Microsoft Certified: Azure Fundamentals

# Learning Path: Azure Fundamentals: Describe Azure Architecture and Services

Genel bulut kavramlarına giriş yapılan modüldür. Genel olarak buluta giriş ile başlanacak ve paylaşılan sorumluluk, farklı bulut modelleri ve benzersiz bulut fiyatlamaları gibi kavramlara değinilmiştir. Modülün öğrenme hedefleri şunlardır;

* Bulut bilişimi tanımlama (Define cloud computing)
* Paylaşılan sorumluluk modelini tanımlama (Describe the shared responsibility model)
* Genel, özel ve hibrit dahil olmak üzere bulut modellerini tanımlama (Define cloud models, including public, private, and hybrid)
* Her bir bulut modeli için uygun kullanım durumlarını belirleme (Identify appropriate use cases for each cloud model)
* Tüketim temelli modeli tanımlama (Describe the consumption-based model)
* Bulut fiyatlandırma modellerini karşılaştırma (Compare cloud pricing models)

## Describe the Core Architectural Components of Azure

Azure’un temel altyapı bileşenlerinin açıklandığı bölümdür. Fiziksel altyapı, kaynakların nasıl yönetildiği konulara değinilmiştir. Modülün öğrenme hedefleri şunlardır;

* Azure bölgelerini, bölge çiftlerini ve egemen bölgeleri tanımlama (Describe Azure regions, region pairs, and sovereign regions)
* Kullanılabilirlik bölgelerini tanımlama (Describe availability zones)
* Azure veri merkezlerini tanımlama (Describe Azure datacenters)
* Azure kaynaklarını ve kaynak gruplarını tanımlama (Describe Azure resources and resource groups)
* Abonelikleri tanımlama (Describe subscriptions)
* Yönetim gruplarını tanımlama (Describe management groups)
* Kaynak grupları, abonelikler ve yönetim grupları hiyararşisini tanımlama (Describe the hiararchy of resource groups, subscriptions, and management groups)

### 2.1.1 What is Microsoft Azure?

Azure, mevcut ve gelecekteki iş zorluklarının üstesinden gelmeye yardımcı olan ve sürekli genişleyen bir bulut hizmetleri kümesidir. Azure; favori araçları, çerçeveleri kullanarak devasa bir küresel ağ üzerinde uygulama oluşturma, yönetme ve dağıtma özgürlüğü sunar.

Azure’un yardımıyla bir sonraki harika çözümü oluşturmak için ihtiyaç duyulan her şeye sahip olunabilir.

* Geleceğe Hazır Olma: Sunduğu yenilikler, bugünkü gelişimi ve yarına yönelik ürün vizyonlarını destekler
* Kendi Koşullarınıza Göre Oluşturma: Seçenekler mevcut, açık kaynak taahhüdü, tüm diller ve çerçeveler desteği sayesinde istenilen şekilde oluşturulabilir, dağıtılabilir.
* Sorunsuz Hibrit Çalıştırma: Şirket içinde, bulutta, uçta, nerede olursanız olun araçlar ve hizmetler ortama entegre edilebilir ve yönetilebilir.
* Buluta Güven: Uzmanlardan oluşan ekip tarafından desteklenen güvenlik sayesinde uyumluluk elde edilebilir.

Azure mevcut uygulamaları sanal makineler çalıştırmaktan akıllı botlar ve karma gerçeklik gibi yeni yazılım paradigmalarını keşfetmeye kadar her şeyi yapmayı sağlayan 100’den fazla hizmet sunar. Birçok ekip bulutu keşfetmeye mevcut uygulamalarını Azure’da çalışan sanal makinelere taşıyarak başlar. Örneğin Azure, kullanıcılarınızla görme, duyma ve konuşma yoluyla doğal bir şekilde iletişim kurabilen yapay zeka (AI) ve makine öğrenimi (ML) hizmetleri sağlar. Ayrıca, büyük miktarda veriyi barındırmak için dinamik olarak büyüyen depolama çözümleri de sağlar.

