



Microsoft Azure Cloud Kavramları

MUSTAFA ÖZDEMİR

İçindekiler

Azure Temel Kavramları	3
Business Agility (İş Çevikliği).....	11
Microsoft Temel Azure Servisleri	13
Microsoft Azure Subscription Kavramı	14
Microsoft Azure Active Directory	17
Microsoft Azure Virtual Networking Kavramı	19
Microsoft Azure Storage Kavramı	29
Bitiş	49

İlk bölümümüzde High Availability , Fault Tolerance , Disaster Recovery kavramlarını inceliyor olacağız. Bu kitap ile birlikte bulut bilişimi kullanmanın sayısız avantajlarından söz edeceğiz aynı zamanda.

“ High Availability “ yani “ Yüksek Kullanılabilirlik “ anlamına gelmektedir. Kabul edilebilir bir sürekli performans , Servislerde geçici süreliğine problem ve arızalara rağmen Donanım veya Veri Merkezini Sürdürme kabiliyeti diyebiliriz ve buradaki en önemli nokta bizi arızalardan veya problemlerden korumaktır. Yani buradaki mottomuz **“ Kabul Edilebilir Sürekli Performans “**

Örnek olarak ; Web sitenizin Trafığı değişse çok artarsa veya çok azalırsa veya Azure Servisleri hata verirse yada en kötüsü donanım arızalanırsa yada çok daha kötüsü tüm veri merkezinde problem olsa bile Organizasyon uygulamalarımız ve sistemlerimiz kabul edilebilir sürekli performans halinde çalışsa mükemmel olmaz mı ? Olur. Peki Azure bunu nasıl başarıyor . **Şimdi ona bakalım :**

Azure Veri merkezlerindeki enerji sistemleri kendini gücünü üretmekte , Veri Merkezine gelen gücün yani 2 Veri merkezinizden 1’inde kesinti olursa diğeri ayakta kalır. Enerji sistemlerinde daima yedeklilik mevcuttur.

Azure Veri merkezlerinde Soğutma sistemlerinde olağan derecede çok dikkat edilmekte , Farklı ve kaliteli iklimlendirme sistemi kullanılmaktadır. Soğutma ; Su soğutma ve hava Soğutma sistemleri gibi.

Azure Veri Merkezlerindeki Network yani Ağ donanımları Switch’ler , Router’lar ve bir çok ağ donanımları bulunmakla birlikte ; Servis sağlayıcıları hizmet vermektedir. Yani 2 Veri Merkezinden 1 tanesi yine çalışmıyorsa veya kesinti mevcutsa diğeri 1 tane veri merkezi ayakta olabilir.

“ Availability Zone “ yani **“ Erişilebilirlik Alanı “** olarak anılmaktadır. Bunu şöyle açıklayabilirim . Bir anlama gruplandırmadır. 1 veya daha fazla Veri Merkezinin bir araya getirilmesidir. Bu sayede Organizasyon uygulamalarınızı ve Sistemlerinizi dağıtık bir mimaride tutabilirsiniz. Örnek olarak ; Birden Fazla Availability Zone gibi. 2 Availability Zone alanına dağıtım sağladığımız düşünürsek , 1 tane Availability Zone’daki bir Veri Merkezimiz kesintiye uğradığında , tüm sistemlerimizi 2 Veri Merkezimizde çalıştırabiliriz. Yani uygulamalarınız ve sistemleriniz bu süreçte up durumda olabilir. Örnek olarak Availability Zone bölgelerinde doğal afet , deprem yada acil durum yaşanır ; Erişilebilirlik Alanlarından daha yüksek olan **“ Region Redundancies “** bunları yani birden fazla Erişilebilirlik alanı bir araya getirmektedir.

Microsoft'un sitesinde Azure'un 60'dan daha fazla bölgesi olduğunu görebilmekteyiz. Azure'un Dünya çapında 140 ülkede var olduğunu görürüz. Neredeyse Dünyanın neresinde olursanız olun. Azure Bölgesine her zaman yakın yeredesinizdir 😊

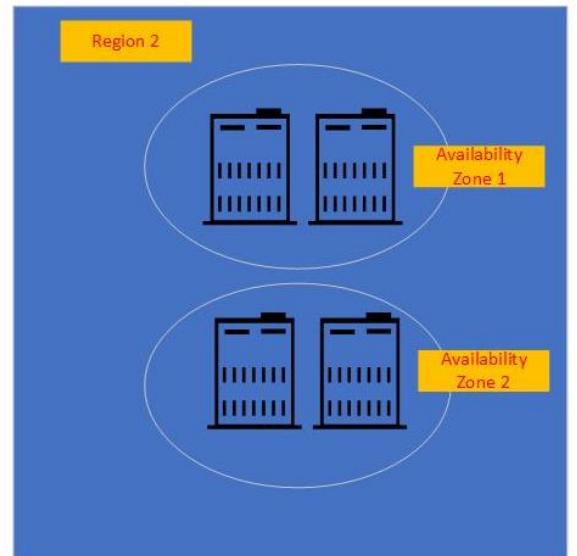
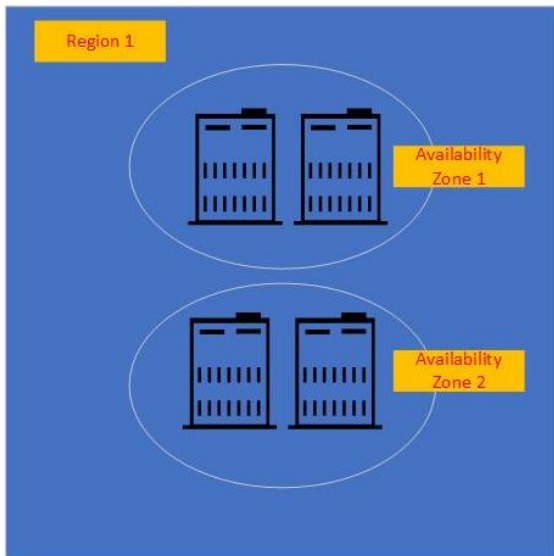


<https://infrastructuremap.microsoft.com/explore>



Bir Bölge , Birden Fazla Availability Zone'ları bir araya getirmektedir. Aşağıdaki şekile göre anlatmam gerekirse ; Soldaki Region 1 ve içerisinde 2 adet Availability Zone görüyoruz ve bunların her birinde 2 Veri Merkezi görüyoruz. Tek bir veri merkezinde bir problem yaşandığında , Availability Zone konfigürasyonları sağlandıysa , Organizasyon uygulamamız ve Sistemimiz ikinci bir Veri Merkezinde olabilmektedir ve Çalışmaya devam edebiliriz. Tüm Availability Zone'ları etkileyen Aynı şekilde bir felaket anı olursa, Uygulamalarımızı ve Sistemlerimizi birden fazla Availability Zone'da dağıtma seçeneğimiz mevcut. Yani Zone'lerden biri düşse bile diğer zone çalışmaya devam edebilir. Ve Son olarak Region 1 'de bulunan Tüm Availability Zone'lar ve tüm Veri Merkezleri çöktüğünde diğer Region 2'den faydalanabiliriz.

Daha çok örneklemek gerekirse ; Region 1 'de Deprem oldu. Bu sırada Tüm uygulamalarınızı Region 2'de barındırabilir ve çalışmaya devam edebilirsiniz.



Şimdi değineceğimiz sonraki şey “ **Fault Tolerance** ” yani “ **Hata Toleransı** ”

1 veya birden çok sistemin düzgün çalışmaya devam etmesi için Sistemin Yeteneğini ifade eder aslında. **Fault Tolerance’nin 2 yolu mevcut : Proaktif Yol ve Reaktif Yol diyebiliriz.**

Proaktif Yol , Hatalar oluştuğunda bunları ele almanın bazı proaktif yolları ve sistemlerimizin düzgün çalışmaya devam etmesini sağlamak için verilerimizi , uygulamalarımızı ve kaynaklarımızı düzenli olarak yedeklemek ve herhangi bir şey olduğunda ve gerektiği zaman Recovery işlemi yapmak için hazır olmamız gerekmekte ve tekrar sistemlerimizin , uygulamalarımızın çalışmasını sağlamak gerekmektedir.

Ayrıca Birden fazla Availability Zone’da dağıtabiliriz veya daha önce bahsettiğim gibi 1 Availability Zone varsa veya bölge çöküyor ise , Sistemlerimiz başka yerde ayakta kalacaktır. Ayrıca birden fazla Availability Zone’da veya bölge 1 tanesi düşse bile trafiğimiz otomatik olarak yeniden yönlendirme sağlanacaktır.

Ve tabikide sistemler için en önemlisi Telemetry Verisi, Verilerimizin , Uygulamalarımızın sağlığını izleyebiliyoruz. Yani Verilerimiz ve uygulamalarımızla alakalı birşey yaşanmaması adına hemen aksiyon alacağımız veriler ediniyor oluyoruz.





Hatalar yaşanmadan önce bu yoldaki süreçleri izleyerek aksiyon alırsak , Ortamımızdaki Hataları azaltmış oluruz.


Reaktif Yol , Sistemlerimizi devre dışı bırakan birşey olursa , bununla alakalı aksiyon almamızdır. Uygulamalarımızı mümkün olduğunca ayağı kaldırmaya çalışırız. Verilerimizi, uygulamalarımızı ve kaynakları farklı bir çevreye , Farklı bir Availability Zone veya Bölgede tekrar ayağı kaldırarak olabildiğince hızlı bir şekilde çalıştırabiliriz. Ayrıca , Availability Zone’larımızdan veya bölgelerimizden biri kapalı durumdaysa , Farklı bir Availability Zone hedefleyebilir yada Region yani bölge ve sistemlerimizi oraya dağıtarak tekrar hızlı bir şekilde çalışmasını sağlayabiliriz.

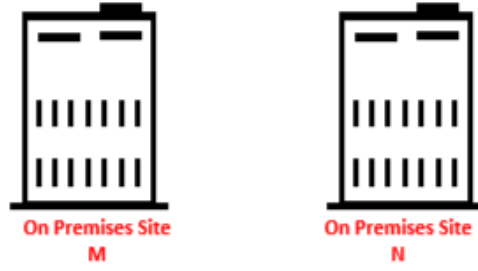
Yani Azure’da ilk evrede başarısızlıklardan uzak durmaya çaba göstermek , birden fazla Availability Zone’a veya Bölgeye deployment yani dağıtmak , Hata aldığımızda ise onu olabildiğince hızlı çözüme kavuşturabilmek için almış olduğumuz yedekleri kullanmak ve yedeklerden geri dönmemiz gerekmektedir.

Son değineceğimiz konu ise “ **Disaster Recovery** ” yani “ **Felaketten Kurtarma** ”

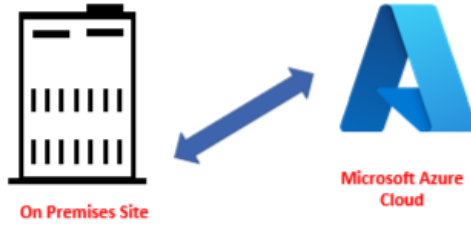
Bu bir sistemin yedekleme yeteneğidir diyebiliriz. Ortamınızda gereksinim duyulduğunda Verileri ,Uygulamaları veya kaynaklarımızı Restore etme diyebiliriz ve aslında bunu çeşitli şekillerde yapabiliriz :

-  On-premises to on-premises
-  On-premise to Azure
-  Other cloud to Azure
-  Azure to Azure

-  **On-premises to on-premises** ; On-Premise yapınız varsa , M ve N Veri Merkezleri gibi . Verilerimizin , Uygulamalarımızın tüm yedeklerini saklayabiliriz. Böylece On-Premise yapıdan On-Premise yapıya Restore işlemi yapabiliriz.



- ✚ **On-premise to Azure** ; On-Premise yapınızda herhangi birşey olduğunda yedeklerimizi Azure ortamında muhafaza edebilir ve orada Recovery işlemi sağlayabiliriz.



- ✚ **Other cloud to Azure** ; Sistemlerimiz farklı bir Cloud Service Provider yani Farklı Servis Sağlayıcısıdaysa , Verilerimizin, Uygulamalarımızın yedeklerini Azure ortamındaki kaynaklara veya Azure Site Recovery ile geri yükleme sağlayabiliriz. Kapasiteniz ne olursa olsun , Diğer Bulut hizmetinden doğrudan Azure'a Restore etme olasılığınız mevcuttur.



- ✚ **Azure to Azure** ; Verilerimiz ve uygulamalarımız zaten Azure ortamında mevcut ise ve çalışıyorsa, Tüm yedeklerimizi Azure ortamında birden fazla farklı bölgede muhafaza edebiliriz. 1 Bölgede kesinti olması durumunda ikinci bir bölgede çalışmaya devam edebiliriz ve bu şekilde Azure'dan Azure'a Restore işlemi gerçekleştirebiliriz.

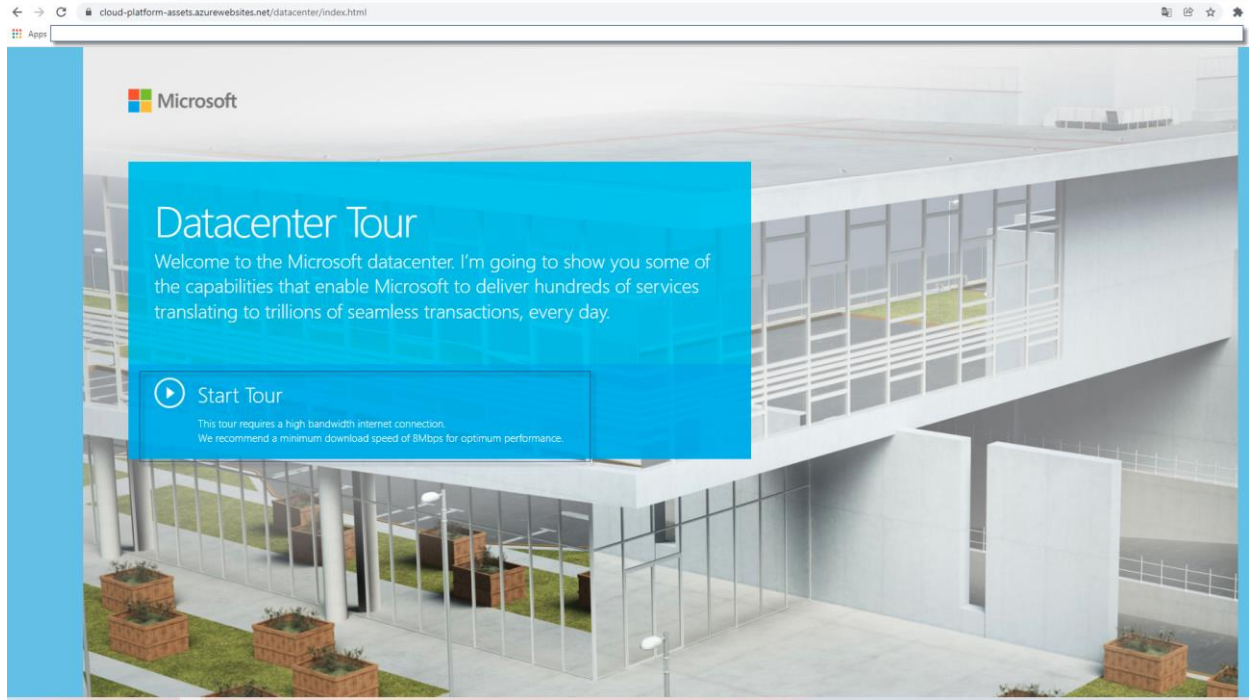


Yukarıda birden fazla Disaster Recovery çeşidi olduğunu görmüş olduk. Yani bir Felaket yaşadığımızda ister kendi Veri Merkezimize , Başka bir Cloud Service Provider veya bir Azure Veri Merkezi ve daha fazlasında Servislerimizi Restore işlemi sağlamak için çözümlere sahibiz ve onları tekrar çalışabilir duruma getirmek için çözümlere sahibiz.

Bu kadar Veri Merkezi Veri Merkezi dedik 😊 O zaman Azure Veri Merkezini Turlamaya ne dersiniz ?

<https://cloud-platform-assets.azurewebsites.net/datacenter/>

Sayfa içeriğinde Start Tour seçeneğini seçerek turlamaya başlayabilirsiniz. Lobi , Sunucular , Soğutma, Güç sistemleri , Herşeyi nasıl modüler halde çalıştırdıkları ve Azure Datacenter'lar nasıl çalışır veya hiç kesintisiz halde durulması sağlar. Mümkün olduğunca incelemenizi öneririm.

