 millionth user, what will happen to your site?

An appliance like DataPower can load balance your incoming traffic. You can set limits on the number of requests and gracefully handle the surges. Coupled with IBM's technology like Cloud, you can build a plan for failover or fail-up. And as you increase the number of DataPower appliances, multi-box management can let you respond and rebalance the traffic.

2. Bring Your Own Device (BYOD)

In tight economic times the idea of giving employees a stripend and letting them manage the device offers some cost savings numbers that are hard to resist. Many already do this with their phones so they can take conference calls at night or while travelling, so why not extend this to applications and data?

One difference between terminating a phone and terminating access to a web application is what happens when that person leaves? Either voluntarily or by your choice…..how do you "stop" access from continuing? With a phone plan, you can stop paying, have the phone shut off. But, if you don't "own" the device, you may not be able to stop an application request from being generated and hitting your service, at least initially. The challenge may be you CAN stop it from being responded to? If you can identify and correlate the incoming request with a particular person and device and application you can have your perimeter respond and not have to overload your backend. After all a former employee may still need to get to heath care providers or other HR functions in the interim, so you may find you need a better level of granularity over the access you need to provide at the edge of your enterprise.

3. Good users & bad users

Continuing on the BYOD topic, are you prepared to filter requests at the edge? This awareness of gating traffic at the edge may become more visible to your end users, and mobile users are very aware of response time. So how do you let the "good users" have easy access and stop the "bad users" as early as you can (so that you minimize the "bad load" on your application infrastructure)? More traffic from mobile devices will drive more requests and if you cannot vett them at the edge the load will go to your backends to deny and this may not provide the efficiencies you need.

4. MILLIONS of devices, with many apps per device.

Many of the new applications for mobile devices bring interesting challenges. So, while your new mobile applications will help you penetrate new markets and get new users, this means you will need to be able to scale to handle.

5. Will you support the app yourself? Or outsource its development or hosting?

Another decision access for mobile applications is whether or not the business determines that a mobile application is something "core" to the business or something that can be hosted externally or perhaps even supported as a service that business partners might use to build out a new supply chain ecosystem. Creativity is central to the design of mobile applications and many find that creating applications for the various application platforms require a specific skill set (graphic designers, UI experts) that they may not want to invest in. However, the UI may need to call a service layer that IS critical to your business.

6. Do you have well defined tiers?

MVC is a well known paradigm for the "old style" of application development, but it was rooted in the recognition that there were application tiers needed, each with its own functions that could be optimized.

The new HTML5/CSS/JS/JSON/REST pattern also benefits from the definition of a set of tiers. When you have static content to render, it makes sense to optimized or "cache" this information. When you need to dynamically generate content you often don't do that in your "DMZ" but put this function inside your application infrastructure, but perhaps on a dedicated set of resources. Either way it may be a good idea to "cache" this content so that repeated requests are processed as "static" requests (because you hit the cache without having to go to the next tier).

7. How flexible are your policies for edge enforcement?

The one thing that all mobile apps share is the demand of the end user for response time. The mobile user is demanding user expecting an almost immediate response. And if they don't get it, they go on to the next app (unless the request is compelling). For businesses that want to control the rate and pace of the information flowing from their enterprise to a mobile audience, it may be time to look at policy management and start planning for the ability to "adjust" operational parameters in a more dynamic and flexible way. Policy enforcement at the edge can provide things like "step up" authentication if there is reason to suspect a threat to your business service, or it can provide "rate limits" with options to slow or fail requests that go beyond a mobile users' quota.

8. Do you know what OAUTH is?

Ok here's the dirty little secret. We all share passwords. We all know that sharing passwords is bad, but considering the alternatives, we do it anyway. So what if there was an option for you to direct that the local print kiosk can print your latest travel photo's BUT ONLY the travel photos on your phone? Would you use it? This type of exchange is what OAUTH provides. It allows the resource owner (that's you) to offer a service (GET photo) so that the local kiosk (the requestor of the travel photo's) can be authenticated (your service need to have someone like you register that kiosk XYZ is ok) and authorized (you say which photo's the kiosk can access) to print pictures.

9. Do you trust third parties (i.e. Google and Apple) to do the right thing with your data?

Ok another dirty little secret, privacy is dead, right? Some believe this to be true, some still try to protect information (you CAN set privacy settings on Face book, whether or not you do so is up to you). As we move to this new public world of personal information disclosure there are still needs to provide alternative channels of delivery for information for which protection is mandated (i.e financial, health).

Mobile devices are great for providing information on the go, but they still are

somewhat limited (by virtue of visual real estate as well as capacity) in their ability to multi-task. What this drives then is the need for “notifications” which is a new use of an old technology --- async messaging. Applications can be designed to recognize a “shoulder tap” or a “ping” --- message incoming, application update available. Currently this information as well as the approval/check of the application itself when offered through a public app store is controlled by the major mobile application providers (Apple, Google) and for many this is just fine. There are also emerging “enterprise” offerings in which companies can control this information including IBM Worklight which provides a framework for Universal Notification.

10. How will you know if your app (or app user) goes rogue?

The reality of life on the internet is that bad things happen. There are just too many moving parts—mobile devices that are stolen, mobile devices that are “rooted”, mobile users that have their access information compromised, applications with “gaps” in their security models that are exploited, internet protocols with “gaps” in their security models that are exploited, new hackers, new threats today—many of these that we couldn’t have coded for yesterday because we didn’t know they existed.

The only thing anyone can do is be aware of the risks and to protect yourself with tools and information that can help you stop a “little” bad thing from becoming a “big” bad thing. DataPower’s flexible policy enforcement and XML threat protection can be a tool that helps you respond. It can help you set policies and notify the right people if an application starts to act outside its profile. It can allow your operations to shut down or rate limit access to a service by a device or a set of devices.

For more information
To learn more about the IBM WebSphere DataPower SOA Appliances, please contact your sales representative or visit the following website: http://www-01.ibm.com/software/integration/datapower/

For IBM Worklight, visit the following website: http://www-01.ibm.com/software/mobile-solutions/worklight

About the author
Maryann Hondo
Senior Technical Staff Member, IBM Software Group

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
May 2012