Nicole Welch

cloud first

May 14, 2019

Azure Design Considerations–Enrollments, Subscriptions, and Resource Groups

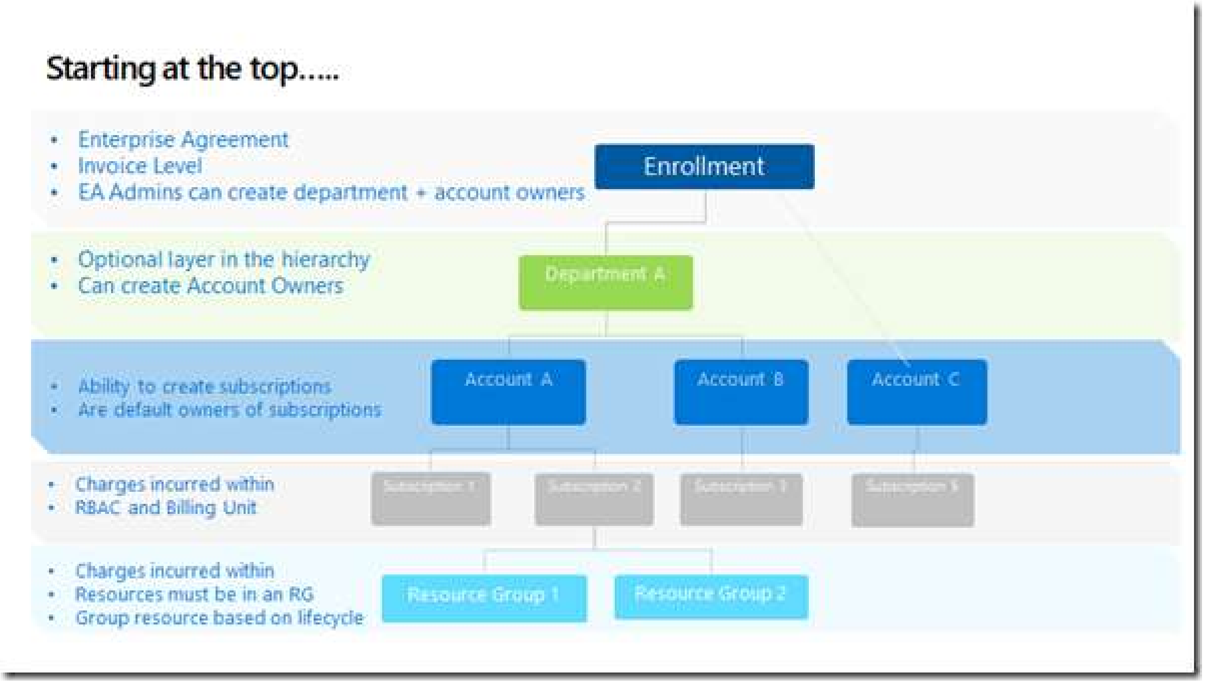
Leave a comment

When I first meet with new Azure EA customers, one of their first topics is "how do I set this up?" Azure is very flexible, but this means you have design decisions to make:

- how many enrollments do I need?
- should I use departments?
- should I separate teams using subscriptions or resource groups?
- where do I apply RBAC (define access)?

While there are wrong answers, there is no one right answer. Each organization will need to evaluate their needs, organizational structure, and use case(s) to see what works best for them now. And if things change in the future, this design should change too.

Let's break down the different control points.



Starting at the top…..