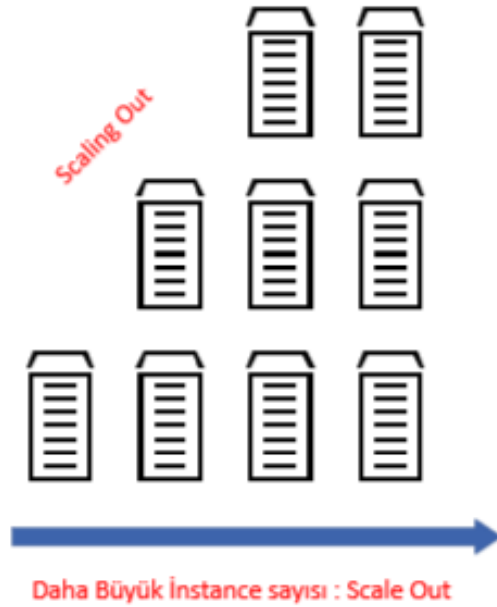


İkinci bölümümüzde Bulut Bilişimde önemli avantajlardan birini sağlamak için birbirine bağlanan 2 kavramı açıklamaya çalışacağız. Scability ve Elasticity kavramlarını inceliyor olacağız.

Bu kavramlardan her ikisinde düşünmeye çalışalım bir kopyalamanın kendi Veri Merkezimizde bize nelere mal olacağını aktarmak istiyorum.

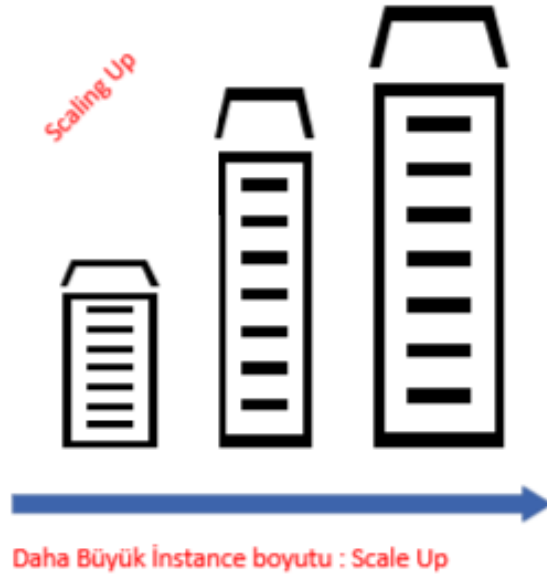
Scability , yani ölçeklenebilirlik ; Instance sayısını veya mevcut kaynaklarınızın boyutunu arttırma yeteneğidir ve bunu 2 farklı şekilde yapabiliriz. Mevcut kaynaklarımızdan Instance sayısını arttıracak şekilde ölçeklendirebiliriz.

Aşağıdaki şekillere göre örnek olarak sunucularımızın sayısını arttırabilirsiniz. Yani soldan 1 sunucu ile başlıyoruz ve ölçeklendirebiliriz. 1’den 4 sunucuya 4’de 6’ya kadar sunucuya arttırım yapabilmekteyiz ve Her sunucu aynı CPU,RAM, Sabit sürücü kaynaklarına sahip olacaklar. Yalnız buradaki artan kaynağı ise sunucu havuzuna ekleyerek isteklerimizi karşılayabilecek duruma gelmiş oluruz. Bu işlemler pek krik olmayan işlemlerdir. Ölçeğimizi genişletmek için çevrimdışı herhangi bir makinede işlem yapmak zorunda değiliz. Tek yapmamız gereken bahsetmiş olduğumuz havuza ek olarak bir sunucu eklemek yani ortamdaki istediğimiz özellikleri veya servisleri yerine getirmemiz gereken sunucular ve Diğer sunuculardan belli bir iş yükü yüzdesini almak için otomatik olarak kullanabilir hale gelmektedir. Yani kısacası ölçeklendirme , daha fazla isteklere karşılık verebilmemiz için sunucu sayısını arttırıyor.



Farklı bir ölçeklendirme türü de vardır. Buna Scalling Up yani Ölçek büyütme denmektedir. Ölçek büyütme sunucularımızın sayısını arttırmaz . Alttaki şekile bakarsak , 1 Cpu ve 8 GB Ram donanımlı bir sunucu ile başladığımız düşünelim. İş yükümüz arttıkça mutlaka sistemimize gelen trafik değil , ancak her sunucunun iş yükü olarak artışlar gerçekleştirilmeli ve Sunucularımızı büyütebilme imkanına sahip oluruz. 1 CPU ve 8 GB Ram’den , Potansiyel olarak 2 CPU ve 16 GB RAM’li donanıma yükseltebiliriz ve iş

yükümüz daha da arttıkça, daha büyük bir makineye gidebiliriz. Ve Diyelim ki 4 CPU ve 32 GB Ram’li donanıma geçebiliriz. Yapımızdaki mevcut Sanal Makineye daha fazla kaynak ekleyebiliriz.



Yani genellikle ölçeklendirmenin 2 metodu mevcut.

Ölçekleniyor veya ölçeklenmiyor olsun. Her ikisinde kaynaklarımızı artırma esnekliği sağlamaktadır.

Şimdi değineceğimiz sonraki şey “ **Elasticity** “ yani “ **Esneklik** “

Tüm Azure Cloud ortamını Lastik Bant gibi düşünebiliriz. Bunu şuna benzetebilirim. Lastik Bandı çekip daha büyük yapabiliriz yada onu çekmeyi bırakıp daha da küçük yapabiliriz. Esneklik artma yeteneğidir yada Azure ortamındaki mevcut kaynaklarımızın Instance sayısını veya boyutunu azaltabilirsiniz. Bunu ortamınızdaki yoğunluğa veya yüke göre yapabilirsiniz. Her iki yönde de ölçeklendirebiliriz. Azure ortamımızdaki sunucular genişletebilir yada arttırabilirsiniz. Azure ortamınızdaki sunucu sayısını ölçeklendirebilir ve azaltabilirsiniz.

Elasticity ile Ram yada CPU’ya dayalı olarak otomatik ölçeklendirme yapabilirsiniz. Bunu otomatik işlemin yanısıra manuel işlem şeklinde de gerçekleştirebiliriz.

Elasticity Uygulamalarımızın ve sunucularımızın yük veya iş yükündeki değişikliklere dayanmaktadır. Azure ortamınızdaki uygulamalarımızdaki ve uygulamalarımızdaki yük değişikliklerine yanıt vermek için kaynaklarımızın miktarına göre konfigüre edebilirsiniz.

Bulut avantajı olarak sadece kullandığımız kadar öderiz. Fazladan 1 sunucu kurmamız gerekirse hatta 50’ye yakın sunucuyu ortamımızda istersek sadece 50 sunucu için çalıştığı kadar ücret ödemekteyiz. Onlara ihtiyacımız kalmadığında ise artık onlara ücret ödememekteyiz.

Yani 1 tek veritabanı ile başlayabilir ve trafiğimiz , yoğunluğumuz daha çok arttıkça 6 tane yada isteğimize göre artırma işlemi gerçekleştirilebilmektedir. Bu işlemleri manuel olarak ta gerçekleştirebiliriz. Ve 6 adete yakın veritabanına ihtiyacımız kalmadığında bunları 1 tane olacak şekilde konfigüre işlemi gerçekleştirebiliriz.



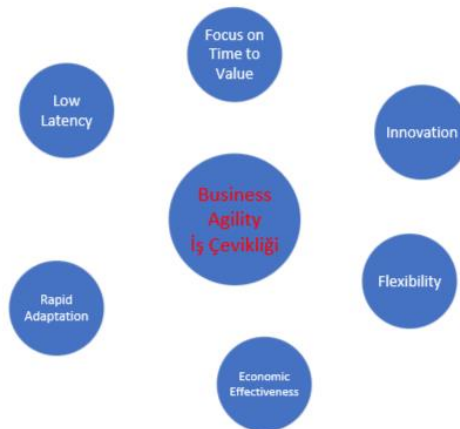
“ **Elasticity = Scalability** ” diyebiliriz.

Uygulamalarımızdaki değişikliklere gerçek zamanlı olarak yanıt vermek , ekstra iş yükü gerektiren zamanlarda istenilen kaynakları sağlamamıza büyük fayda sağlamaktadır. Bunu Azure dışındaki On-premise sistemde yaptığımızı düşünürsek ; Biraz daha maliyetli olduğunu söyleyebiliriz. Sunucu satın alınması , kurulum sağlanması, yönetimi ve sağlıklı çalışmasını sürdürme işlemlerini ve süreçlerini sağladık ve bu harcamaların geri dönüşünde ise zarar etmiş olurduk ve Sürekli ürün tedarik sağlamak çok maliyetli olduğunun bilgisini vermek isterim. Kullanılmayan kaynağında boşa kalmasına neden olmuş oluruz.

Business Agility

Kitabımızın bu bölümünde Azure Cloud Ortamımızda nasıl iş çevikliğinin nasıl kazanabileceğimizden bahsediyor olacağız.

Microsoft Azure kullanarak daha fazla iş çevikliği kazanabiliriz. İlk önce iş çevikliğinin ne anlama geldiğini açıklamak istiyorum: Bir organizasyonun Pazar ve çevresel değişikliklere verimli ve uygun maliyetli yollarla ve mevcut kaynaklardan istifade ederek müşterilerinin taleplerine hızla uyum sağlama yeteneğidir. Kısacası , her türlü değişime hızlı uyum sağlama yeteneğimizdir diyebiliriz. Her organizasyon pek tabiki müşterilerine mümkün olan en iyi sürede ürün sunması ve bu süreci en uygun maliyetle gerçekleştirmektir.



İlk nokta Focus on Time to Value yani Değer verme zamanına odaklanmak . Bunun anlamı Piyasaya mümkün olan en kısa sürede yeni ürünler çıkarmak istiyoruz. İster müşterilerle ister organizasyon içeriğindeki çalışanlarımız olsun Ürünlerimiz ile ilgili daha kısa geri bildirim döngüleri istiyoruz ve organizasyonumuz için yatırımımızın daha hızlı geri dönüşünü istiyoruz. Azure bize tüm bu şekillerde

yardımcı olmaktadır. Yeni kaynaklar sağlamak veya kaynaklarımızı ölçeklendirmek ve büyötmek için Lazım olan süreyi kısaltmak isteriz. Ve işimize daha fazla odaklanarak , Bilgi Teknolojileri yönetimi yerine , ürünlerimizi pazara sunabiliriz. Mümkün olduğunca çabuk ve bu geribildirim döngülerini kısaltabiliriz.

İkinci nokta Innovation yani iş içinde Yeniliğe odaklanmak. Her zaman işleri yapmanın daha iyi yollarını aramak isteriz. Daha yeni ve daha iyi teknolojileri kullanmak ve Azure Cloud bunu tekrardan yapmamıza izin vermektedir. Bilgi Teknolojileri yönetimine az odaklanarak , daha fazla işimizi geliştirmemize destek vermektedir. Azure daha ucuz maliyeti ile sadece kullandığımız kadar ödeyerek, bunun yerine farklı noktalara odaklanabiliriz. Veri merkezine veya sunuculara değil , Ürünlerimizi daha iyi hale getirmek için Daha çok çalışanlarımız veya fikirlerimiz üzerinde zamanımızı değerlendirebiliriz. Microsoft Azure'daki yalnızca sınırlı kaynaklar için ödeme yaparız. İşimizin ve çalışanlarımızın fikirleri daha fazla inovasyon sağlamaktadır.

Üçüncü Nokta Low Latency yani düşük gecikme süresine bakacağız. Bir işe karar verildiğinde bu kararın doğru mu yanlış mı olduğunu öğrenene kadarki süreden bahsediyoruz. Çünkü bir karara göre ne kadar erken harekete geçilebilirse , organizasyon bu kararının doğru yada yanlış ve başka ne yapılması gerkeiyordu bu gibi süreçlerin ne kadar erken olduğunu bilir. Azure sağlama yeteneği ile yüzlerce hatta binlerce sunucu bile anında çalışır hale gelmektedir. Bu bize uzun vadede çok daha az zaman ve maliyet sağlamaktadır. Sunucularımızı Satın almak ve yapılandırmak zorunda kalmadan Azure Cloud ortamında dağıtmamıza odaklanmamızı sağlamaktadır . Bu bulunmuş olduğumuz piyasaya daha hızlı cevap vermemizi sağlamaktadır.

Dördüncü Nokta Economic Effectiveness yani Ekonomik etkinliğe bakacağız. Organizasyonda yürütmüş olduğumuz süreçlerimizde mümkün olduğunca uygun kaynak kullanımı ve maliyet ile gerçekleştirmek isteriz ve Azure ile Organizasyonumuzda yüzlerce veya binlerce Sunucu hemen temin edilebilmekte, yalnızca kullandığımız kadar ödeyebilmekteyiz . Kendi veri merkezlerimiz konusunda fiziksel koruma veya işlemleri yürütmek yılda milyonlarca dolara mal olabilmektedir. Artık eskisi kadar personel çalıştırmak yada bulundurma zorunluluğumuz kalmamaktadır. Organizasyonumuzun Bilgi Teknolojileri kaynaklarımızı veri merkezinde yönetmemiz ve artık ekstra sunucu satın almak zorunda değiliz. Bunun yerine Azure Cloud avantajının Scalability yani ölçeklendirme özelliğine güvenerek bu sayede Yalnızca Kullandığımız Kadar ödüyoruz . Kendi veri merkezimiz yerine sadece bulutu kullanarak kendi organizasyonumuz için ekonomik farkındalık sağlayabiliriz.

Beşinci Nokta Rapid Adaptation yani Hızlı Adaptasyona bakacağız. Organizasyon olarak pazardaki değişikliklere hızla uyum sağlama yeteneğimiz anlamına gelmektedir. Azure ile daha önce bahsettiğim gibi , ihtiyacımız olan ve bize yetenek veren herhangi bir sayıda ve türde kaynağı hemen dağıtmak için pazardaki değişikliklere hızla uyum sağlayabiliyoruz. Örnek olarak anında gelişen sunucu kurulumları veya istekleri için hızlıca aksiyon alabilir. Sadece kullandığımız kadar ödeyebiliyoruz ve piyasa koşullarına organizasyonumuz hızlı bir uyum sağlamış olmaktadır. Microsoft Azure ile Bilgi Teknolojileri kaynaklarımızın tedarik edilmesini ve yapılandırılmasını sağlayarak olabildiğince hızlı şekilde yada anında gerçekleşmektedir.

Altıncı nokta Flexibility yani Esneklik kavramına bakacağız. Organizasyonumuz için uzun vadede daha fazla esneklik sağlamaktadır. Microsoft Azure Cloud ortamının avantajlarından hızlıca yararlanmak için hızlıca hareket edebileceğimiz için yeni fırsatlar sayesinde işimiz daha esnek hale gelmektedir. Organizasyonumuzun dahil olmadığı ,Yeni pazarlardan ve yeni alanlardan yararlanabiliriz ve bu organizasyonumuzu değişikliklere karşı daha esnek kılmaktadır. Aksi takdirde dezavantajlı olabilir ve

böylece bir bütün olarak , Microsoft Azure dünyanın dört bir yanındaki bölgelere Yüksek kullanılabilirliğe sahip olmamız, Ortamımızdaki Teknik problemlerden ve felaketlerden kurtulma yeteneği ile organizasyonumuz için daha fazla esneklik sağlamaktadır.

Bu saymış olduğumuz 6 kavram için organizasyonunuza katkısı çok fazla olacaktır. Günün sonunda daha iyi bir iş yürütüyor olacaksınız ve sizi yoran , rutin operasyon işlemlerini en az indirgeyerek , geliştirme süreçlerine ve işlerine dahil olmak mümkün hale gelebilecektir. Microsoft Azure ile bu konuda mevcut ortamınızdaki herşeyi en iyi ve hızlı şekilde yönetiyor olursunuz.

Temel Azure Servislerini İnceleme

Kitabımızın bu bölümünde ise Microsoft Azure Cloud ortamına ait Compute Servisleri inceliyor , detaylandırıyor olacağız.

İlk öncelik hangi konulardan bahsediyor olacağız. Hemen onları maddeler halinde sıralayalım :

- ✚ Subscription yani Abonelik kavramı
- ✚ Microsoft Azure Active Directory kavramı
- ✚ Microsoft Azure Virtual Network yani Sanal Ağ kavramı
- ✚ Microsoft Azure Virtual Machine yani Sanal Makine kavramı -Bununla alakalı güzel bir kitap çıkarmıştım 😊 Onu inceleyebilirsiniz.
- ✚ Microsoft Azure Storage yani Depolama kavramlarını

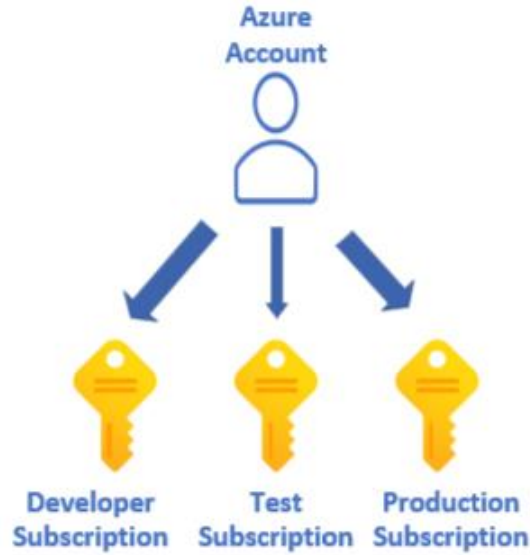
Yeterince detaylandırmaya çalışacağım. O halde hiç zaman kaybetmeyelim.