### 2.1.2 Get Started with Azure Accounts

Azure hizmetlerini oluşturmak ve kullanmak için Azure aboneliği gerekir. Bir Azure hesabına sahip olduktan sonra ek abonelikler oluşturmakta kullanıcı özgürdür. Örneğin, şirketiniz işletmeniz için tek bir Azure hesabı ve geliştirme, pazarlama ve satış departmanları için ayrı abonelikler kullanabilir. Bir Azure aboneliği oluşturduktan sonra, her abonelik içinde Azure kaynakları oluşturmaya başlayabilirsiniz.

A diagram of a diagram of a software company

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-core-architectural-components-of-azure/media/account-scope-levels-9ceb3abd.png>

### 2.1.3 Describe Azure Physical Infrastructure

Azure için fiziksel altyapı, veri merkezleriyle başlar. Veri merkezleri büyük kurumsal veri merkezleri ile aynıdır. Bunlar özel güç, soğutma, ağ altyapısına sahip raflarda düzenlenmiş kaynaklara sahip tesislerdir. Azure’un dünya çapınca veri merkezleri vardır ancak bu veri merkezlerine doğrudan erişilmez. Veri Merkezleri, Azure Bölgeleri ve Azure Kullanılabilirlik Bölgeleri olarak gruplandırılır.

#### 2.1.3.1 Regions

Bölge, gezegen üzerinde birbirine yakın ve düşük gecikmeli bir ağla birbirine bağlanmış, en az bir ancak potansiyel olarak birden fazla veri merkezi içeren coğrafi alanlardır. Azure’da bir kaynak dağıtılırken genellikle dağıtılması istenilen bölge seçilmesi gereklidir. Belirli VM boyutları veya depolama türleri gibi bazı hizmetler veya sanal makine (VM) özellikleri yalnızca belirli bölgelerde kullanılabilir.

#### 2.1.3.2 Availability Zones

Kullanılabilirlik bölgeleri bir Azure bölgesi içinde fiziksel olarak ayrı veri merkezleridir. Her kullanılabilirlik bölgesi, bağımsız güç, soğutma ve ağ iletişimi ile donatılmış bir veya daha fazla veri merkezinden oluşur. Kullanılabilirlik bölgesi, bir yalıtım sınırı olacak şekilde ayarlanır. Bir bölge çökerse diğeri çalışmaya devam eder. Kullanılabilirlik bölgeleri yüksek hızlı, özel fiber optik ağlarla birbirine bağlanır.

A diagram of a diagram

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-core-architectural-components-of-azure/media/availability-zones-c22f95a3.png>

#### 2.1.3.3 Region Pairs

Çoğu Azure bölgesi, aynı coğrafyada (ABD, Avrupa veya Asya gibi) en az 300 mil uzaklıktaki başka bir bölgeyle eşleştirilir. Bu yaklaşım, tüm bölgeyi etkileyen doğal afetler, sivil ayaklanmalar, elektrik kesintileri veya fiziksel ağ kesintileri gibi olaylar nedeniyle kesinti olasılığını azaltmaya yardımcı olan bir coğrafya genelinde kaynakların çoğaltılmasına olanak tanır. Azure'daki bölge çiftlerine örnek olarak Doğu ABD ile eşleştirilmiş Batı ABD ve Doğu Asya ile eşleştirilmiş Güneydoğu Asya verilebilir.

A diagram of a computer

Description automatically generated with medium confidence

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-core-architectural-components-of-azure/media/region-pairs-7c495a33.png>

### 2.1.4 Describe Azure Management Infrastructure

Yönetim altyapısı, Azure kaynaklarını ve kaynak gruplarını, abonelikleri ve hesapları içerir.

#### 2.1.4.1 Azure Resources and Resource Groups

Kaynak Azure’ın temel yapı taşıdır. Oluşturulan, saklanan, dağıtılan her şey bir kaynaktır. VM’ler, sanal ağlar, veri tabanları, billişsel hizmetler vb. Azure’da kaynak olarak kabul edilir.

Kaynak grupları kaynakların gruplandırılmasıdır. Bir kaynak oluşturulduğunda, onu bir kaynak grubuna yerleştirmek gerekir. Bir kaynak grubu birçok kaynak içerebilirken, tek bir kaynak aynı anda yalnızca bir kaynak grubunda yer alabilir. Bir kaynak grubuna bir eylem uygulandığında, bu eylem kaynak grubundaki tüm kaynaklar için geçerli olur. Bir kaynak grubu silinirse, tüm kaynaklar silinir. Bir kaynak grubuna erişim izni verilir veya erişimi reddedilirse, kaynak grubundaki tüm kaynaklara erişim izni verilmiş veya reddedilmiş olur.

