Governance in the Cloud

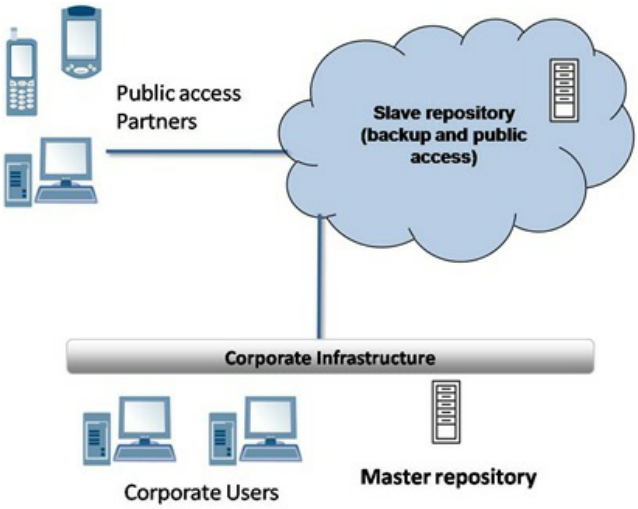
Lori MacVittie, 2008-09-09

David Linthicum of Real World SOA asks whether SOA governance should be delivered as a service, from the cloud.

Core to this proposition is the use of a registry/repository in the cloud:

> This repository would provide more than just WSDL, but a complete design time and runtime SOA governance system delivered out of the cloud, perhaps linked with a local slave repository within your firewall.

One of the problems with this, I see, is that in a SOA where governance is actively used and policies enforced, governance becomes crucial to not only the day-to-day development efforts but also to run-time execution. I like David's suggestion of a master-slave relationship, but I think it ought to be reversed. The local repository ought to be your master with the slave repository - and public access - in the cloud.



This has the effect of providing a backup repository for corporate use, supporting business continuity and disaster recovery plans, but also allows services to be shared with partners and the public, if desired, without requiring access to corporate infrastructure. Keeping the master repository inside the corporate infrastructure further reduces the potential impact of latency and service interruptions on the business. A local repository mitigates only the impact of a service interruption, it can't address the potential degradation of performance imposed by integrating policies stored remotely.

There are also security concerns that must be considered, and primary amongst them is the question of whether it is wise to store security policies in a potentially publicly accessible repository, as security policies are necessarily a part of SOA governance, especially for run-time governance.

There are certainly some intriguing possibilities here, and David is right to ask whether the cloud can be leveraged for SOA governance functionality. Given that SOA governance is a service regardless where it is deployed, it would make sense to use the cloud to deliver that service in some circumstances. When services will be shared with the public or partners, it makes a great deal of sense to make use of the cloud to govern and deliver those services. But when they are internal only or highly sensitive, it seems that pushing them out to the cloud would be increasing risk rather than mitigating it.

The hybrid model introduced with Cloud Bursting seems to be a very good fit for SOA governance. While SOA governance would not be using cloud bursting in the same way many web applications would - that is, for additional compute resources on-demand - the core concept of using both corporate and cloud computing resources to architect a more flexible, scalable solution seems highly applicable. If services might be heavily used by partners and/or the public, then taking advantage of the cloud to govern those services would alleviate the need to scale up the corporate infrastructure to support it, essentially offloading the cost of management and maintenance of the required additional hardware and software to the cloud provider.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113