- Enterprise Agreement
- Invoice Level
- EA Admins can create department + account owners

- Optional layer in the hierarchy
- Can create Account Owners

- Ability to create subscriptions
- Are default owners of subscriptions

- Charges incurred within
- RBAC and Billing Unit

- Charges incurred within
- Resources must be in an RG
- Group resource based on lifecycle

(https://nicolewelchblog.files.wordpress.com/2019/05/image.png)

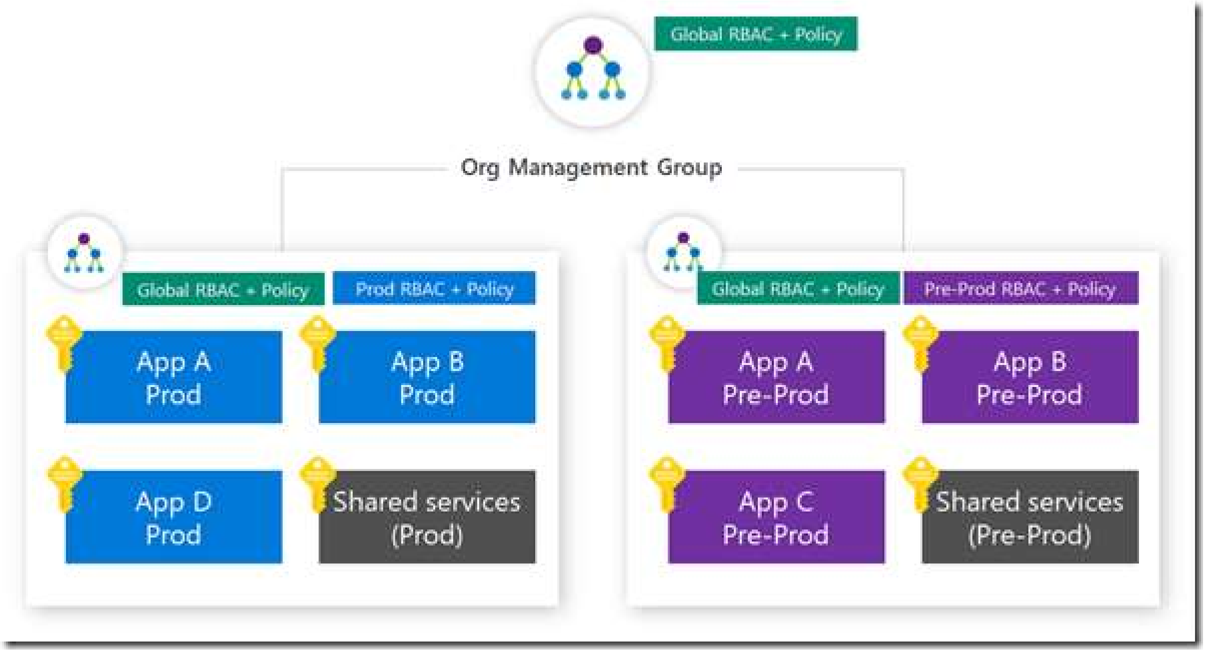
First off, consider if multiple enrollments are needed or if multiple subscriptions within a single enrollment will suffice.

	Subscriptions	**Enrollments**
Separate Invoice		X
Able to view charges at this level	X	X
Can use unique AAD Tenant	X	X
Can view charges in EA Portal	X	X
Can share an ExpressRoute	X	X
Simple to Administer	X	

Then consider how to further separate resources leveraging subscriptions and resource groups:

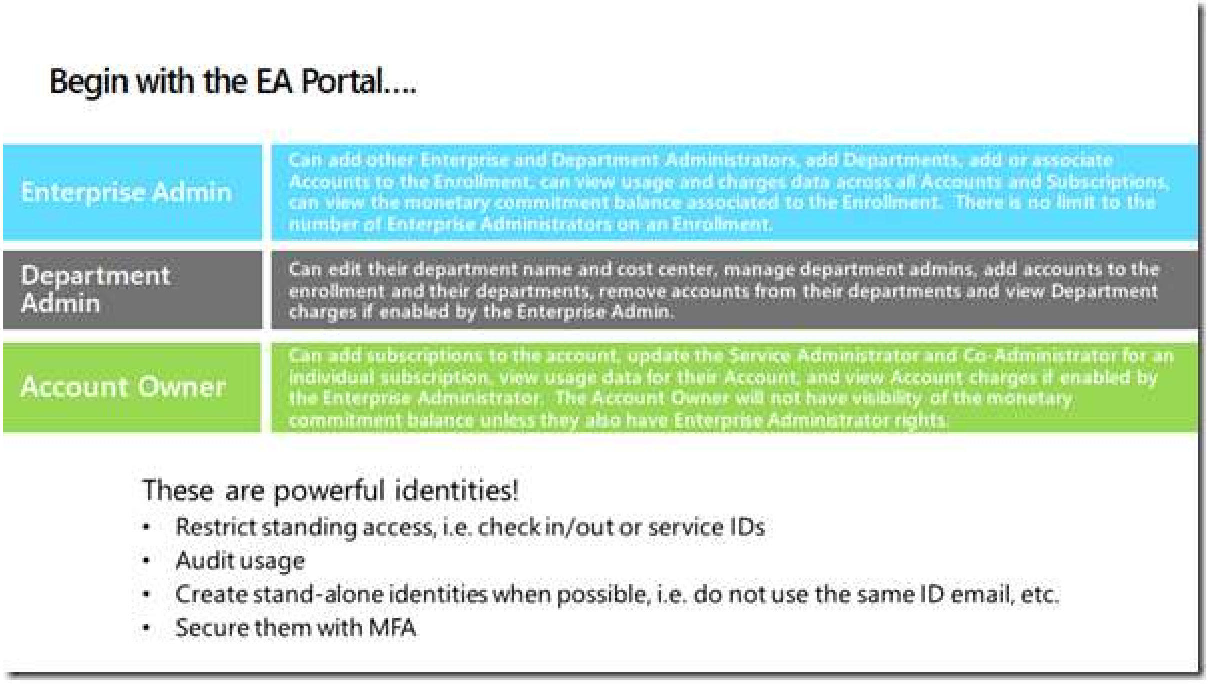
	Resource Groups	**Subscriptions**
RBAC supported	X	X
Easy to view Billing	X (in Azure portal only)	X (in EA and Azure portal)
Resource can be shared across	X (natively)	Requires additional configuration and only some resources are supported
Azure Policy supported	X	X
Best for Sandbox		X
Best for restricting access in a common environment (i.e. PROD)	X	
Simpler to Administer	X	Multiple subscriptions create administrative overhead
Can share a single ExpressRoute	X	X

Keep in mind subscriptions can be grouped and administered in a hierarchy using Azure Management Groups (https://docs.microsoft.com/en-us/azure/governance/management-groups/ (https://docs.microsoft.com/en-us/azure/governance/management-groups/)). Management groups allow you to set Azure Policy and RBAC centrally for governance with low overhead support.



(https://nicolewelchblog.files.wordpress.com/2019/05/image-1.png)

Finally, in the EA portal itself make sure you are thoughtful in how roles are assigned and controlled.:



Begin with the EA Portal....

Enterprise Admin	Can add other Enterprise and Department Administrators, add Departments, add or associate Accounts to the Enrollment, can view usage and charges data across all Accounts and Subscriptions, can view the monetary commitment balance associated to the Enrollment. There is no limit to the number of Enterprise Administrators on an Enrollment.
Department Admin	Can edit their department name and cost center, manage department admins, add accounts to the enrollment and their departments, remove accounts from their departments and view Department charges if enabled by the Enterprise Admin.
Account Owner	Can add subscriptions to the account, update the Service Administrator and Co-Administrator for an individual subscription, view usage data for their Account, and view Account charges if enabled by the Enterprise Administrator. The Account Owner will not have visibility of the monetary commitment balance unless they also have Enterprise Administrator rights.

These are powerful identities!

- Restrict standing access, i.e. check in/out or service IDs
- Audit usage
- Create stand-alone identities when possible, i.e. do not use the same ID email, etc.
- Secure them with MFA

(https://nicolewelchblog.files.wordpress.com/2019/05/image-2.png)

That’s my two cents on how to get started, but keep in mind this is a journey. I recommend lots of whiteboard sessions to play with the different options and then test them out again real-world use cases. The best designs appropriately limit access but are easy to implement and maintain.

Posted by Nicole Welch in Azure
Tagged: Azure, design, ea, enrollment, subscription