

VBL Engineering Compliance Checklist

Last updated by | Paul Kelleher | 17 Jun 2020 at 07:38 GMT

Business Policy/Rules

Guidelines to ensure that resources, costs and process are either adhered to by Deny rules if non compliant, Automated Actions applied unless excluded

Item Name	Type	Notes	Estimation	Value Area	A	B
Resource Group Templates	Automation	Create RG with agreed networking NSGs Logging Worspace Alert Groups Tags etc				
Resourice Group RBAC	Process	RBAC Per RG 2 fixed Owners + DIET RO Pim to Cont RE default				
Resource Group Creation	Policy	Restrict RG Creation to PIM Contributor or above				
RG Required Tagging	Policy	Enforce RG compliance (whole subscription not enforced)				
RG Tag Propagation	Automation	if not exist copy RG level tags to child resource				
RG Tag Compliance	Policy	ensure values are within acceptable array values				
Storahe Accounts	Policy	Best Practice Storage Account config				
Location Selection	Policy					
PublicIP Banned	Policy	Block all public IP creation unless the RG has tag "publicip-approved:sarf/vsts reference"				
Secure KeyVault	Policy	Use a KeyVault that is restricted to known networks				
Validate Networking	Polcy	Validate that the correct routes via FW are used				

Capacity & Size

Processes to check resources are active,correctly sized and using the best mix of resource size

Item Name	Type	Notes	Estimation	Value Area	A	B
Azure VM Sizes	Policy	Restrict VM Sizes to in-built list or additonal sizes in AllowedInstanceSKUs Tag				
Azure VM OS	Audit	Development (&other?) Linux should be Centos Image Based				
Azure Avail/Scale Sets	Audit	For 24x7 Services have Autoscale and Low-CPU discount instance size switching been looked at?				
Azure Disks	Automation	Check Last Access times and if >1week tag/flag for investigation				
Azure Disks	Automation	Check Capacity Used Space [rule set depending on environment and % of disk use change per week				
Storage Account	Automation	Check Last Access times and if >1month tag/flag for archive				
Storage Account	Automation	Check USed/Provisioned Space [<10	>60%]			
Storage Account	Automation	Limit Storage Accounts dev:2 uat:2 systest:unlimited production:unlimited				

Non-Production

Development instances should be treated as lower cost, frequently removed, rappidly changing, so ensuring minimal sizes are used in the first case, then scaled up and put into HA configurations for testing and production. THe number of resources that can be multi-purpose should be leveraged

Item Name	Type	Notes	Estimation	Value Area	A	B
Check AutoShutdown	Automation	Check tags for instances for AutoShutdown tag unset for reporting				
AutoShutdown Controller	Automation	run every 30mins try to shutdown tagged and send error if still on at 19:00				
AutoStart Controller	Automation	run as scheduled				
Storage Accounts	Policy	enforce re-use of single logging/system RG storage and single storage account for the contained apps				

DevOps Tooling

Item Name	Type	Notes	Estimation	Value Area	A	B
Environment Sizing	Policy	dev:devtestlabs uat:laaS systest:laaS/HA production:laaS/HA/Alerting				
root@ns3046440:/home/dev/pknw1/azcli-scripting#						