AZ 203 Azure Developer - Part 3

11 March 2020

17:11

Blob Containers

Access Levels

Machine generated alternative text:
Pub•l« O 
private 
Ec«s) 
real 
MC.«.S 

* Containers have flat structure but we can segregate items inside them in virtual folder structure

Machine generated alternative text:
x 
first 
Cherkw 
Contrd (LAM) 
kcess 
Properti« 
C) Delete 
frst 
Search by 
Acquire 
Break Lease 
1/21,m19. s:1309 PM 
Upload blob 
files O 
O.erwrite if files exist 
Advarxed 
Auttv•nticaton tne O 
Blob type O 
Bkx* 
as blobs freeommer&d) 
Block O 
to fad-et 

* For effective management of files ie things like moving files in other folders or other storage accounts etc - tool AzCopy can be used - command line tool. This performs server side copies/operations by default.
  + We can login to azure account first using PST-->use this azcopy exe to copy/move files etc from source to destination path.
  + Source and dest are full file paths or blob item paths
  + Command also need access key OR we can generate SAS token on the source file and use that to perform copy/move etc operation. (URIs/SAS tokens etc are all available under blob properties.
  + If copy is performed across storage accounts then keys will be different else source and destination keys will be same.

Machine generated alternative text:
PS C: a: 
have a for yN to login. For old experience Kith 
have us the to y•aJ have access... 
"id-: "7.d168af-Æ.9-4286-a218-afc724i3e.43% 
"Pay-As-Yw—Go (Azv•e 
"state": "Enabled" 
-scottscwrs@.R1wk cm" 
-user 
PS C: 
'Pattern: /SourceKey: 
ey/eppx72F" 
Finished 1 04 total 1 file(s). 
tae19-ei-2i s..—ry: 
Total files transferred • 1 
transfer successfully : 
Transfer failed : 
Elapsed ti—: 
PS C: 
use 
1%in - 

Acquire and Break Lease -

* On the blob items we can acquire lease and it will lock that resource for all kind of operations like modifying/delete etc till the time lease ir broken

Machine generated alternative text:
Dashi:oatd > Resource groups newstorage > 
az%.dnewstocsge2 • Blobs first 
Delete 
Acquire kase 
Lease status 
Expired lease follcwhg bk*B. tir leze is 
active. tik ID *ith any reqtæst to Mae to 
to Of 
x 
first 
Contrd (LAM) 
kcess 
Properti« 
Search Noes by 
Break lease 
1/21/2019. s:4CS9 PM 
1/21/2019. PM 

Storage Access Tier -

* By default its Hot tier where items are available in real time instantaneously and standard pricing is applied.
* We can go to blob item properties and change its tier if we don’t have regular access requirements like for backups etc. Storage becomes cheaper but access becomes a bit expensive.
* There is additional Archive tier where its item won't be available at all until its hydrated back to hot or cool tiers first.

Machine generated alternative text:
Azure storage offers different storage tiers. which allow you to store Blob object data in the 
most cost-effective manner. The available tiers include: 
• Premium storage (preview) provides high-performance hardware for data that is 
accessed frequently. 
Hot stora is o timized for storin data that is accessed fre uent;• 
• storage is optimized for storing data that is infrequently accessed and stored for at 
least 30 days. 
• Archive storage is optimized for storing data that is rarely accessed and stored for at 
least 180 days with flexible latency requirements (on the order of hours). 

Pricing

For storage archive is 90% cheaper than Hot tier.

Machine generated alternative text:
Data storage prices 
A' ate pet 
First SO (1B) / rnmth 
Next 450 TB Month 
SOO 1B / Mcnth 
soon 
son 
soot92 
S001S2 
SO.01S2 
som2 per G8 
som2 per Ge 
SOD02 per GB 

Machine generated alternative text:
Operations and data transfer prices 
Write Operations• (pet 10.000) 
and Create CmtSr•r (per 
10000) 
Operations" 1000m 
other Operatims 1 ODOOX except 
Delete. 
Data GB) 
Data write 6B) 
soos 
9.10 
SO 05 
soma 
902 

<https://github.com/Azure-Samples/storage-blob-dotnet-getting-started>

Azure AD - Identity checks - identity as a service.

