



(Graphic source: [Wikipedia](#))

Title: Understanding Azure Subscription.

Notes from the field.

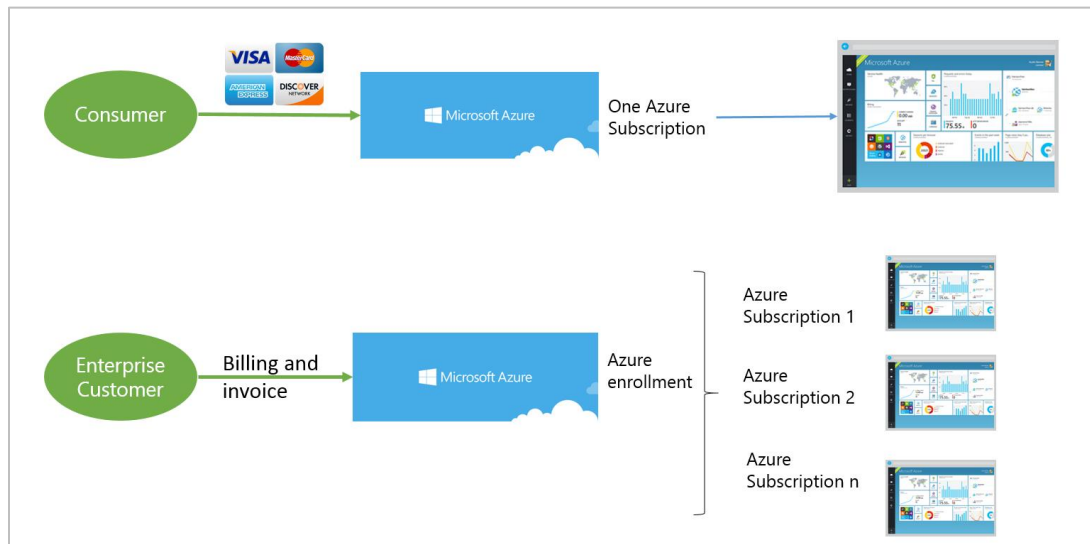
Author: Phani Tipparaju
Cloud Architect, Greater New York region.

Phani Founder and Chief Architect of BrainScale, a cloud services company. He has around 16 years of experience. His current role involves helping customers succeed and optimize in the cloud. He has delivered many Azure boot camps, has done many evangelism sessions on various topics across Azure for many customers across North East US. He can be reached at phani@brainscale.com. He is also an author with Pluralsight. He blogs at <http://allthingsazure.com>.



Chapter 1: Understanding Azure Subscription Layout

One of the first questions that I get from customers who are serious about Azure or Cloud in general is "Where do I start?", Microsoft Azure is sold in two different forms- one for consumers, who would just like to go to <http://azure.microsoft.com/en-us/pricing/free-trial/> and swipe their credit card and get started. The other way is to buy Azure as an Enterprise Agreement. No points for guessing this, enterprise agreements are for enterprise customers and of course you commit to a certain amount and based on the commitment, you get discounts. For consumers who buy it as a single subscription based off of their credit card, all you get is a single subscription. You cannot spawn off multiple subscriptions off of that one subscription, but of course you can leverage all the features of Azure like IaaS, PaaS, SaaS alike. However, for enterprise customers you get to deal with two portals and not one. The first portal you will start dealing with is the ea.windowsazure.com. It is also called as enterprise portal [EP]. EP is the place where you can create departments, assign owners to these departments and under each department you can have one or more subscriptions.



So, if you are an individual user typically you would buy azure here (<http://azure.microsoft.com/en-us/pricing/purchase-options/> PAY AS YOU GO). And go to this portal here (manage.windowsazure.com) to build your project(s) - VMs, Network, PaaS services etc.

If you are an enterprise customer, a super admin(s) would manage enrollments here (ea.windowsazure.com) and individual project users shall go to portal here (manage.windowsazure.com) to build your project(s) – VMs, network, PaaS services etc.