İlk Azure Compute Servisimiz “ Subscription “ ile başlayalım :

Subscriptions



Microsoft Azure ortamında bir Subscription konseptimiz mevcut. 1 veya 1’den fazla aboneliğiniz mevcut olabilir. Ancak bir abonelik kapsamaktadır. Birden çok Azure Bölgesindeki kaynaklar ve kiracılar birden çok kaynaklar ve kaynak grubu içerebilir.

Azure Subscription, Organizasyonunuzda veya kişisel Lab ve Proje kullanımlarında Microsoft Azure ortamını kullanmak için gereklidir. Bu abonelik, Organizasyon veya kişisel kullanımlarınız için Azure ürünlerine ve hizmetlerine erişimi Doğrulanmış ve yetkilendirilmiş şeklinde Azure ortamına erişmenizi sağlamaktadır.



Azure Ortamınızda Organizasyonunuz için oluşturduğunuz Azure Hesabı, Farklı maliyetlendirme ve faturalandırma modellerine sahip bir veya birden fazla Subscription’a (Aboneliğe) sahip olabilir.

Subscription kavramından bahsettik. Şimdi ise Abonelik Sınırlarından bahsedelim. Microsoft Azure’da iki tür Abonelik sınırı mevcuttur:

-  Billing boundary
-  Access control boundary

Billing Boundary, Faturalandırma Sınırı olarak anılmaktadır. Bu Abonelik sınırı türünde, Organizasyon veya kişisel kullanımlarınız için Azure Hesabının kullanımı için nasıl maliyetlendirileceği veya faturalandırılacağını belirler.

Organizasyon veya kendi kullanımınızda olan hesaplar için farklı faturalandırma gibi ihtiyacınız mevcut ise birden çok abonelik oluşturabilirsiniz. Azure Yapınızda oluşturmuş olduğunuz her aboneliklerinizi ayrı ayrı Faturalandırma İşlemi ve Fatura Raporlarına erişme imkanı bulursunuz. Bu sayede Organizasyonunuzda maliyetleri daha rahat düzenlersiniz veya yönetme imkanı sağlamış olursunuz.

Access Control Boundary, Erişim Denetim Sınırı olarak anılmaktadır. Bu Abonelik sınırı türünde, Azure ortamınıza abonelik düzeyinde Erişim Yönetim Politikaları uygulayabilir, Farklı organizasyon yapılarına yansıtmak için ayrı abonelikler oluşturabilirsiniz. Bunu Örnek olarak açıklayalım o halde;

Organizasyonunuzda farklı Azure Abonelikleri uyguladığınız farklı departmanlarınızın olması şeklinde güzel bir örnek verilebilir. Bu Faturalandırma modeli, Kullanıcının kullandığı kaynak erişimlerini kontrol etmenizi ve yönetmenizi sağlamaktadır.

Organizasyon Yapınızda Kaynak ve Fatura yönetimi amacıyla Ek Azure Abonelikleri oluşturmak da isteyebilirsiniz. Aşağıda belirteceğimiz kavramları ayırmak için ek abonelikler oluşturmaya seçebilme imkanınız mevcuttur.

- ✚ **Environments (Ortamlar):** Kaynaklarınızı yönetirken, kurulum için abonelikler oluşturabilirsiniz. Ne gibi işlemlerde kullanılabilir? Developer ortamları, Testing ortamları , Güvenlik yada Uyumluluk için verilerinizi Production(Canlı) ortamdan izole edebilme gibi işlemleri sağlayabilirsiniz.
- ✚ **Organizational Structures (Organizasyon Yapıları):** Yukarıda bahsetmiş olduğumuz gibi Farklı Organizasyon yada departmanlar için abonelikler oluşturabilirsiniz. Her departmanın Azure Ortamını veya Kaynak kullanım oranı aynı olmamaktadır. Onun için Yapınızdaki Departmanların yapılarına ve Kaynak Kullanım oranlarını düşük maliyetli kaynaklarla sınırlayabilirsiniz.
- ✚ **Billing (Faturalandırma):** Faturalandırma amacıyla ek abonelikler de oluşturmak isteyebilirsiniz. Maliyetler, ilk olarak abonelik seviyesinde toplanmışsa, yönetme ve izleme işlemleri için ayrı abonelikler oluşturmak isteyebilirsiniz. Örnek olarak; İhtiyaçlarınıza göre yani Production ortamınıza ayrı, Developer ve Testing işlemleri için ayrı ayrı abonelikler oluşturabilirsiniz.
- ✚ **Subscription Limits (Abonelik Sınırları):** Microsoft Azure Abonelikleri bazı katı sınırlamalara tabidir. Örnek vermek gerekirse; Abonelik başına Azure ExpressRoute (Organizasyonunuzda Azure Veri Merkezi ile Altyapınız arasında özel bağlantılar oluşturmak için kullanılmaktadır.) devre sayısını 10'a kadar oluşturabilirsiniz. Özellikle bu sınırların üzerine çıkabilmek için ek aboneliklere ihtiyacınız olabilir.

Organizasyonunuzda birden fazla aboneliğiniz mevcutsa bunları fatura bölümleri halinde düzenleyebilirsiniz. Her Fatura bölümü, O ay yapılan masrafları göstermektedir. Örnek olarak şöyle bir ihtiyacınız olabilir? Organizasyonunuz için tek bir fatura, fakat ücretleri Departman, Ekip veya projeye göre düzenlemek istiyorsunuz. Organizasyon ihtiyaçlarınıza göre, aynı faturalandırma hesabı için birden fazla fatura oluşturabilirsiniz. Bu işlemi yapabilmek için ek Faturalandırma Profilleri oluşturabilirsiniz. Her Faturalandırma profilinin kendine göre aylık faturası ve ödeme yöntemi olacaktır.

Microsoft Azure Active Directory

Azure ortamında kullanıcıları ve izinleri yönetme önemsiz bir konu değildir. Uzman bilgisi ve becerileri gerektiren büyük bir görevdir. Azure Active Directory , Kullanıcıları ve izinleri yönetmek için kullanılan bir ana araçtır.

Active Directory , Adı çok benzer olsa da , Azure kelimesi olmadan oldukça farklı bir üründür. Herşeyden önce Geleneksel bir ofis için tasarlanmıştır. (Ofisteki Fiziksel bilgisayarlar , Yazıcılar ve Fiziksel Erişim)

Active Directory , Web için tasarlanmamıştır ve kendine has bir mimarisi vardır.

Kimlik Doğrulama bir kavram olarak değişmemiş olsa da , Bunun yapmanın yolu ve bunu sağlayacak hizmetler Active Directory'de Azure'dan çok farklıdır.

Genellikle AAD olarak anılmaktadır. Microsoft'un Active Directory adlı bir ürünü var ve Azure Active Directory ile aynı ürün değildir. Tamamen çok farklı ürünlerdir.



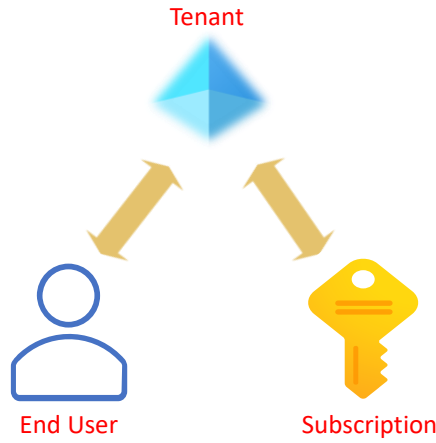
Azure Active Directory (AAD) Service , Azure'daki diğer herşey gibi bir hizmettir. Ancak AAD , Active Directory'den biraz farklıdır. AAD hesabı olmadan Azure hesabınız olamaz. Her Azure hesabının bir ilk kullanıcısı ve sahibi olmalıdır. Azure Active Directory Instance'dan bu kullanıcı olması gerekmektedir. Yani aldığınız ilk şey Yeni bir Azure hesabı oluşturduğunuzda bir AAD hizmetidir.

Örnek vermek gerekirse , Tenant yani kullanıcı kavramıyla başlayalım. Tenant , Kuruluşunuzun Azure ortamındaki bir temsilidir.

Tenant , Azure Active Directory'nin ayrılmış bir örneğidir. Her Azure AD Tenant farklıdır ve Azure AD kiracılarından ayırdır.

Tek bir Kullanıcı , İster Guest ister Member olsun Maksimum 500 kiracıya ait olabilir. Her kullanıcı en az bir kiracının üyesidir. Kullanıcının tek bir kiracının üyesi olması gerekmektedir.

Ve abonelikler , Kullanılan Azure Kaynakları için her ay bir fatura kesilmektedir. Birden fazla aboneliğiniz mevcut ise Tek bir Tenant içerisinde bunu konumlandırabilirsiniz.



Özellikle Hibrid Bulut Mimarisinde AAD'nin bir kaç önemli hususu var. Bu bir çok kuruluş için bir gerçektir. Hibrid Bulut Mimarisinde Organizasyonunuz içerisinde bazı hizmetleriniz mevcut ve Bazıları Azure ortamında barındırılmaktadır. Hibrid Bulut Altyapısı kurmak istediğinizde Azure Active Directory , Hem Organizasyon On-Premise yapınızda hemde Azure Cloud'da Kullanıcılarınızı yönetmenize yardımcı olabilir.



Özetlemek gerekirse ;

Azure'da kullanıcıları ve izinleri yönetmek için AAD ana araçtır.

Öncelikle Active Directory , On-Premise yapıdaki Kullanıcıların , Bilgisayarların , Yazıcıların ve Daha fazlasının yönetim aracıdır. Azure Active Directory ile aynı değildir.

Azure Active Directory hizmeti olmadan bir Azure hesabınız olamaz ve yeni bir Azure hesabında oluşturulan ilk hizmettir.

Tenant , Azure AD'nin ayrılmış bir örneğidir ve organizasyonunuzu temsil eder. Aynı zamanda Azure AD'nin ilk Instance'dır.

Bir Kullanıcı , 500 Tenant kadar Member veya Guest olabilir. Abonelik , Faturalandırma şeklinde devam etmektedir.

Hibrid Yapılarda , Azure Active Directory Organizasyon kullanıcılarını yönetmenize olanak tanımaktadır.

Azure Virtual Networking

Azure Virtual Network , Ortamınızdaki Sanal Makineler , Web Uygulamaları ve Veritabanları gibi kaynaklarınızın birbirleriyle iletişim kurmasını sağlar. Azure Virtual Network , Azure kaynaklarını birbirine bağlayan bir dizi kaynak olarak da tanımlayabiliriz. Genellikle VNet olarak adlandırılmaktadır. Bu kavramın “ **Sanal Ağ** ” olarak anılmasının sebebi ona erişirken donanıma erişiminizin bulunmamasıdır. Tıpkı bir Sanal Makine gibi, kullanımı size ait. Fakat Fiziksel Donanım gizlenmiştir. Yani bir anlama soyutlanmıştır.

Azure Virtual Network, Aşağıdaki Temel Network özelliklerini kullanıcılarına sağlamaktadır:

- ✚ Microsoft Azure Cloud kaynaklarınızın birbirleriyle iletişim kurması
- ✚ Hybrid yapınız mevcut ise On-Premise yapınızın Azure ortamıyla iletişim kurması
- ✚ Ağ Trafikini Yönlendirme , Trafiği Filtreleme işlemleri
- ✚ Virtual Network’leri birbirine bağlama işlemleri
- ✚ İzole ve Segmentasyon İşlemleri

Azure Virtual Network kaynaklarını oluşturmadan önce ayrıca 2 kavramdan bahsetmek isterim:

Adress Spaces ve Subnet Kavramları bu kavramlar Nedir ? Azure Virtual Network içerisindeki rolleri nelerdir ? Bunlardan kısaca bahsedelim:

Adress Spaces : Adres Alanı olarak anılmaktadır. Kullanılabilen IP adresleri aralığıdır. IP Adresi , bir evin sokak adresi gibidir. Yapınızdaki kaynağı benzersiz bir şekilde bulmak için tasarlanmıştır.

Bir Virtual Network kaynağına bağlı olan her hizmet veya kaynak, kendi alanı içindeki İp Adreslerine sahiptir. Aynı VNet üzerindeki hizmetler bu şekilde birbirini bulabilir ve iletişim kurabilir. VNet'e bir adres alanı atarsanız ve her bağlı cihaz, hizmet veya kaynak bu adres alanında atanan bir IP adresini otomatik olarak almaktadır.

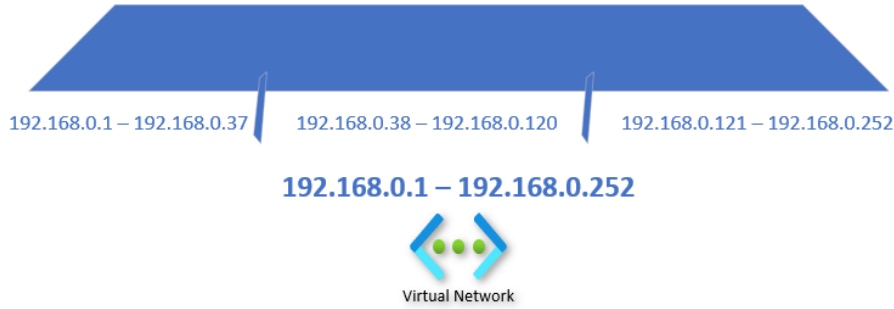


Subnet : Sanal Ağınızı bir veya daha fazla alt ağa bölmenize olanak tanımaktadır. Sanal Ağımızın Address Space yani Adres Alanını bir kısmını her alt ağa tahsis etmekteyiz. Bunu yaparak aynı VNet üzerinde birden çok ağa sahip olabilirsiniz.

Subnet işlemleri Neden bu kadar önemlidir? Buna neden ihtiyaç duyarız?

Hangi hizmetlerin birlikte çalıştığını takip etmeyi kolaylaştırır, Adres tahsisi daha verimlidir.

Ancak tek önemli nedeni: Bir Network Security Group yani Ağ Güvenlik Grubu kullanarak tek tek alt ağları güvence altına alabilmenizdir.



Her Virtual Network tek bir bölgeye aittir. Yani bir VNet üzerindeki hizmetlerin ve kaynakların tümünün fiziksel olarak aynı bölgede olduğunu düşünebilirsiniz. Bölgeler arasında iletişim kurabilmek için VNet'leri birbirine bağlayabilirsiniz.

Her VNet tek bir Subscription'a yani Aboneliğe aittir. Yine de her abonelikte birden fazla Virtual Network olabilir.

Her Azure Kaynağı gibi bu bahsetmiş olduğumuz Kaynakların Avantajları mevcuttur. Bir Virtual Network'ün Ne gibi Avantajları mevcuttur. Bunlardan bahsedelim biraz:

- ✚ Bir düğmeyi tıklayarak bir oluşturduğunuz Sanal Ağı ihtiyaçlarınıza göre ölçeklendirebilirsiniz.
- ✚ Sanal Ağlar, Azure'un temel bir parçası olduğundan ölçeklendirmeden de yararlandığını yukarıdaki maddemizde belirtmiştik. Adres alanınızda aniden oluşan taleplere ihtiyacınız olursa aniden VNet yada bunları hemen karşılayabilirsiniz.
- ✚ Sanal Ağlar, kaynaklarınız için High Availability yani yüksek kullanılabilirlik sağlamaktadır. Bu genellikle Peering Virtual Network aracılığıyla gerçekleşebilmektedir. Bir Load Balancer yani Yük dengeleyici kullanarak veya bir VPN Virtual Gateway yani VPN Ağ Geçidi aracılığıyla 2 VNet'i birbirleriyle haberleştirebilirsiniz.
- ✚ Oluşturduğunuz Sanal Ağlarla, Hizmetleri ve Ortamınızdaki ürünleri çok verimli ve basit bir şekilde izole edebilirsiniz. Alt Ağları ve Ağ Güvenlik Gruplarını kullanarak, kaynaklarınızı bir VNet içinde yönetebilir ve düzenleyebilirsiniz.