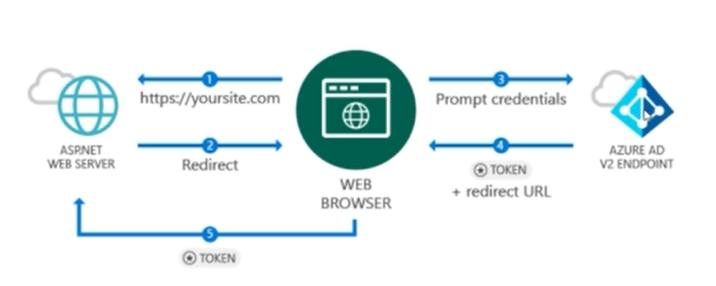
* Azure AD Connect - tool installed on-prem to sync on-prem AD with azure AD.
* App Registrations in Azure AD - once done , it will provide SSO model to login to all registered apps using azure AD.
* We can also use Azure AD without on-prem sync and users/groups etc can be created directly as well.
* Creation - standard way - org Name and unique domain name (initially xxx.nmicrosoft.com and later we can use custom domains)
* To browse to AD we can use switch directories under account login section OR under azure AD options.

\*\*\*Azure Ads may take some time for caching to catch up so we should wait for sometime

* IMP - all resources created in as subscription are actually under a default directory implicitly.

* Code sample of this is present

Machine generated alternative text:
AzureADQuickStarts / AppModelv2-WebApp-OpenlDConnect-DotNet 



Approach using web apps with Azure AD based authentication

1. Create web app and deploy to Azure (web app for testing can be from github account above)
2. Azure AD -- App Registrations -- New App Registration --Provide Application Type and Sign-on URL as base URL and need to be https URL -- we get App ID
3. Update web.config of the downloaded sample with Client ID and Redirect URI settings

Machine generated alternative text:
cappSettings> 
add 
add 
A: add 
€ add 
(add 
< add 
add 
< add 
-webpages:version" value: "3.e.e.e- 
key: 
-webpages :Enab1ed" value; "false" / > 
key. 
idationEnab1ed- value' "true" / > 
key' 
key• -Unobtrusive'avaScriptEnabied" value• "true- 
-clientld- 
key. 
key: 
-Tenant" value: / > 
—¯AuthOrity" value: / > 
key- 
key: 

1. Create a new user in Azure AD and use that to login to the test web site and check.
2. Under Register App - we should set it Multi-tenant property to Multi-tenant - \*\*\*this is not clear\*\*\*

IMP - while adding users in Azure AD we are restricted to add users with same domain as domain of AD. If we want to add other users with other domains then those domains should be registered with this instance of Azure AD.

Machine generated alternative text:
Home > Another Users - A" users use' 
User 
John Doe 
• name 
john oso ft. 
Prof.l. O 
Not configured 
Default 
Groups O 
O groups selected 
Ole 
Show 

* By default - when this user tries logging in in web app now , Azure AD will ask for change in psw with its default policies.
* This login page will be of Azure AD and not part of web app itself -- it will ask for permissions to this user which App is asking for and post getting consent it will redirect to home screen of home ie Redirect URI
* Sample code uses OWIN standard for authentication and add OpenIDAuthenticationProvider to the app startup - very similar to .net core approach.

* We can enable Multi-factor authentication as well in azure AD - for this portal will redirect to another microsoft site - once set for a user azure AD will show more UI pages for setting it up when user tries to login and will provide options on SMS/tokens etc.

<https://github.com/Azure-Samples/active-directory-dotnet-native-desktop>

Access Control -

RBAC - give min privileges.

* Access Control (IAM) - available at various levels including in subscription level.
* Role is assigned to a user / groups / service principals - so also related to AD users.
* There are large number of built-in roles.
  + Contributor - almost all access but can not add other users.
  + Reader - only read
  + Owner - full control.
* Roles are built in based on each service and reader/writer/owner etc.
* Custom roles can also be created.