Chapter 2: Inside a subscription

So far so good, but real questions now specially for enterprise users are-

Q1. How many subscriptions can I create?

Q2. How many subscriptions should I create?

The answer to question 1 is you can technically create as many subscriptions that you want in the EP.

The answer to question 2 is 'depends'. So let's explore the 'depends'.

A subscription is like an account or a container with following properties-

1. One service administrator
2. One or more co-administrators.
3. Now you also have subscription 'owner', 'contributor', 'reader' and roughly seventeen other roles as part of the Azure RBAC release.
4. It provides an isolation boundary for IaaS assets like network/subnets. Virtual machines in a subscription when they are created can readily choose the network/subnet.
5. By virtue of point 4, other assets like databases (IaaS VM), Windows Server based Active Directories can be readily shared by VMs in that subscription unless you configure explicit NSG rules to avoid that.
6. Subscription also is a rolled up unit of billing. As of this writing (03/27/2015) the concept of 'Tagging' is introduced in Azure, but not all PaaS services have enabled it yet. So you still cannot get billing information based on lower elements like- how much do bunch of these VMs cost unless you do the excel math. I hear this is a roadmap feature and should be coming soon- you should soon be able to get usage and pricing and calculate the billing based on those two data points and group it by tags.

So, today the answer to how many subscriptions should you create would depend on billing requirements like chargeback that you are looking for and the network assets that you need to readily share. Please note that you can of course have multiple VPN connections between two networks belonging to two different subscriptions. That way you can mitigate the network sharing problems as long as VPN speeds can meet your requirements.

Chapter 3: Resource groups to the rescue

At this point I want to introduce the graphic on the cover page called **Matryoshka doll**, also known as **Russian nesting doll** or **Russian doll**, refers to a set of wooden dolls of decreasing size placed one inside the other. (From Wikipedia).



For an enterprise customer with Azure EA, the model is pretty much like 'Matryoshka' doll wherein at the top most level you have 'Azure Enrollment' which can have one or more 'Accounts', each account can have one or more 'subscriptions' and each subscription can have one or 'resource groups'. There is a difference though, a 'Matryoshka' doll signifies one of each kind, and nonetheless I wanted to signify the nesting concept.

A resource group becomes an interesting isolation layer considering RBAC. RBAC is '**R**ole **B**ased **A**ccess **C**ontrol'. When you apply RBAC at resource group level, you are essentially saying that there can be an owner, reader, network contributor- only people in this role can perform network level activities, VM contributor- only people in this role can deal with VMs and so on. There are around 20 roles for various components of Azure like storage, Azure SQL DB etc. For more details about RBAC check my blog posts on RBAC- [Part 1](#) and [Part 2](#).

So, the question that arises now is in which case I should use multiple subscriptions and in which case should I just have one subscription and have 1-n resource groups (top limit for number of resource groups in a subscription is 1000). What really is the guidance? The answer to this question is this- If network or other shared services like 'Active Directory' or DNS are not applicable then you can have as many subscriptions and work off of that. If sharing those services across projects is an important

consideration then it's best to have one subscription and on relatively bigger network address space and carve out subnets for various projects based on that and have relevant 'network security groups' (NSGs). You can share the network, AD, DNS, Databases across all the projects by configuring relevant NSG rules. In this case you still can achieve isolation for various projects within a subscription by using 'resource groups' and still share common shared services, which could be in a dedicated subnet and resource group of its own. If you really require chargeback model for customers, and you use PaaS services like HDInsight, Azure Machine Learning or any of the other PaaS services where tagging or 'resource group' feature is not yet available, you will still have to use multiple subscriptions, at least for now till tagging is enabled for those PaaS services.

Summary

If the scope of your project is IaaS (network and VMs), then planning one subscription and multiple resource groups should be easiest way to achieve isolation and chargeback. With RBAC roles you get excellent mechanism to control fine grained access within a project (project mapped to resource group) to multiple actors. It's important to understand these aspects before taking the plunge to randomly just create multiple subscriptions or having everything in one subscription.