Şimdi Yukarıda Bahsetmiş olduğumuz Virtual Network Temel özelliklerini kısaca açıklayalım:




İzolasyon ve Segmentasyon, Azure Ortamınızda bulunan veya oluşturmuş olduğunuz Birden çok izole Sanal Ağ oluşturmanıza Azure olanak tanımaktadır. Yapınızda Virtual Network oluşturma işlemi sağladığınızda Public veya Private IP Adres Aralıklarını kullanarak Private bir IP Adres alanı oluşturabilme imkanına sahipsiniz. Bu IP adres alanını Alt Ağlara bölebilirsiniz. Yapınızda oluşturmuş olduğunuz birden fazla Virtual Network kaynaklarınızı birbiriyle haberleşmeyecek şekilde yalıtılabilme imkanınız mevcuttur.

Hybrid yapınız mevcut ise On-Premise yapınızın Azure ortamıyla iletişim kurması , Azure Ortamınızda bulunan yada oluşturacağınız Azure Kaynaklarının birbirleriyle güvenli bir şekilde iletişim kurabilme imkanına sahipsiniz. Bu işlemleri gerçekleştirebilmenin 2 Yöntem mevcuttur :

Birinci Yöntem olarak , Virtual Network Kaynaklarınız , sadece Sanal Makinelerinizi değil , Aynı zamanda örnek verebileceğim Azure Kaynaklarıyla da Bağlantı sağlayabilmektedir. Bu Kaynaklara Örnek Vermek gerekirse : Azure Kubernetes Servisi , Azure VM Scale Set için Application Hizmet Ortamı , Power Apps.

İkinci Yöntem olarak , Service Endpoint yani Hizmet Uç Noktaları Diğer Azure Kaynakları türlerine bağlanmak için kullanılabilir. Bu kaynaklara Örnek vermek gerekirse : Azure SQL Veritabanları ve Storage Account . Yani bu Yöntem , Yapınızdaki Birden çok Azure kaynağını birbirine bağlamanıza , Kaynaklarınızın Güvenliğini arttırmak ve Kaynaklarınız arasında En uygun olan yönlendirmeyi sağlamak için Sanal Ağlara imkan tanımaktadır.

Ayrıca Azure Virtual Network ile Azure ortamınızda bulunan Kaynaklarınızı Şirket içi yani On-Premise yapıda bulunan kaynaklarla haberleştirebilirsiniz. Azure Aboneliğinize bağlı Hem Local hemde Cloud ortamlarınızı kapsayan bir Network oluşturabilirsiniz. Bu işlemleri sağlayabilmeniz için 3 Yapıyı ortamınızda Devreye almanız gerekmektedir. Bu Yapıları kısaca açıklamak gerekirse:

-  **Point-to-Site Virtual Private Networks** : Bu yapıya Noktadan Site'a Bağlantı denilmektedir. Organizasyonunuzun dışındaki bir bilgisayar ile şirketinizdeki kaynaklarınıza Güvenli ve Şifrelenmiş şekilde bağlantı sağlarsınız.
-  **Site-to-Site Virtual Private Networks** : Bu yapıya Site'den Site'ye Bağlantı denilmektedir. On-Premise yapınızdaki VPN Cihazınızı veya Azure ortamınızdaki Azure Virtual Network Gateway aracılığıyla Azure ortamınızdaki Cihazlarınız On-Premise yapıdaki Network yapısındaymış gibi haberleşme sağlayabilirsiniz. Azure ile On-Premise arasındaki Bağlantı Şifreli ve İnternet üzerinden çalışmaktadır.
-  **Azure Express Route** : Azure ortamınızda Daha Fazla Bandwith'e yani Bant Genişliğine ve daha da yüksek seviyelere ihtiyaç duyduğunuz ortamlar için tam uyumlu olduğunu söyleyebilirim. Azure Express Route ile bağlantınız İnternet üzerinden değil , Özel Bağlantı sağlanmaktadır.

Ağ Trafikini Yönlendirme , Trafik Filtreleme işlemleri , Azure Yapınızdaki herhangi bir Virtual Network'teki , On-Premise ağlarındaki Subnet'ler arasındaki trafiği Azure'a yönlendirebilirsiniz.

Ayrıca Yönlendirmeyi kontrol edebilir ve Bu konfigürasyonlarınızı aşağıda sıralayacağım gibi geçersiz kılabilirsiniz. Bunları açıklamak gerekirse ;

- ✚ **Route Table** , Bir Route Table , Trafik nasıl yönlendirileceği hakkında kurallar tanımlamanıza imkan tanımaktadır. Network Yapınızdaki Paketlerin Subnet'ler arasında nasıl yönlendirildiğini kontrol altına alan Birden çok Özel Route Table oluşturabilirsiniz.
- ✚ **Border Gateway Protocol (BGP)** , Azure VPN Gateway'leriyle veya On-Premise yapınızdaki BGP yollarınızı Azure ortamında bulunan Azure Virtual Network'lerinize yaygınlaştırmak için kullanım sağlayabilirsiniz.

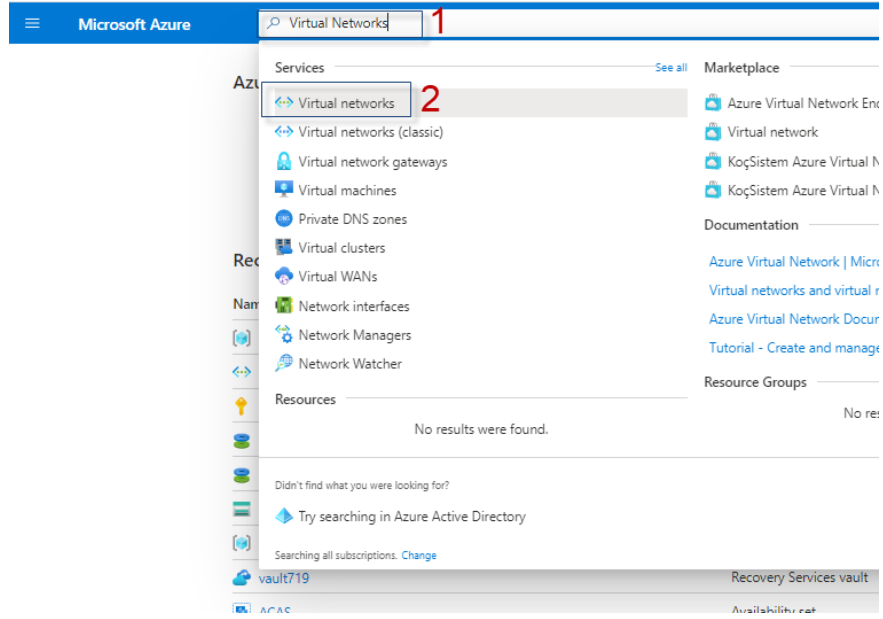
Azure Virtual Network yapınızdaki Subnet'ler arasındaki trafiği aşağıdaki yöntemlerle Filtreleyebilirsiniz. Bunlardan kısaca bahsetmek gerekirse :

- ✚ **Network Security Groups** , Yani Ağ Güvenlik Grupları olarak anılmaktadır. Bir Network Security Group yapınızda bulunan birden çok gelen ve giden Güvenlik kurallarına göre kaynaklarınız arasında , Dışarıdan veya İçeride trafiğe izin vermek , Trafik engellemek için Source (Kaynak) , Destination IP (Hedef IP) , Bağlantı Noktaları , Protokol faktörlerine göre kurallar tanımlayabilirsiniz.
- ✚ **Network Virtual Appliances**, Yani Ağ Sanal Cihazları olarak Anılmaktadır. Bir Network Virtual Appliances , Özel bir Sanal Makinedir.Bu Özel Sanal Makine Belirli bir Network işlevlerini yerine getirmektedir. Bu işlevlere örnek vermek gerekirse : Firewall Devreye alma veya WAN optimizasyonu gerçekleştirme gibi örnekleyebiliriz.

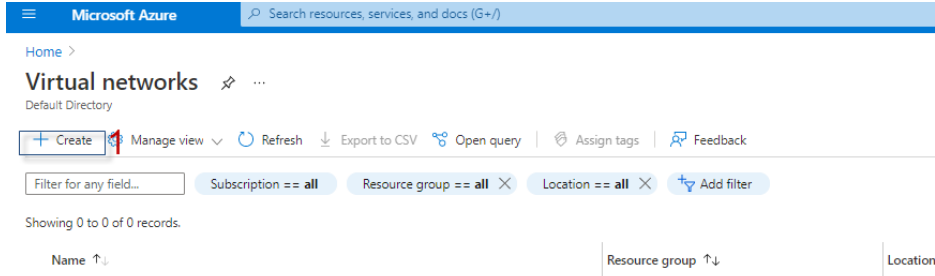
Virtual Network'leri birbirine bağlama işlemleri , İleride bahsedeceğimiz Virtual Network Peering hizmetini kullanarak , Virtual Network'leri birbirine bağlayabilirsiniz. Peering yani Eşleme sayesinde , Her birinde Kaynaklarınızı etkinleştirir ve Birbirleriyle iletişim kurmasını sağlayabilmektedir. Bu Virtual Network'ler Aynı Region'larda bölgelerde olması farketmeksizin birbirleriyle haberleşebilir duruma gelmektedir.

Virtual Network Kaynağı oluşturması sağlayabilirsiniz. Onunla alakalı adım adım uygulama gerçekleştiriyor olacağız :

İlk olarak Azure Ortamına Yeni bir Virtual Network oluşturmak için Azure Ortamınıza giriş yaptıktan sonra Azure arama çubuğuna “ **Virtual Networks** ” yazarız. Virtual Network oluşturma işlemlerine başlamak için seçeneği seçerek devam ederiz.



Virtual Network oluşturma ekranına gitmek için **“ Create ”** seçeneğini seçeriz yada aşağıda **“ Create Virtual Networks ”** seçeneğini seçeriz.



No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your on-premises network using an Azure VPN Gateway or ExpressRoute.

2

[Create virtual network](#)
[Learn more](#)

Bir Virtual Network yapılandırma işlemi için aşağıdaki adımları uygulayarak , işlem sağlayabilirsiniz :
 Subscription Konfigürasyonları , Oluşturacağınız Virtual Network konfigürasyonları , IP Adres konfigürasyonları , Güvenlik Konfigürasyonları , Etiketleme Konfigürasyonlarını sağlayarak Virtual Network oluşturma işlemi sağlamış olursunuz.

Create virtual network ...

Basics IP Addresses Security Tags Review + create

1 2 3 4 5

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

[Review + create](#) [< Previous](#) [Next : IP Addresses >](#) [Download a template for automation](#)

“ Project Details ” bölümünde Azure ortamınızda bulunan Subscription’lardan istediğiniz **“ Subscription ”** seçerek devam ederiz. Ardından Azure ortamınızda herhangi bir Resource Group oluşturmadıysanız , **“ Resource Group ”** tanımlı checkbox’un altındaki **“ Create New ”** seçeneğini seçerek , Resource Group oluşturma işlemleri gerçekleştirebilirsiniz.

“ Instance Details ” bölümünde **“ Name ”** kutucuğuna Virtual Network kaynağınıza Bulunduğunuz Subscription’da Benzersiz bir ad olarak tanımlanması önem arz etmektedir. Adı seçerken , Hatırlaması kolay ve Yapınızda diğer oluşturmuş olduğunuz Virtual Network’lerden rahatlıkla ayırt edilebilecek , Açıklayıcı olacak şekilde belirlemeniz yararınıza olacaktır. **“ Region ”** konfigürasyonlarında oluşturacağınız Virtual Network hangi Azure Region’da bulunmasını isterseniz ilgili region seçeneği seçerek **“ Next : IP Addresses ”** seçeneğini seçerek devam ederiz.

Create virtual network ...

Basics IP Addresses Security Tags Review + create

1 2 3 4 5

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

[Review + create](#) [< Previous](#) [Next : IP Addresses >](#) [Download a template for automation](#)

“ **Address Space** ” bölümünde oluşturacağınız Virtual Network üzerinde adres alanı tanımlarsınız , Bu belirleyeceğimiz Adress Spaces , Aboneliğiniz içinde ve Bağlantı sağladığınız Diğer Ağlardan benzersiz olmalıdır. Azure yapımız için bize önerilen şuan varsayılan olarak gelen Adres Alanı , “ **10.0.0.0/16** ’lık “ Adres Alanını seçeriz. Bu adres alanında Tanımlanan adresler , “ **10.0.0.0 ile 10.0.255.255** ” arasında tanımlanmış olmaktadır. İkinci bir Adres Alanı oluşturmak isterseniz. Altteki kutucuğa istemiş olduğunuz IP Adres Alanını yazarak , ikinci bir Adres Alanı tanımlayabilirsiniz. Burada dikkat etmeniz gereken nokta , Birinci olarak belirlemiş olduğunuz IP Adres Alanı ile İkinci Adres alanında belirlemiş olduğunuz IP Adres alanı çakışacak şekilde belirlenmemelidir. (Adres Alanı oluşturma işleminde 10.0.0.0 /24 şeklinde yazmalısınız. Kullanacağınız IP Aralığını sağında görebilirsiniz.)

Oluşturmuş olduğumuz IP Adress Spaces IPv4 kategorisindedir. Fakat yapınızda “ **IPv6** ” kategorisine uygun cihazlarınız mevcutsa yada IPv6 yapısında bir Adres Alanı oluşturmak isterseniz , “ **Add IPv6 address space** ” seçeneğinin yanındaki kutucuğu işaretlemeniz gerekmektedir.

“ **Add Subnet** ” seçeneğini seçerek , oluşturacağınız Virtual Network Adres aralığında bölümlleme yapan bir veya birden çok Subnet oluşturabilirsiniz. Subnet’ler arasında yönlendirme , Varsayılan Trafiğe bağlı olacağını vurgulamak isterim. Subnet konfigürasyonlarımızı Default olarak önerilen konfigürasyonlara göre gerçekleştirerek devam ederiz. “ **Next : Security >** ” seçeneğini seçerek devam ederiz.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual network >

Create virtual network ...

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

☐ Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

Subnet name	Subnet address range	NAT gateway
default	10.0.0.0/24	-

Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

Review + create < Previous Next : Security > Download a template for automation

“ **Next : Security >** ” seçeneğini seçtikten sonra “ **BastionHost , DdoS Protection Standart , Firewall** ” konfigürasyonlarını istediğinize ve yapınıza göre konfigüre edebilirsiniz. Buradaki Default konfigürasyonları ile devam edeceğim. **Fakat ilk öncelik bu kavramları kısaca açıklamak isterim :**

BastionHost , Virtual Network içinde sağladığınız tamamen platform tarafından yönetilen yeni bir “ **Platform as a Service (PaaS)** ” hizmetidir. SSL (Secure Socket Layers) üzerinden direk Azure Portalı üzerinden Güvenli ve Sorunsuz şekilde SSH veya RDP bağlantılarını gerçekleştirebilirsiniz. Azure Bastion aracılığıyla bir Sanal Makineye bağlandığınızda , Ortamınızdaki Sanal Makinelerinizin Public IP Adresine ihtiyacı bulunmadığının bilgisini vermek isterim. Etkinleştirmek için “ **Enable** ” seçeneğinin yanındaki seçeneği işaretleyerek konfigürasyonları sağlayarak ortamınızda aktifleştirebilirsiniz. “ **Disable** ” seçeneği ile bu özelliği devredışı bırakabilirsiniz.

DdoS Protection Standart , DdoS Koruma Planı olarak anılmaktadır. Bu Virtual Network kaynağınızda tüm korunan kaynaklar için bir DdoS saldırısının etkilerine karşı koruma sağlamak için Saldırı Bildirimi ve Telemetri aracılığıyla Azure ortamınızdaki kaynaklarınız için Advanced DdoS azaltma sağlayan Ücretli bir hizmettir. Temel DdoS koruması , varsayılan olarak ve hiç bir ek ücret ödmeden Azure platformuna entegre edildiğini vurgulamak isterim. Etkinleştirmek için “ **Enable** ” seçeneğinin yanındaki seçeneği işaretleyerek konfigürasyonları sağlayarak ortamınızda aktifleştirebilirsiniz. “ **Disable** ” seçeneği ile bu özelliği devredışı bırakabilirsiniz.

Firewall , Azure ortamında hizmet vermektedir. On-Premise yapılarda bulunan Fiziksel Firewall cihazlarından herhangi bir farkı bulunmamaktadır. Firewall Konfigürasyonu “ **Enable** ” yanındaki kutucuğu işaretleyerek , Aktifleştirme sağladığınızda Azure ortamınız için Firewall oluşturabilirsiniz. Azure Virtual Network’e bağlı Kaynaklarınızı koruyan , Yönetilen bir Cloud tabanlı Ağ Güvenlik hizmetidir. “ **Disable** ” seçeneği ile bu özelliği devredışı bırakabilirsiniz.

Ardından konfigürasyonlar gerçekleştirdiğinizde “ **Next : Tags >** ” seçeneğini seçerek bir sonraki etiketleme adımına geçebilirsiniz.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The 'Security' tab is selected, and the 'BastionHost', 'DDoS Protection Standard', and 'Firewall' options are all set to 'Disable'. The 'Next : Tags >' button is highlighted with a red box and a red number 4.