SAS Tokens -

* Another way to control access to resources
* With Access Keys anyone will have full access to that resource eg: storage account so it's not a great solution to control access.
  + There are 2 keys and logic is to recycle the keys. 2 keys provide more control to control the downtime.
* SAS tokens - provides great control like start and end datetime of the token usage - http/https usage - what storage service accessible with this token - R/w permissions and Resource type ie Container/ individual Object/Service .
* IMP - token are signed as well using an Access Key and in itself token once passed can not be revoked and is valid for its entire duration. To stop the access we can regenerate the Access key and that way token gets invalidated.

Generating/managing/using SAS tokens in code - need to look online

Securing Data & Encryption -

* Storage accounts are encrypted by default using Storage Service Encryption but we can use our own keys.

Machine generated alternative text:
Stor"e protects data at rest. Ange Stot ergrypts ytxjr data as Mitte-v decrypts 
it. 
Mkrosdt to 
Heze rote that after r. asta ard my existi" ti€s stev"e get ervyptcd a 
" cress 

* Using our own keys which are present in key vault

Machine generated alternative text:
Use your own 
Encryption 
key 
@ frtyn K" 
Cor#Jre required settirys 
• Ervryptön key 
Cot#Jre required settirys 
a 
key 

* If we want data to be encrypted during transmit as well then we need to enable SSL at storage account level and setting is present under configurations of storage account.

Security in Azure SQL - at server level we have transparent data encryption which again either use MS managed keys or our own keys from key vault.

This option is available at each individual database level as well but depends on parent server setting. We can turn it off in cases like where app itself is encrypting data and we don’t need to do it again at DB level etc.

Machine generated alternative text:
- Transparent data encryption 
Save X Dirard Feedbxk 
Errrypts emups. bgs ret to 
108i& IDE to 
Use y•cwr key O 
Key vault 
Select a key vault 
Sel«t a key 
the selected key the TOE pt 
SQI Ge Key. to tip k" vait. 
only to TOE If needed. try grantir" 
k_ 

IMP - master database in azure sql cannot be encrypted - keys used for TDE are stored in master database and by design it can not be encrypted.

Azure Key-vault - it is a very cheap service and has 2 tiers A1 standard and Premium with premium tier having hardware based generated keys.

* Security of key vault itself can be controlled to within a set of VNETs as well.
* Key - is public-private key pair for encryption.
* Secrets - some secrets that apps may need to use. Once generated in key vault it provides a URI to access the secret itself which can then be used in systems to get access to secrets. Secrets also have versioning option

Machine generated alternative text:
weather-service-api 
+ C) Ddete 
08321Sdf4f74d— Erded 
x 
BXkup 
db83215df4f74de1ac38e2a7e8d46edb 
Save X Ciscard 
1/23/2019. &49-31 PM 
1/23/2019. PM 
Secret Idmtifier 
Settings 
Set date? 
expo aton date ? 
O tags 
Content 

Machine generated alternative text:
nanespace lers 
public c lass : Controller 
public async System Threading. Tasks. Index() 
AzureServicerokenProvider azureSerwicerokenProvider • A2ureServicetokenProvider(); 
var keyVaultClient • Keyvaultclient( 
neu ient .xuthent Iback(atureServiceTokenprovider.KeyvaultrokenCal Iback)); 
var secret 
.Conf 
- S%ecret: 

* Certificates - for things like SSL/Https and for signing purposes.

IMP - there is a way to access key-vault from ARM templates as well without hard coding the keys/secrets etc.

<https://github.com/Azure-Samples/key-vault-dotnet-manage-key-vaults>

Scaling -

* Free plans don’t have scaling options. Also based on tier scaling options can be manual or auto scaling.
* Scale up and Scale out are two ways.
* In app services - tier can be changed after setup as well and it will be handled seamlessly.
* Auto scaling is not supported in basic tiers.
* Auto scaling can be dependent on many sources like - Resource Usage like CPU/Memory/Disk utilization etc/Queue lengths being read by app service/queues in service bus queue etc.
  + We can add many rules for scale up as well as scale down.
  + Also rules can be based on a fixed schedule like scale down in night time etc.