“ **Tags** ” bölümde oluşturacağınız Virtual Network kaynağının daha kolay bulunabilmesi için etiketleme standardı belirleyerek , oluşturma işlemlerini gerçekleştirebilirsiniz. Kaynak oluşturma işlemlerinin kontrol edilebilmesi ve oluşturma işlemlerinin sürecini başlatabilmek için “ **Next : Review + create >** ” seçeneğini seçerek devam ederiz.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal, specifically the 'Tags' tab. The breadcrumb navigation is 'Home > Virtual network >'. The tabs are 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Tags' tab is active, showing a description: 'Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags'. Below this is a note: 'Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.' There are two input fields: 'Name' (labeled with a red '2') and 'Value' (labeled with a red '3'). At the bottom, there are three buttons: 'Review + create', '< Previous', and 'Next : Review + create >' (labeled with a red '4'). To the right of the 'Next' button is a link: 'Download a template for automation'.

Yaptığımız konfigürasyonlarda herhangi bir hata olmadığını ve Kaynağı oluşturma işlemlerinde herhangi bir engel olmadığını “ **Validation passed** ” uyarısı olarak anlamış oluruz. Ardından kaynak oluşturma işlemlerine başlamak için “ **Create** ” seçeneğini seçeriz.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal, specifically the 'Review + create' tab. The breadcrumb navigation is 'Home > Virtual networks >'. The tabs are 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Review + create' tab is active, showing a green checkmark and the text 'Validation passed'. Below this is a table with the following details:

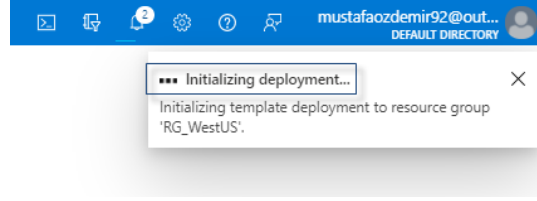
Basics	
Subscription	Visual Studio Enterprise Subscription
Resource group	RG_WestUS
Name	Ozdemir_Vnet
Region	West US

IP addresses	
Address space	10.0.0.0/16
Subnet	default (10.0.0.0/24)

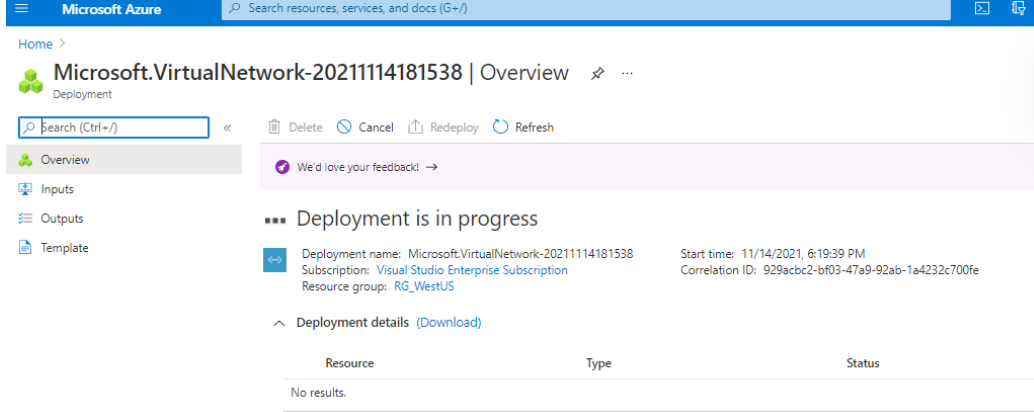
Tags	
Tags	None

At the bottom, there are three buttons: 'Create' (labeled with a red '2'), '< Previous', and 'Next >'. To the right of the 'Next' button is a link: 'Download a template for automation'.

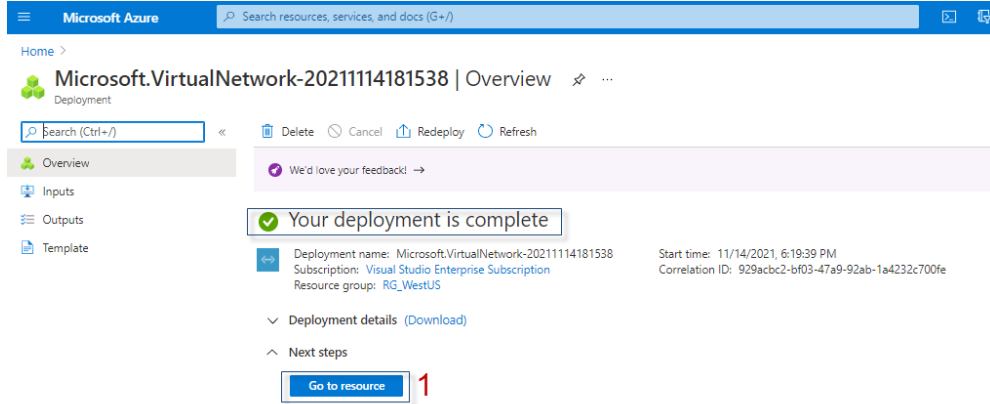
Oluşturma işlemleri başladı.



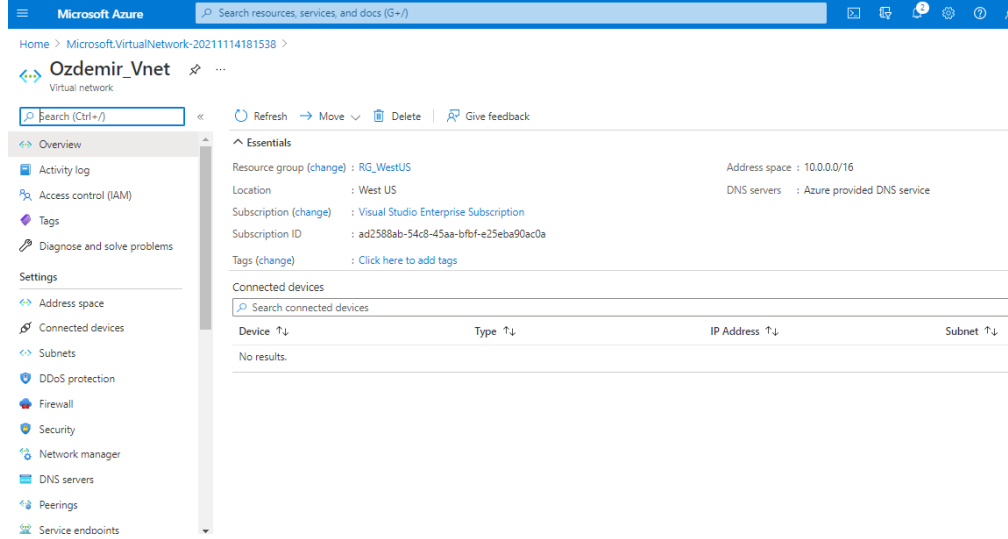
Virtual Network oluşturma işlemleri devam etmektedir.



Virtual Network kaynağımızın oluşturma işlemi tamamlanmıştır. Oluşturmuş olduğumuz Virtual Network kaynağına ve konfigürasyonlarına erişmek için “Go to resource” seçeneğini seçeriz.



Oluşturmuş olduğumuz Virtual Network kaynağımızın konfigürasyon ekranımıza problemsiz eriştiğimizi gördük ve Virtual Network kaynağımıza bağlı herhangi bir Azure ortamında oluşturmuş olduğumuz yada olan bir cihazımızın bulunmadığını görmüş oluruz. Bağlı cihazımız için Hizmet veya Kaynağı oluşturma esnasında Virtual Network konfigürasyonlarında “ **Ozdemir_Vnet** ” adındaki Virtual Network kaynağını seçerek , Bu Virtual Network kaynağına bağlayabilme imkanına sahip olabiliriz.



Virtual Network Kaynağı oluşturma işlemimiz tamamlanmıştır.

Microsoft Azure Storage

Storage Account yani Depolama hesabı olarak geçmektedir. Storage Account, Verileriniz için benzersiz bir azure ad alanı olarak tanımlayabiliriz. Bu sakladığınız her nesnenin Azure Depolamada yani Stroage'da bir web adresi mevcuttur. Bu web adresi Benzersiz Storage Account adınızı içermektedir. Depolama hesabınıza verdiğiniz ad, Ana web adresi olmaktadır.

Storage Account ve Unique Azure Namespaces birbiriyle bütünleşik bir kavram olduğunun bilgisini vermek isterim.

Depolama Hesabı = Benzersiz Azure Ad Alanı açıklayabiliriz.

Daha iyi anlayabilmek adına ;

Yapımızda oluşturacağımız yada oluşturacağımız Stogare Account’umuz örnek olarak Özdemir olsaydı , Depolama ad Alanı veya adresi aşağıda gösterildiği gibi o formatta olurdu. Bu Aynı zamanda Depolama Hesabınızın adı anlamına gelmektedir. Azure ortamında benzersiz olması gerekmektedir. Aksine bu durum problem yaratabilir.

ozdemir.<storage type>.core.windows.net

Storage Account yani Depolama Hesabı, Tüm Azure Depolama türlerinin temeli olarak tanımlanabilmektedir. Azure Storage servisini organizasyonunuzda kullanabilmeniz için önce veri objelerinizi depolama işlemi gerçekleştirebilmeniz için Azure Storage Account oluşturmanız

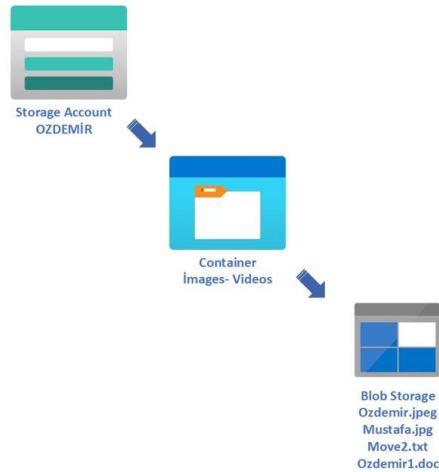
gerekmektedir. Azure Portal , Azure Powershell veya Azure CLI arayüzlerinden Azure Storage Account oluşturma işlemlerinizi gerçekleştirebilirsiniz.

Şimdi bunlar ilk olarak bilgi olarak aklımızda kalsın. Bunun yanında Azure Storage Account oluşturma işlemi sağladıktan sonra Blob Storage oluşturma işlemi sağlayacağız. Onun için detaylı olarak Blob Storage mimarisinden , Nerelerde kullanılmaktadır daha detaylı olarak aşağıda bahsediyor olacağız. **O halde hemen başlayalım :**

Blob kavramının açılımı **Binary Large Object** olarak diyebiliriz. Peki Blob Ne anlama gelmektedir. Bunu açıklayalım. **Blob** , Günümüzde kullanılan en yaygın terimlerden biridir. " **İkili Büyük Nesne** " olarak geçmektedir. Diğer bir açıklama yapmak gerekirse ; Blob kavramını , Bit ve Byte'lardan oluşan hemen hemen herşey olarak tanımlayabiliriz. Yani bir anlama Blob , Veri Bloğu olarak da anılabilmektedir. Bu Veri Blokları Storage Account yani Depolama hesabının içindeki Container'larda muhafaza edilmektedir. Buradan Blob Storage mimarisinin üç katman olduğunu çıkarabiliriz. Storage Account , Container ve Blob üçlüsü .

Azure Yapınızdaki Azure Storage Account'unuzda birden çok Blob Container olabilmektedir. Bunların içeriğinde verilerinizi depolayabilirsiniz. Örnek vermek gerekirse ; Bir kutu , Container bir Blob Container olsun , Kutunun içeriğinde her ne olursa olsun, Dışarıdan istediğim verileri bu Blob ögesinin içine koyabiliyorum. Hangi türde bir veri oldukları yada Hangi boyutta bir veri olduklarının bir önemi yok. Bu Blobların veya öğelerin her birinin benzersiz bir adresi olacağını yukarıda söylemiştim. Örnek olarak kutumuzun içeriğindeki herhangi bir veriyi almak istiyorum : Kutunun içeriğindeki verilerimizi doğrudan ve hızlı bir şekilde sorunsuz bir şekilde alabiliriz. Yani burada dikkat etmemiz gereken nokta bu verilerimizin Tam olarak nerede olduklarını görebilir, bulabilir ve bilebiliriz. Yani Şöyle Blob Container düşünün , Karışık bir Sepet olarak hepsi Logic halde yani Mantıklı bir şekilde baştan aşağı tag'lenmiş halde yani etiketlenmiş diyebiliriz.

Blob Storage , çok yönlü kullanılcı olacak şekilde tasarlanmıştır.



Peki Nerelerde Kullanabiliriz ?

- + Her çeşit dosyayı muhafaza edebilir ve Distributed yani Dağıtılmış erişim sağlayabilirsiniz.
- + Video ve Ses Akışı
- + Ortamınızdaki Log istediğiniz ortamları için Günlük Dosyalara Yazma işlemleri
- + Yedekleme ve Geri yükleme gibi işlemler ve Felaketten kurtarma , verilerin arşivlenmesi.
- + İmage'lar genellikle çeşitli farklı boyut ve biçimdedirler ve Blob Storage, Bunları doğrudan bir Browser'a depolamayı sağlamaktadır.

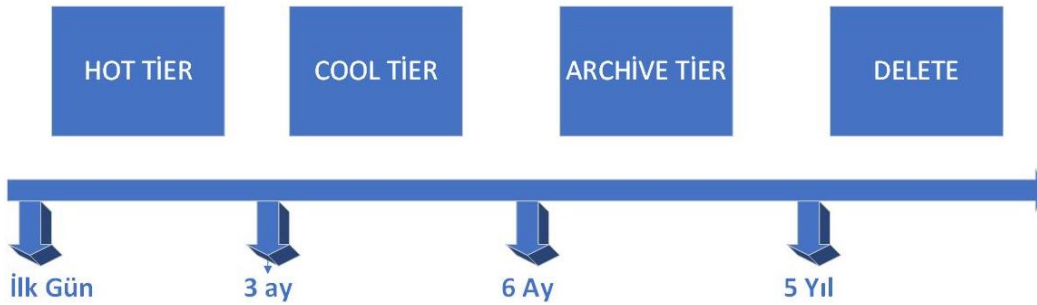
Azure Storage , üç çeşit Blobu desteklemektedir :

- + Block Blob
- + Append Blob
- + Page Blob

Bunları açıklamak gerekirse ;

- + **Block** , Blokları ve ikili verileri yaklaşık 4,7 TB'a kadar depolamayı desteklemektedir. Block Blob'ları , Veri bloklarından oluşmaktadır. Bireysel olarak yönetilebilmektedir.
- + **Append (Ekleme) Blob'ları** , Block blobları gibi bloklardan oluşur. Ancak ekleme işlemleri için optimize edilmiştir. Append Blob , sanal makinelerden veri kaydetme gibi senaryolar için gerçekten çok iyi çalıştığını söyleyebilirim.
- + **Page (Sayfa) Blob'ları** , 8 TB'a kadar Rastgele erişim dosyalarını depolamayı desteklemektedir. Dosyanın herhangi bir bölümünün herhangi bir zamanda erişilebilir durumda olduğunu vurgulamak isterim. Bu Page Blob'ları sanal bir sabit sürücüye depolanabilmektedir. Örnek verirsek; bir VHD dosyasına. Azure ortamındaki Sanal Makine için disk olarak hizmet verebilme imkanına sahipsiniz.

Blob Storage için 3 Adet Maliyetlendirme söz konusu bunları sıralayarak , açıklamak gerekirse ;



Ortamınızda Sık Sık eriştiğiniz Dosyalar mevcutsa **Hot Tier** tam size göre. Bu Katman Daha düşük erişim sürelerine ve daha yüksek erişim maliyetlerine sahiptir.

Ortamınızda Daha düşük depolama maliyeti istiyorsanız **Cool Tier** tam size göre . Bu katman Hot Tier'e göre kıyaslandığında High Availability yani Yüksek Erişilebilirlik sunmaktadır. Bu katman genellikle 30 Gün boyunca kalıcı verileriniz için tasarlanmıştır.

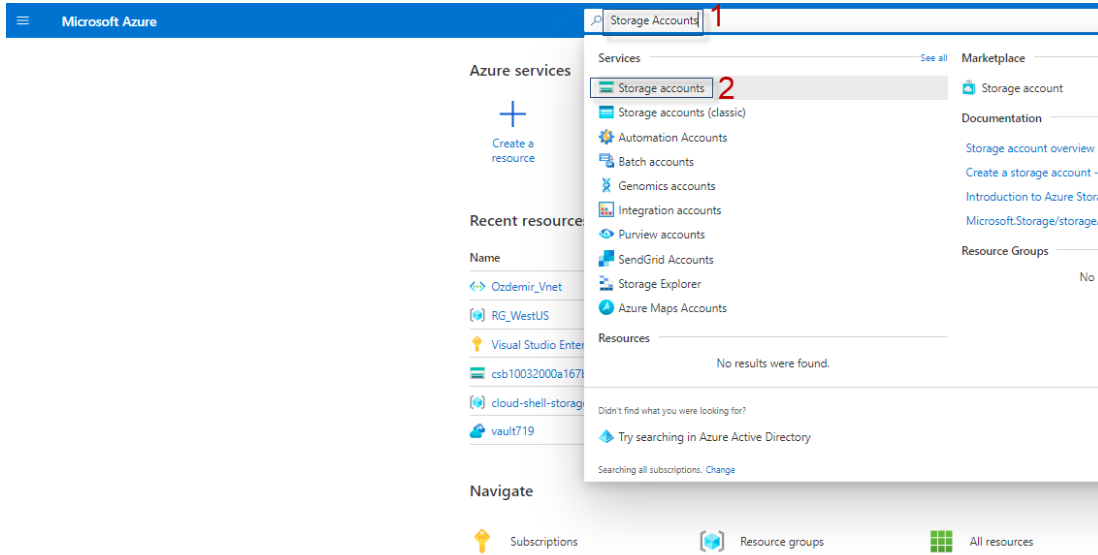
En düşük maliyete ve en yüksek erişim sürelerine sahip **Archive Tier**. Kalıcı ve arşivlemeniz gereken dosyaları bu katmana alabilirsiniz.

Şimdi bu anlattıklarımızı Azure Portal üzerinden adım adım uygulayalım. Yapacağımız işlemleri ilk öncelik sıralamak istiyorum :

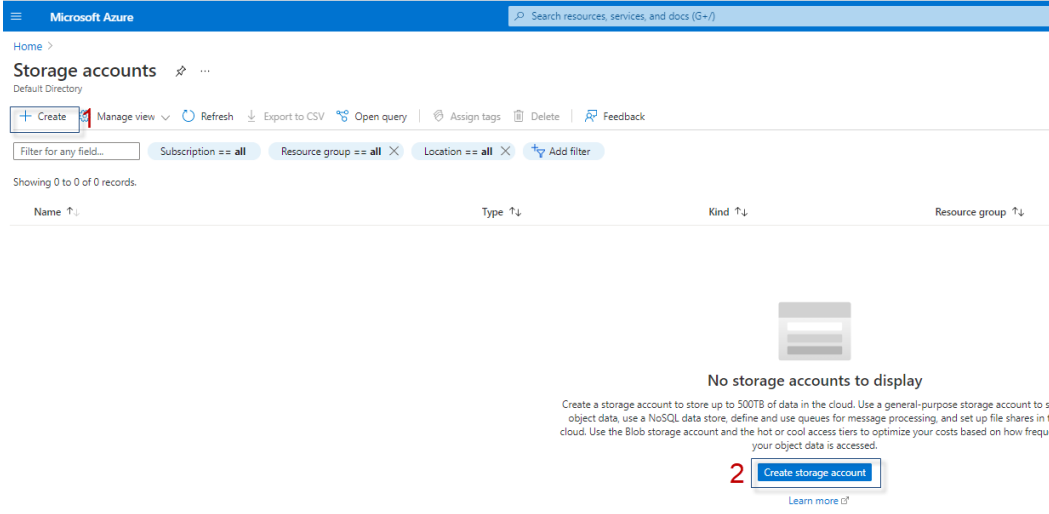
- ✚ Yukarıda belirtildiği gibi Azure Blob Hizmetini kullanabilmek için Bir Azure Storage Account oluşturacağız.
- ✚ Storage Account'umuzun Blob Servisi içinde images block container'ı oluşturacağız. Ardından bu İmage'leri adlandırıyor olacağız.
- ✚ Blob yükleme işlemi gerçekleştireceğiz.

O halde Başlayalım:

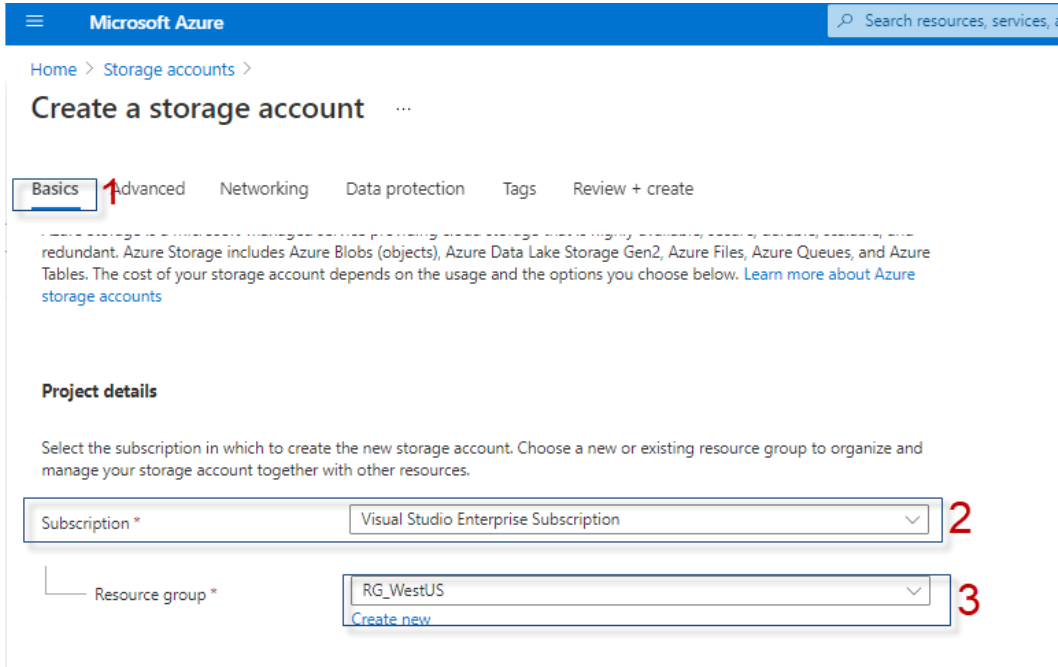
İlk olarak Azure Portalına gireriz . Sonrasında Storage Account ile alakalı konfigürasyonları sağlarız. İlk olarak arama çubuğumuza " **Storage Accounts** " kaynağını yazarız. Hizmetler kısmından ilgili seçeneği seçeriz.



Storage Account oluşturma işlemi için " **Create** " seçeneğini yada aşağıdaki " **Create storage account** " seçeneğini seçeriz.



" **Basics** " adımında Azure ortamımızda bulunan " **Subscription**'umuzu " seçeriz. Ardından oluşturacağımız Storage Account'umuzun hangi " **Region** " olacağını seçeriz. Ortamınızda Resource Group mevcut değilse Checkbox altındaki " **Create New** " seçeneğini seçeriz.



" **Storage Account Name** " kutucuğuna Storage Account oluşturma işlemlerinde problem çıkmaması adına benzersiz bir isimlendirme sağlamanız gerekmektedir. Bu isimlendirme 3 ile 24 karakter uzunluğunda ve sadece Küçük harf ve rakamlarla oluşturulmalıdır. Yapınıza göre veya isteğinize göre isimlendirme sağlayabilirsiniz. Ben " **ozdemir** " ismini vereceğim.

" **Region** " bölümünde ise Storage Account'umuzun hangi bölgede olmasını istersek onu seçeriz. Yapınıza ve isteğinize göre Region konfigürasyonu sağlayabilirsiniz. Region'lardaki seçiminiz " **Redundancy** " seçeneklerinin daha da çeşitlenmesine sebep olabilmektedir. " **LRS (Locally Redundant Storage)** , **GRS (Geo-redundant Storage)** dışında , **ZRS (Zone Redundant Storage)** , **GZRS (Geo-zone-redundant Storage)** " gibi yapılarda seçilebilir hale gelmektedir.

" **Performance** " bölümünde ise " **Standart** " seçeneğinin yanındaki kutucuğu işaretleriz. Yani Standart Genel Amaçlı v2 Storage Account şeklinde seçerek ilerleriz. Bu seçenekleri seçerek , Storage Account Block Blob'ları , Dosya Paylaşımları veya Page Blob'ları için üstün performansa sahip olmak isteyip istemediğimizi belirleriz.

" **Redundancy** " bölümünde ise " **Locally -redundant storage (LRS)** " seçeneğini seçeriz. Yani Yerel olarak Yedekli Depolama anlamına gelmektedir.

" **Next : Advanced >** " seçeneğini seçerek " **Advanced** " aşamasına geçeriz.

" **Storage Account Name** " kutucuğuna Storage Account oluşturma işlemlerinde problem çıkmaması adına benzersiz bir isimlendirme sağlamanız gerekmektedir. Bu isimlendirme 3 ile 24 karakter uzunluğunda ve Sadece Küçük harf ve rakamlarla oluşturulmalıdır. Yapınıza göre veya isteğinize göre isimlendirme sağlayabilirsiniz. Ben " **ozdemir** " ismini vereceğim.

" **Region** " bölümünde ise Storage Account'umuzun hangi bölgede olmasını istersek onu seçeriz. Yapınıza ve isteğinize göre Region konfigürasyonu sağlayabilirsiniz. Region'lardaki seçiminiz " **Redundancy** " seçeneklerinin daha da çeşitlenmesine sebep olabilmektedir. " **LRS (Locally Redundant Storage)** , **GRS (Geo-redundant Storage)** dışında , **ZRS (Zone Redundant Storage)** , **GZRS (Geo-zone-redundant Storage)** " gibi yapılarda seçilebilir hale gelmektedir.

" **Performance** " bölümünde ise " **Standart** " seçeneğinin yanındaki kutucuğu işaretleriz. Yani Standart Genel Amaçlı v2 Storage Account şeklinde seçerek ilerleriz. Bu seçenekleri seçerek , Storage Account Block Blob'ları , Dosya Paylaşımları veya Page Blob'ları için üstün performansa sahip olmak isteyip istemediğimizi belirleriz.

" **Redundancy** " bölümünde ise " **Locally -redundant storage (LRS)** " seçeneğini seçeriz. Yani Yerel olarak Yedekli Depolama anlamına gelmektedir.

" **Next : Advanced >** " seçeneğini seçerek " **Advanced** " aşamasına geçeriz.

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ * 1

Region ⓘ * 2

Performance ⓘ * 3 ☒ Standard: Recommended for most scenarios (general-purpose v2 account)
☐ Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ * 4

[Review + create](#) [< Previous](#) [Next : Advanced >](#) 5

" **Advanced** " adımımda ise ilk olarak " **Security** " bölümündeki konfigürasyonları kısaca açıklıyor olacağız.

" **Require secure transfer for REST API operations** " seçeneği Güvenlik Aktarım seçeneği olarak geçmektedir. Bu seçeneği aktifleştirme işlemi sağladığınızda HTTP'leri kullanan Storage Account sadece REST API işlemlerine izin vererek Storage Account'uzun güvenliğini arttırabilirsiniz. Bu konfigürasyonu etkinleştirdiğinizde , HTTP isteklerinin hepsi reddedilecektir. Şunu hatırlatmak isterim : Azure Storage , Size Özel Domain isimleri için HTTP'leri desteklemediğinden , özel bir Domain isimleri kullanırken bu seçenek işaretli olsa dahi uygulanmaz. Son olarak TCP Protokolü üzerinden yapınızdaki Blob'larınız için NFSv3 (Network File System Version 3) aracılığıyla yapılan bağlantılar problemsiz gerçekleşir. Fakat yapınız için Pek Güvenli olmadığının bilgisini vermek isterim.

" **Enable infrastructure encryption** " seçeneği ise Altyapı Şifrelemesi olarak geçmektedir. Yapınızdaki Storage Account'unuzun verilerine alternatif bir Şifreleme katmanı dahil etmektedir. Fakat Microsoft Azure , Default olarak Storage Account verilerini şifreleme işlemlerini sağlamaktadır.

" **Enable blob public access** " seçeneğinde ise oluşturacağınız yada oluşturduğunuz Blob'u Public Erişime açmaktadır. İlgili özelliği yapınızda etkinleştirme işlemi sağladığınızda , yapınızdaki Storage Account içindeki blob'lara Everyone erişime izin vermek için Container'ların Access Control List'lerin yapılandırılmasına izin verilmektedir. Devredışı bırakıldığında , Temel Access Control List yapılandırmalarından bağımsız olarak , Storage Account içindeki Blob'larınıza everyone erişim izini geçersiz olmaktadır.

" **Enable Storage account key access** " seçeneğinde ise oluşturacağınız veya oluşturduğunuz Storage Account için Key erişimi Devredışı bırakıldığında , Shared Access Signatures (SAS) yani Paylaşılan Erişim imzaları dahil olmak üzere, Shared Key ile Yetkilendirilen Account'lara gelen tüm istekler reddedilmektedir. Etkinleştirme gerçekleştirdiğinizde , Shared Key kullanarak Storage Account'a erişim sağlayan Client'ınız Uygulamaları çalışamaz hale geldiğini hatırlatmak isterim. Bu seçeneği Default halde bırakarak ilerleriz.

" **Default to Azure Active Directory authorization in the Azure Portal** " seçeneğinde ise etkinleştirme sağladığınızda Azure Portalınızda Default olarak Azure Active Directory ile Blob'lara , Kuyruklara ve Tablolara yönelik isteklerin yetkilendirilmesi sağlanmaktadır.

" **Minumum TLS version** " seçeneğinde ise Storage Account'unuza ait verileri kullanan Uygulamalarınız için gereken Minumum TLS sürümünü konfigüre edebilirsiniz. Seçeneklerde , " **Version 1.0 , Version 1.1 ve Version 1.2** " bulunmaktadır. Ortamınızdaki güvenliği ve Uygulamanızın uyumluluğu açısından TLS 1.2 şeklinde konfigürasyon sağlamak yararınıza olacaktır.

Microsoft Azure

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking Data protection Tags Review + create

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ☒ 2

Enable infrastructure encryption ☐ 3

Enable blob public access ☒ 4

Enable storage account key access ☒ 5

Default to Azure Active Directory authorization in the Azure portal ☐ 6

Minimum TLS version 7 Version 1.2

" **Advanced** " adımındaki konfigürasyonlara devam ediyoruz.

" **Data Lake Storage Gen2** " Hiyerarşik Ad Alanı olarak anılmaktadır. Büyük Veri Analizi yöntemiyle kullanılan iş yüklerinize büyük ölçüde ivme kazandırmakta ve Dosya Seviyesinde tanımlamış olduğunuz ACL'leri etkinleştirmektedir.

" **Secure File Transfer Protocol**) " Güvenli Dosya Transferi Protokolü olarak anılmaktadır. Organizasyonunuzdaki kullanıcılarınızın bu SFTP aracılığıyla Blob'lara erişmesine imkan sağlamış olursunuz , oluşturduğunuz yada oluşturacağınız Storage Account'unuz için SFTP Protokolünü devreye almaktadır. Ortamınızda STFP erişimleri için yapınızda Local User'ları oluşturulması gerekmektedir. " **Enable SFTP** " seçeneğinin konfigüre edilemediğini görürüz. Bunun nedeni Hiyerarşik ad alanı Account'larımız için Subscription seviyesinde etkinleştirme sağlamadığımız için konfigüre edilememektedir.

" **Blob Storage** " bölümünde ise " **Enable network file system v3** " seçeneğinde konfigüre edilemediğini görürüz. Bunun nedeni ilk önce ortamınızda Hiyerarşik Ad Alanı etkinleştirilmemesinden kaynaklıdır. Etkinleştirme sonrası , konfigürasyon ve etkinleştirme işlemlerini gerçekleştirebilirsiniz.

" **Allow cross-tenant replication** " seçeneğinde ise Nesne Replikasyonunu farklı Azure Active Directory Tenant'ındaki oluşturduğunuz yada oluşturacağınız User Account'a replike edilmesini sağlayabilirsiniz.

Tenant'ler arası Replikasyonu devredışı bırakmak ise , Yapınızdaki aynı Azure AD Tenant içerisinde bulunan nesnelerin replikasyonuna sınır koymaktadır.

" **Access Tier** " Hesap Erişim Katmanı olarak anılmaktadır. Bu seçenektekiler ise yukarıda açıkladığım gibi " **Hot** " ve " **Cool** " gibi senaryolar mevcuttur. **Bunlardan tekrardan bahsetmek gerekirse ;**

Sık Sık eriştiğiniz Dosyalar için **Hot Tier** , Bu Katman , Daha düşük erişim sürelerine ve daha yüksek erişim maliyetlerine sahiptir.

Daha düşük depolama Maliyetine sahiplik için **Cool Tier**, Bu Katman Hot Tier'e göre kıyaslandığında Yüksek Erişilebilirlik sunmaktadır. Bu katman genellikle 30 Gün boyunca Kalıcı Verileriniz için tasarlanmıştır.