Machine generated alternative text:
(App Service plan) 
t (App Service plan) 
X Dirard Disable 
• Autoscale setting 
Resou g' m.p 
Default 
Auto created scale condition 
Delete warning 
• based a metrk to a 
Wistarxe cant 
"K'•de •.cak• •n •a o' Add ' uk• tha•. 
is to at kas.t 
Mininum 
Tha e—cutd of match 
candt%cn 
Scale rule 
Metric scn.ce 
Cure-nt 
Curent 
(dassk) 
qt.m.æ 
Ins.ts 
Ott*f 
Averaw 
• Metric 
CRJ 
time grain 
• statigic 
Geat« thu. 
70 

* VM Scale Sets - PAAS like but still IAAS. It is available as separate service - With this we get set of identical VMs and LB on top of it.
  + It supports up-to 1000 VMs so for very high workloads needing massive performance.
  + There is an option of setting scale set for Low Priority - where MS will provide underlying VMs when they are only available - this reduces cost but guaranteed performance is less.
  + We have 100 VMs in a single placement group and MS ensures that they are designed in a such a way that all of them don’t go down at same time. Beyond 100 VM requirement it will add more placement groups.

Machine generated alternative text:
Create virtual machine scale set 
Use rnatypd 
O 
advanced 
beymd 100 instances 
size 
set be to I a Of 
wt can gian iA.xement grcx_.ps. capo-co to to 1.0@ 
tip cfwxteristics of tip scale set. 
Lean 

Auto scaling options in Scale Set

Machine generated alternative text:
• Mmimurn runber of VMS O 
• Moirnurn nurnber VMS O 
• CPU 
• Number 0' VMS to increase by 
CPU threstold O 
• Nurnt. o' VMs to decrease by 
10 
75 
25 

* In case of single VMs - scaling option is scale up with down time. In case there is availability set under a LB, then scaling is easier where we can initiate a new VM and put it under availability set and done.
* Transient Faults -
  + We need to add resilience to our apps.
  + In case scaling down is happening and a VM is getting removed, there may be some code which gets cut in between leading to transient faults or failures.

1. Re try / Back-off logic - need to implement logic on retry and if still it doesn’t work then either rollback the transaction or use some logic to back off.
2. Other option is use of queues/databases or other messaging services - we design app to be more async.
3. We need to expect that APIs can fail and handle errors gracefully.

<https://github.com/Azure-Samples/app-service-dotnet-scale-web-apps>

Caching and CDN -

* Redis cache - open source caching framework for in-memory caching. It has its own unique URI

Machine generated alternative text:
Redis Cache 
•2 
Mkrog»ft Azure C.ac:tæ on open source Redis It 
m:cess to a t" Mkrosoft. Users of tx»th 
'Eh set «oSyStern. hmte-.g aryl from 
Mkrog»ft Azure Cm:tæ ttw 
• - rode. kW 
tier SEA 
• qar&d — A r+cated in a tm marypd 
M*rosoft. with a h*lh availabity 
• Pr«'ü..rn • tip 
t*tt« c«npared to Bask or 
eriwxed 
Azure C.:t-æ F*lps stay as bad 
does the of ens*.e. this 
separate dKtrüNted cad* layer alkms data to "Operuient* for effkient 

* Better to have cache in same location as our apps for low latency.
* It is in-memory based but premium tiers have data persistence where cache of a given session can be stored to disk and later retrieved again.
* This shouldn’t be used as primary data source in apps since its for caching purpose only and there is potential of loosing data.
* Pricing varies from very low to very high cost per month depending on Data persistence, storage capacity , dedicated or shared infrastructure , network security for access control etc.

Using it with .Net -

* Nuget package - redis nuget - StackExchange.Redis.
* MS has its own versions for redis as well. They are official packages but StackExchange.Redis is industry standard used mostly.
* We have redis connection string for StackExchange as well in portal