Bunları kıyaslarsak , Hot Katmanı , Sık erişilen veriler için idealdir . Cool Katmanı ise , Seyrek erişilen veriler için idealdir.

Bunlardan üçüncü olarak Archive Katmanıda mevcut . Fakat bu erişim katmanı , Account seviyesinde değil , Sadece Blob seviyesinde Konfigüre edilebilmektedir.

" **Hot** " olarak konfigüre ederek , işlemlerimize devam ederiz. (Yapınıza göre ve ihtiyacınıza göre konfigürasyon sağlamak yararınıza olacaktır.)

" **Azure Files** " bölümünde ise Maksimum 100TiB'a kadar dosya paylaşımını desteklenmektedir. Konu açılmışken şunu da belirtmek istiyorum : Büyük Dosya Paylaşımlı Storage Account'lar Coğrafi olarak yedekli Depolama yapılarına dönüştürülememektedir.

" **Table and queues** " bölümünde ise etkinleştirme işlemi sağladığınızda Yapınızdaki SQL Veritabanınızdaki Dosyaları yani Tabloları ve Kuyrukları güvenlik amacıyla şifreleme işlemi sağlamaktadır. Etkinleştirme işlemi sağlandıktan sonra Storage Account oluşturma işlemi tamamlandıktan sonra konfigürasyon değiştirilemediğinin bilgisini vermek isterim. Konfigüre işlemi sağlamanız esnasında değiştirilememe durumunu göz önünde bulundurmalısınız.

Bir sonraki " **Networking** " adımına geçmek için " **Next : Networking >** " seçeneğini seçerek devam ederiz.

Microsoft Azure

Home >

Create a storage account ...

Basics **Advanced** 1 Networking Data protection Tags Review + create

Data Lake Storage Gen2 2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). [Learn more](#)

Enable hierarchical namespace ☐

Secure File Transfer Protocol (SFTP) 3

Enables the Secure File Transfer Protocol for your storage account that allows users to access blobs via an SFTP endpoint. Local users need to be created before the SFTP endpoint can be accessed. [Learn more](#)

Enable SFTP ⓘ ☐

Blob storage 4

Enable network file system v3 ⓘ ☐

Allow cross-tenant replication ⓘ 5 ☒

Access tier ⓘ 6

☒ Hot: Frequently accessed data and day-to-day usage scenarios

☐ Cool: Infrequently accessed data and backup scenarios

Azure Files

Enable large file shares ⓘ ☐ 7

Tables and Queues

Enable support for customer-managed keys ⓘ ☐ 8

Review + create < Previous **Next : Networking >** 9

" **Network connectivity** " bölümünde " **Connectivity Method** " konfigürasyonlarında ; Storage Account'unuza genel olarak , Public IP adresleri veya Service Endpoint aracılığıyla veya Private Endpoint kullanarak özel olarak bağlanabilirsiniz. **Şunu belirtmek istiyorum ki : " Public endpoint (all networks) " seçeneğini seçersek , Tüm Ağlar bu Storage Account'a erişebilecek. Fakat tavsiye edilen, Bu kaynağa ağınızdan Özel olarak erişmek isterseniz , " Private endpoint " seçeneğini seçebilirsiniz.**

" **Public Endpoint (all networks)** " seçeneğini seçerek devam ederiz. (Yapınıza veya ihtiyacınıza göre uygun olanı belirlemeniz yararınıza olacaktır.)

" **Network routing** " bölümünde kaynaktan Azure Endpoint noktasına giderken trafiğinizi belirleyebilirsiniz. Çoğu Organizasyonlar için önerilmektedir. " **Routing prefence** " konfigürasyonlarında ise " **Microsoft Network Routing** " seçeneğini seçtiğinizde trafiğinizi kaynağından kabul edilebilir sürede Microsoft Bulutuna yönlendiriyor olacaktır. " **İnternet Routing** " seçeneğini seçtiğinizde trafiğinizi Azure Enpoint'e daha yakın Microsoft Bulutuna yönlendiriyor olacaktır.

" **Microsoft Network Routing** " seçeneğini seçerek devam ederiz. (Yapınıza veya ihtiyacınıza göre uygun olanı belirlemeniz yararınıza olacaktır.)

Bir sonraki " **Data protection** " adımına geçmek için " **Next : Data Protection >** " seçeneğini seçerek devam ederiz.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Networking' tab is active. The 'Connectivity method' dropdown is set to 'Public endpoint (all networks)'. The 'Routing preference' dropdown is set to 'Microsoft network routing'. The 'Next : Data protection >' button is highlighted with a red '4'.

" **Data Protection** " bölümünde " **Recovery** " alanında ortamınızdaki verilerinizin sehven silinmesini veya değiştirilmesine karşı korumanızı sağlamak için konfigürasyonlar yer almaktadır.

" **Enable point-in-time restore for containers** " seçeneğinin yanındaki kutucuğu işaretlediğinizde bir veya daha fazla Container'e daha önceki durumuna geri dönmek için Checkpoint (Bazen Snapshot olarak da anılmaktadır.) denen kavramı burada belirlemiş olduğumuz konfigürasyona göre geri dönebiliriz. Ayrıca bu seçeneği etkinleştirdiğinizde , Versiyon oluşturma ve Blob Soft Delete işlemlerini gerçekleştirebilirsiniz.

" **Enable soft delete for blobs** " seçeneği ise Geçici silme olarak anılmaktadır. Üzerine yazılan Blob'larda dahil olmak üzere , yapınızda daha önceki silinecekler olarak belirlenmiş Blobları kurtarmanıza imkan tanımaktadır. Bu bölümde etkinleştirme işlemi gerçekleştirdiğinizde " **Days to retain deleted blobs** " seçeneğinde kutucukta belirlemiş olduğunuz değer , Silinmek üzere işaretlenen yapınızdaki Blobun kalıcı olarak silinene kadar devam edeceği gün sayısını konfigüre etmiş oluruz. **Default değer olarak " 7 gün " olarak belirleriz.**

" **Enable soft delete for containers** " seçeneği ise Geçici silme olarak anılmaktadır. Üzerine yazılan Blob'larda dahil olmak üzere , yapınızda daha önceki silinecekler olarak belirlenmiş Container'ları kurtarmanıza imkan tanımaktadır. Bu bölümde etkinleştirme işlemi gerçekleştirdiğinizde " **Days to retain deleted containers** " seçeneğinde kutucukta belirlemiş olduğunuz değer , Silinmek üzere işaretlenen yapınızdaki Container'ın kalıcı olarak silinene kadar devam edeceği gün sayısını konfigüre etmiş oluruz. **Default değer olarak " 7 gün " olarak belirleriz.**

" **Enable soft delete for file shares** " seçeneği ise Geçici silme olarak anılmaktadır. Üzerine yazılan Blob'larda dahil olmak üzere , yapınızda daha önceki silinecekler olarak belirlenmiş Dosya Paylaşımlarınızı kurtarmanıza imkan tanımaktadır. Bu bölümde etkinleştirme işlemi gerçekleştirdiğinizde " **Days to retain deleted file shares** " seçeneğinde kutucukta belirlemiş olduğunuz değer , Silinmek üzere işaretlenen yapınızdaki Dosya Paylaşımının kalıcı olarak silinene kadar devam edeceği gün sayısını konfigüre etmiş oluruz. **Default değer olarak " 7 gün " olarak belirleriz.**

Microsoft Azure

Home > Storage accounts >

Create a storage account

Basics Advanced Networking **Data protection** 1 Tags Review + create

Recovery

Protect your data from accidental or erroneous deletion or modification.

☐ Enable point-in-time restore for containers 2
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

☒ Enable soft delete for blobs 3
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Days to retain deleted blobs ⓘ 7

☒ Enable soft delete for containers 4
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Days to retain deleted containers ⓘ 7

☒ Enable soft delete for file shares 5
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)

Days to retain deleted file shares ⓘ 7

" **Data Protection** " bölümünde " **Tracking** " alanında versiyonları yönetmenize ve Blob verilerinizde yapılan değişiklikleri takip etmemizi sağlamaktadır.

" **Enable versioning for blobs** " seçeneğini etkinleştirerek , Recovery yani Kurtarma ve Restore işlemlerinizi için yapınızdaki Blob'larınızın önceki versiyonlarını otomatik olarak koruma sağlamaktadır.

" **Enable blob change feed** " seçeneğini etkinleştirerek , hesabınızda blob'larda oluşturma , değiştirme ve silme değişikliklerinizi takip edebilirsiniz. Etkinleştirme sonrası 2 seçenek karşımıza çıkmaktadır. " **Keep all logs** " ve " **Delete change feed logs after (in days)** "

" **Keep all logs** " seçeneğini seçerek , tüm loglar ortamda kalmalı.

" **Delete change feed logs after (in days)** " seçeneğini seçerek , etkinleştirme sonrası ne kadar Gün kalmasını belirleyebiliriz.

" **Access Control** " alanında " **Enable version-level immutability support** " seçeneğini seçerek , Blob versiyonları için zamana dayalı Bekletme politikaları konfigüre etmenize imkan tanınmaktadır. Account veya Container seviyesinde Default yani varsayılan politikalar konfigüre edilebilmekte veya Belirlemiş olduğunuz Bloblar veya versiyonlar için yapımıza göre politikalar belirleyebilirsiniz. Bu özelliğin Etkinleştirilmesi için versiyon oluşturma işlemi etkileştirmeniz gerekmektedir. " **Tracking** " alanında " **Enable versioning for blobs** " seçeneği aktif olmalıdır. Bir sonraki " **Tags** " adımına geçmek için " **Next : Tags >** " seçeneğini seçerek devam ederiz.

" **Data Protection** " bölümünde " **Tracking** " alanında Versiyonları yönetmenize ve Blob verilerinizde yapılan değişiklikleri takip etmemizi sağlamaktadır.

" **Enable versioning for blobs** " seçeneğini etkinleştirerek , Recovery yani Kurtarma ve Restore işlemlerinizi için yapınızdaki Blob'larınızın önceki versiyonlarını otomatik olarak koruma sağlamaktadır.

" **Enable blob change feed** " seçeneğini etkinleştirerek , Hesabınızda blob'larda oluşturma , Değiştirme ve silme değişikliklerinizi takip edebilirsiniz. Etkinleştirme sonrası 2 seçenek karşımıza çıkmaktadır. " **Keep all logs** " ve " **Delete change feed logs after (in days)** "

" **Keep all logs** " seçeneğini seçerek , Tüm Loglar ortamda kalmalı.

" **Delete change feed logs after (in days)** " seçeneğini seçerek , etkinleştirme sonrası ne kadar Gün kalmasını belirleyebiliriz.

" **Access Control** " alanında " **Enable version-level immutability support** " seçeneğini seçerek , Blob versiyonları için zamana dayalı Bekletme politikaları konfigüre etmenize imkan tanınmaktadır. Account veya Container seviyesinde Default yani varsayılan politikalar konfigüre edilebilmekte veya Belirlemiş olduğunuz Bloblar veya versiyonlar için yapımıza göre politikalar belirleyebilirsiniz. Bu özelliğin Etkinleştirilmesi için versiyon oluşturma işlemini etkileştirmeniz gerekmektedir. " **Tracking** " alanında " **Enable versioning for blobs** " seçeneği aktif olmalıdır. Bir sonraki " **Tags** " adımına geçmek için " **Next : Tags >** " seçeneğini seçerek devam ederiz.

Tracking

Manage versions and keep track of changes made to your blob data.

☒ **Enable versioning for blobs** ¹
Use versioning to automatically maintain previous versions of your blobs for recovery and restoration. [Learn more](#)

☒ **Enable blob change feed** ²
Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)

☒ Keep all logs

☐ Delete change feed logs after (in days)

Access control

☐ **Enable version-level immutability support** ³
Allows you to set time-based retention policies for blob versions. You can set a default policies at the account or container level, or set policies for specific blobs or versions. Versioning is required for this property to be enabled. [Learn more](#)

[Review + create](#) [< Previous](#) [Next : Tags >](#) ⁴

Bu bölümde oluşturacağınız kaynaklarımıza daha kolay bulunabilmesi için etiketleme standardı belirleyerek , oluşturma işlemlerini gerçekleştirebilirsiniz.

Microsoft Azure

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking Data protection **Tags** ¹ Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

²

Name	Value	Resource
<input type="text"/>	:	<input type="text"/> All resources selected

[Review + create](#) [< Previous](#) [Next : Review + create >](#) ³

Ardından kaynak oluşturma işlemlerinin başlaması için gerekli kontroller sağlanarak , kaynağımızın oluşması için herhangi bir engel mevcut mu ? Kontroller aşamasına geçmek için " **Next : Review + create** > " seçeneğini seçerek devam ederiz.

" **Review + Create** " bölümünde Azure ortamında oluşturduğunuz veya oluşturacağımız Storage Account ile alakalı konfigürasyonlarının özet bilgilerini inceleyerek uygun ise oluşturma işlemlerini sağlayabilirsiniz. " **Validation Passed** " uyarısı aldığımızı göre konfigürasyonlarımızda herhangi bir problem olmadığını görmüş oluruz. Oluşturma işlemlerine başlamak için " **Create** " seçeneğini seçeriz.

Microsoft Azure

Home > Storage accounts >

Create a storage account ...

Validation passed 1

Basics Advanced Networking Data protection Tags Review + create

Basics

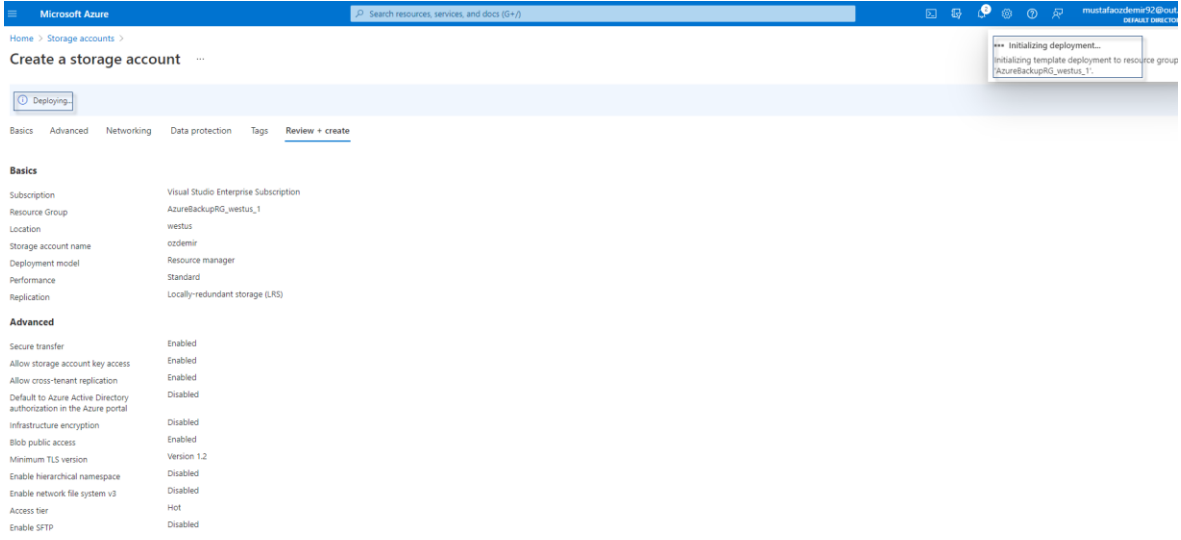
Subscription	Visual Studio Enterprise Subscription
Resource Group	AzureBackupRG_westus_1
Location	westus
Storage account name	ozdemir
Deployment model	Resource manager
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

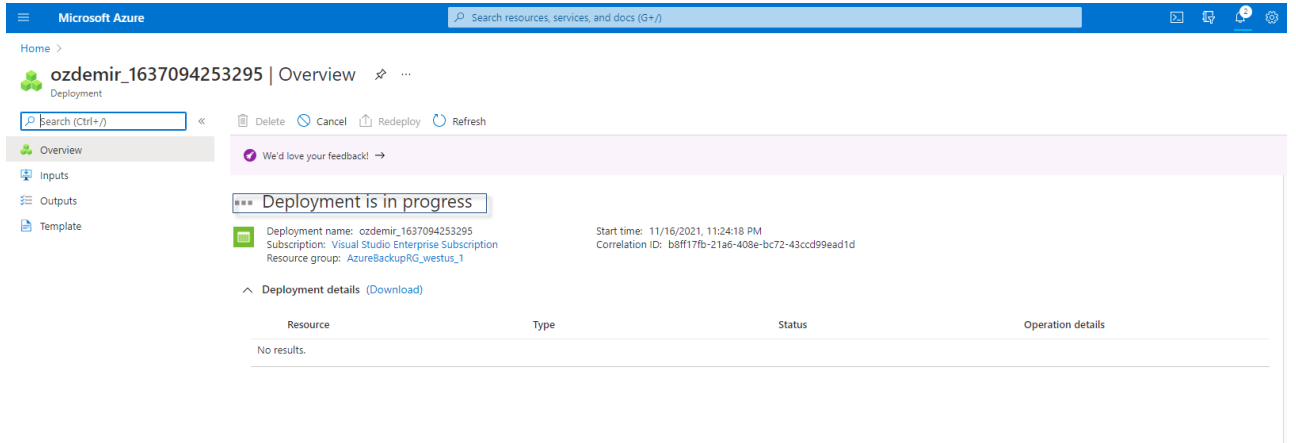
Secure transfer	Enabled
Allow storage account key access	Enabled
Allow cross-tenant replication	Enabled
Default to Azure Active Directory authorization in the Azure portal	Disabled
Infrastructure encryption	Disabled
Blob public access	Enabled
Minimum TLS version	Version 1.2
Enable hierarchical namespace	Disabled
Enable network file system v3	Disabled
Access tier	Hot
Enable SFTP	Disabled

Create 2 < Previous Next > Download a template for automation

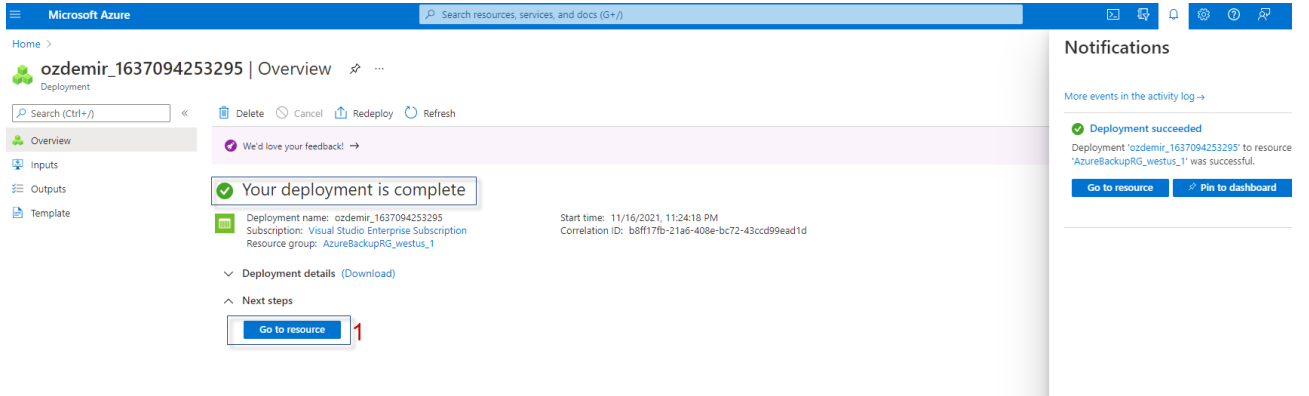
Deployment işlemi başladı.



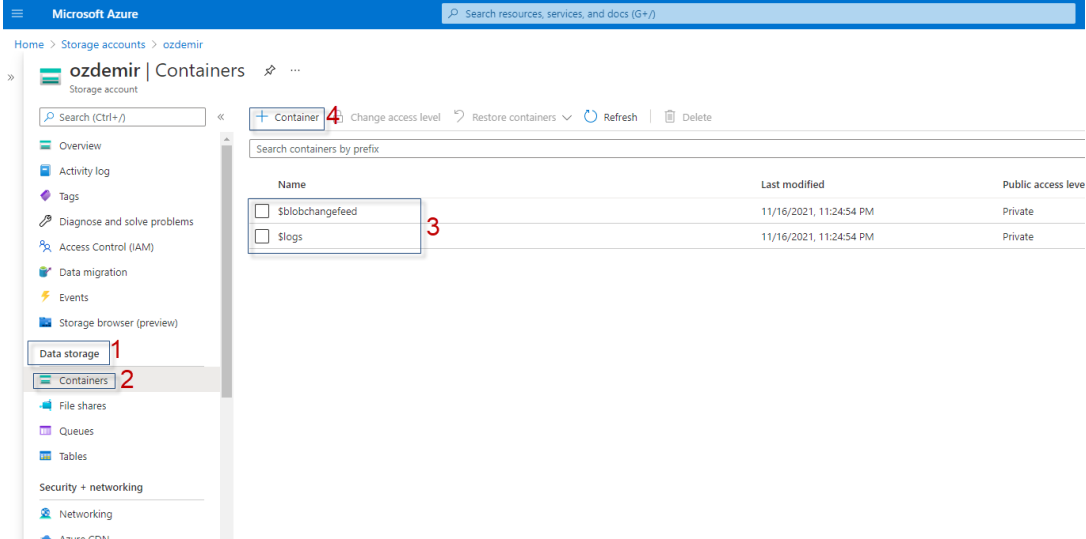
Kaynak oluşturma işlemleri devam etmektedir.



Storage Account oluşturma işlemimiz tamamlanmıştır. Kaynağımızın konfigürasyonu ve arayüzüne gitmek için "Go to Resource" seçeneğini seçeriz.



Storage Account kaynağımızın başarılı problemsiz şekilde oluştuğu görmüş oluruz ve adımlarımıza devam ediyoruz. Bir sonraki adımımız konfigürasyonlar bölümünde " **Data Storage** " alanının altındaki Blob hizmetini kullanmak için " **Containers** " seçeneğini seçeriz. Ardından yapımızda yeni bir Container oluşturacaksa yada Storage Account'umuzda oluşturduğumuz veya var olan Container'larımızı görmüş oluruz. Fakat biz User Defined yani Kullanıcı Tanımlı bir kapsayıcı oluşturacağız. Bunun için " **Container** " seçeneğini seçeriz.



" **Container** " oluşturma işlemlerinde " **Name** " kısmına depolayacağımız dosyalar ile alakalı isimlendirme sağlayabilmekte özgür olduğunuzun bilgisini vermek isterim. " **Public access level** " alanında ise " **Private (no anonymous access)** " seçeneğini seçeriz. " **Public access level** " Container içeriğindeki verilere genel olarak erişilip erişilemeyeceğini belirtmektedir. Varsayılan seçeneği seçmiş olduk. Yani Container verileri hesap sahibine özeldir. Blob'lar için Public Okuma erişimine izin vermek için " **Blob (anonymous read access for blobs only)** " seçeneğini seçebilirsiniz. Tüm Container'a Genel Okuma ve Listeleme erişimine izin vermek için " **Container (anonymous read access for containers and blobs)** " seçeneğini seçebilirsiniz.

Ardından oluşturma işlemleri için " **Create** " seçeneğini seçeriz.

New container ×

1 Name *
images ✓

2 Public access level ⓘ
Private (no anonymous access) ▼

✓ Advanced

3 Create Discard

Ardından Storage Container kaynağımızın oluştuğunu görmüş oluruz.

Search resources, services, and docs (G+)

mustafaazdemir
DEFAULT

Notifications

More events in the activity log →

1 Successfully created storage container
Successfully created storage container 'images'. a few

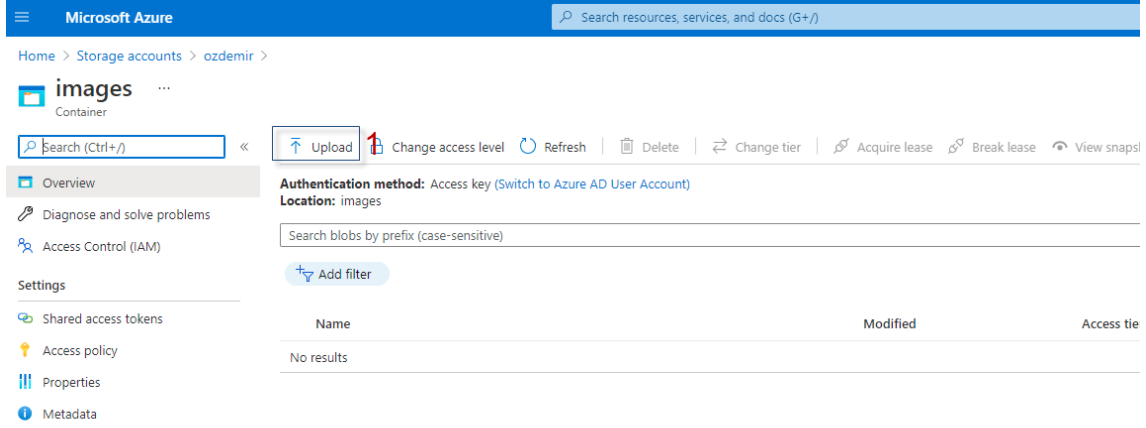
+ Container Change access level Restore containers Refresh Delete

Search containers by prefix

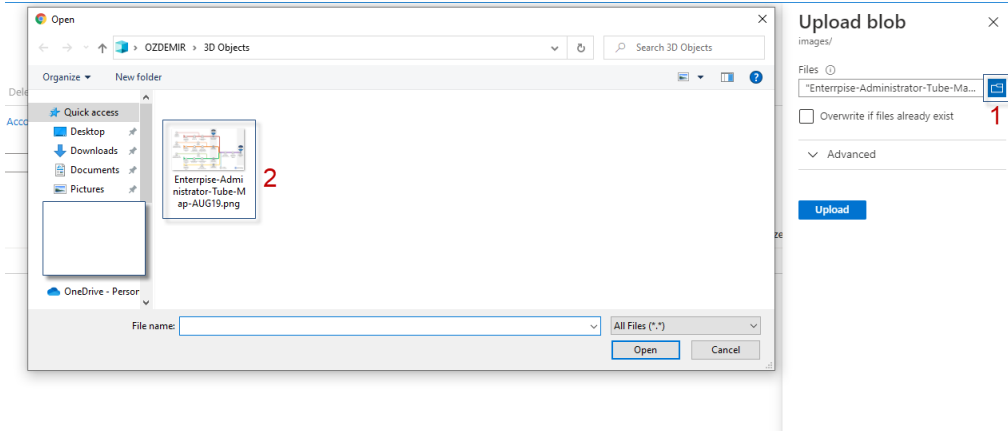
Name	Last modified	Public access level
<input type="checkbox"/> \$blobchangeFeed	11/16/2021, 11:24:54 PM	Private
<input type="checkbox"/> \$logs	11/16/2021, 11:24:54 PM	Private
<input type="checkbox"/> images	11/17/2021, 12:05:35 AM	Private

2

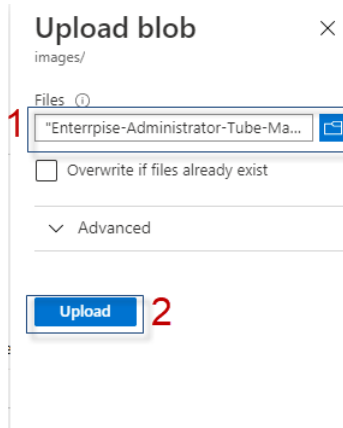
Oluşturmuş olduğumuz " **images** " üzerine çift tıklayarak container içeriğine gireriz. Şimdi Blob yükleyerek test ediyor olacağız. Ardından " **Upload** " seçeneğini seçeriz.



Blob olarak eklemek istediğimiz veriyi seçeriz. Bunun için " **Browse** " anlamına gelen klasör simgesine tıklarız. Bilgisayarımızdan ilgili veriyi seçeriz.



Seçtiğimiz dosyanın " **Files** " alanına geldiğini görürüz. Ardından Blob'un yüklenmesi için " **Upload** " seçeneğini seçerek devam ederiz.



Yüklediğimiz Blob düşmediyse " **Refresh** " seçeneğini seçerek devam edebilirsiniz.

Upload Change access level Refresh 1 Delete Change tier Acquire lease Break lease View snapshots Create snapshot

Authentication method: Access key (Switch to Azure AD User Account)
Location: images

Search blobs by prefix (case-sensitive) Show deleted blobs

Add filter

Name	Modified	Access tier	Archive status	Blob type
Enterprise-Administrator-Tube-Map-AUG19.png	11/17/2021, 12:14:59 AM	Hot (Inferred)		Block blob

Yüklediğimiz Blob'un üzerine tıklayarak , içeriğine gireriz ve Blob'umuzun özel olduğunu görmüş oluruz. " **Change access level** " ile Blob'larımızın dışarıdan veya özelden erişilebilirliğini değiştirme imkanına sahip olduğunuzun bilgisini vermek istiyorum.

Search resources, services, and docs (G+)

emir > images >

« Upload Change access level ...

Authentication method: Access key (Switch to Azure AD User Account)
Location: images

Search blobs by prefix (case-sensitive) Show deleted blobs

Add filter

Name

Enterprise-Administrator-Tube-Map-AUG19.png 1

Enterprise-Administrator-Tube-Map-AUG19.png ...

Blob

Save Discard Download Refresh Delete Change tier Acquire lease Break lease

Overview Versions Snapshots Edit Generate SAS

Properties

URL https://ozdemir.blob.core.windows.net/images/Enterprise-Administrator-Tube-Map-AUG19.png

LAST MODIFIED 11/17/2021, 12:14:59 AM

CREATION TIME 11/17/2021, 12:14:59 AM

VERSION ID -

TYPE Block blob

SIZE 90.02 KiB

ACCESS TIER Hot (Inferred)

ACCESS TIER LAST MODIFIED N/A

ARCHIVE STATUS -

REHYDRATE PRIORITY -

SERVER ENCRYPTED true

ETAG 0x8D9A94625B2E2A9

VERSION-LEVEL IMMUTABILITY POLICY Disabled

CONTENT-TYPE image/png

CONTENT-MD5 /QfrifW6dMrfs0c6uifPmw==

LEASE STATUS Unlocked

LEASE STATE Available

LEASE DURATION -

COPY STATUS -

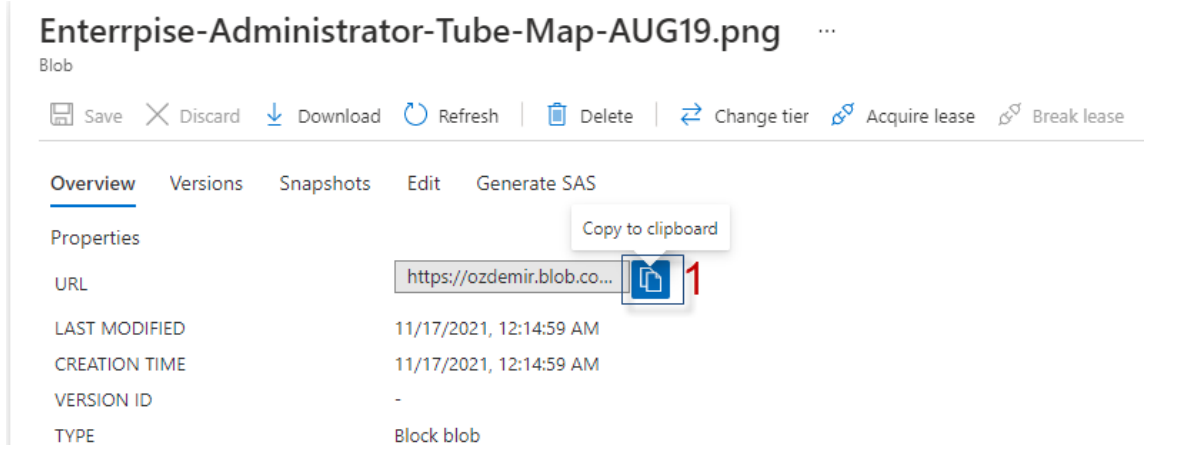
COPY COMPLETION TIME -

Undelete

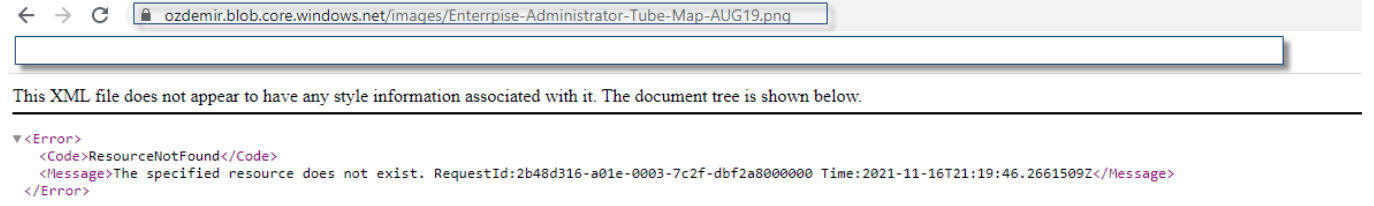
Metadata

Key	Value

Blob URL bölümündeki linki kopyalayarak , Browser arama çubuğuna yapıştırırız.



İlgili URL'İ Browser adres çubuğuna kopyalayarak eriştiğimizde özel olduğu için Blobu göremeyeceğimiz bilgisini vermektedir. Benimde istediğim özel ve gizli olmasıydı.



Böylece işlemlerimiz tamamlamış oluruz.