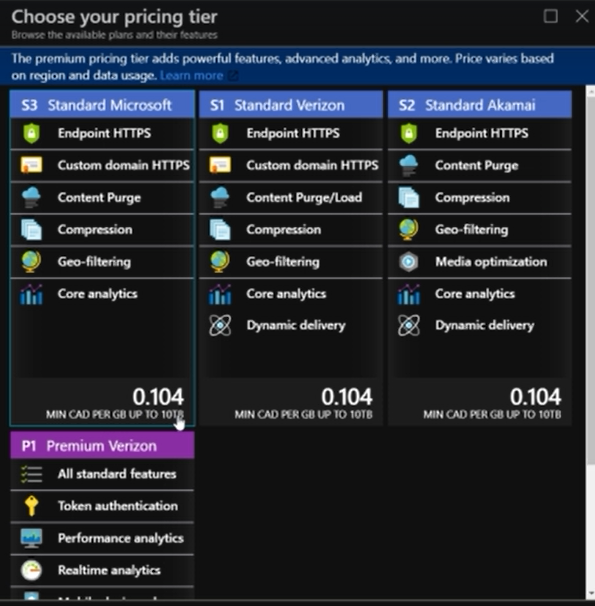
Code sample - for .net objects we can serealize and save as strings. There are many other options as well apart from strings.

Machine generated alternative text:
class Progr•n 
private static string CacheConnection z 
static void args) 
IDatabase cache • lazyConnection.Vaiue.GetDatabase(); 
Cache : " • 
Cache : " cache -wr•fting to Redis " 
Cache : • cache . StringGet( 
cache .KeyExpire(-Session333", 
t ion. Value. ) 
any key... 
Console.ReadLine(); 
private static la:yConnection z neu 
return Connection"ultiplexer 

* CDN - for static content geo caching. - sits in front of web site for faster access to static content - often closer to web server location - we don’t choose any location for it and it's global service -

Machine generated alternative text:
CDN profile 
'Anne 
• Resource qrm.p 
erating__ 
rV•w 
• full details) 
Create a new CON no. 
x 

* Standard and premium tiers from vendors

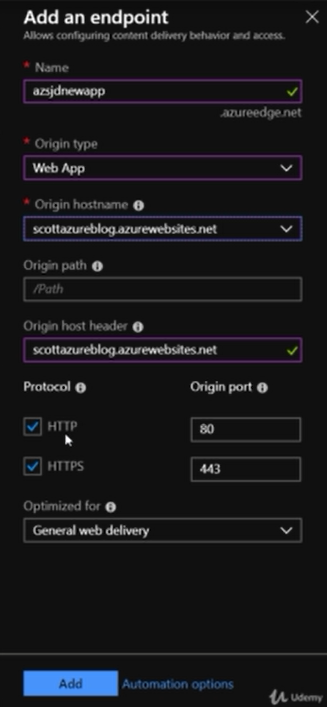


Premium tier is having options for mobile devices where different image can be served with same URI to mobile devices, authentication features on static content etc.

Machine generated alternative text:
0202 
'0 tote 

* CDN Endpoint - once profile is created, we need URI to connect to it . Origin can be web app / storage account or any other custom URL like website hosted on-prem or AWS etc.

Once set it basically replace original host name with name of CDN for static content.



* First time files will be served from web servers and cached in CDN and then retrieved from CDN.
* IMP - when apps are re-built and re-deployed we can automate purging of CDN content as well using automation scripts or other option is adding version # in file name and that way we don’t need to purge and it will be added as new item to CDN cache.

Calling it in code -

----Monitoring and Logging ----

Azure Monitor - is a service which will collect all logs from individual services and consolidate them in single central place - we can query then-- create graphs

Can collect logs from VMs/networks/containers etc

Eg: Under VM Diagnostics we can install an extension for monitoring resources utilization . Agent itself needs its own storage account and storage quota which can be set up manually as well under agent tab.

Machine generated alternative text:
Performance counters 
Logs 
Crash dumps 
Sinks 
Agent 
Ann e metrics — CPU — 
for in*lht this rnætW. cm metrics k%.qK 
tir Azure can to otirr e. 'n 
TO rm. 
Erubte mowtot'nq 
tip data to Of tip 
to at 

Once installed we can configure what we want to monitor and log like counters/event logs/crash dumps/IIS logs etc

IMP - same data from diagnostics can also be sent to Application Insights apart from Azure Monitor.

Difference between Azure Monitor vs App Insights

**Application Insights** : offers rich detection and diagnostics for issues at the **application** layer of your service. This is about YOUR code and how well it runs. AppInsights is well-integrated on top of data from **Azure Monitoring** but can also be used to track desktop and web **applications** deployed anywhere