#### 2.1.4.2 Azure Subscriptions

Azure'da abonelikler bir yönetim, faturalama ve ölçek birimidir. Abonelik, Azure ürün ve hizmetlerine kimliği doğrulanmış ve yetkilendirilmiş erişim sağlar. Azure aboneliklerini Azure ürünleri, hizmetleri ve kaynakları etrafında sınırlar tanımlamak için kullanabilirsiniz. İki tür abonelik sınırı vardır;

* Faturalandırma Sınırı: Bu abonelik türü, bir Azure hesabının Azure kullanımı için nasıl faturalandırılacağını belirler. Azure, maliyetleri düzenleyebilmeniz ve yönetebilmeniz için her abonelik için ayrı faturalandırma raporları ve faturalar oluşturur.
* Erişim Denetimi Sınırı: Azure, abonelik düzeyinde erişim yönetimi ilkeleri uygular ve farklı kurumsal yapıları yansıtmak için ayrı abonelikler oluşturulabilir. Bir işletme içinde, farklı Azure abonelik ilkeleri uygulanan farklı departmanların olması buna bir örnektir.

A diagram of a computer program

Description automatically generated with medium confidence

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-core-architectural-components-of-azure/media/subscriptions-d415577b.png>

#### 2.1.4.3 Azure Management Groups

Kaynaklar kaynak gruplarında, kaynak grupları da aboneliklerde toplanır. Çok sayıda abonelik varsa bu abonelikler için erişimi, ilkeleri ve uyumluluğu verimli bir şekilde yönetmenin bir yolunun bulunması gerekebilir. Azure yönetim grupları, aboneliklerin üzerinde bir kapsam düzeyi sağlar. Abonelikleri yönetim grupları adı verilen kapsayıcılar halinde düzenlenir ve yönetim gruplarına idare koşulları uygulanır. Yönetim grupları, ne tür aboneliklere sahip olunursa olunsun, büyük ölçekte kurumsal düzeyde yönetim sağlar. Yönetim grupları iç içe yerleştirilebilir.

A diagram of a company

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-core-architectural-components-of-azure/media/management-groups-subscriptions-dfd5a108.png>

## Describe Azure Compute and Networking Services

Azure’da bulunan bazı bilgisayar ve ağ hizmetlerine odaklanılan bölümdür. Modülün öğrenme hedefleri şunlardır;

* Konteyner örnekleri, sanal makineler ve fonksiyonlar dahil olmak üzere bilgi işlem türlerini karşılaştırma (Compare compute types, including container instances, virtual machines, and functions)
* VM'ler, Sanal Makine Ölçek Kümeleri, kullanılabilirlik kümeleri, Azure Sanal Masaüstü dahil olmak üzere sanal makine (VM) seçeneklerini tanımlama (Describe virtual machine (VM) options, including VMs, Virtual Machine Scale Sets, availability sets, Azure Virtual Desktop)
* Sanal makineler için gereken kaynakları tanımlama (Describe resources required for virtual machines)
* Azure Web Apps, kapsayıcılar ve sanal makineler dahil olmak üzere uygulama barındırma seçeneklerini tanımlama (Describe application hosting options, including Azure Web Apps, containers, and virtual machines)
* Azure Sanal Ağlarının amacı, Azure sanal alt ağları, eşleme, Azure DNS, VPN Gateway ve ExpressRoute dahil olmak üzere sanal ağı tanımlama (Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, VPN Gateway, and ExpressRoute)
* Genel ve özel uç noktaları tanımlama (Define public and private endpoints)

### 2.2.1 Describe Azure Virtual Machines

Azure VM ile bulutta VM’ler oluşturulabilir ve kullanılabilir. VM’ler sanallaştırılmış bir sunucu biçiminde hizmet olarak altyapı (IaaS) sağlar ve birçok şekilde kullanılabilir. VM'leri hızlı bir şekilde sağlamak için önceden oluşturulmuş bir imaj oluşturulabilir veya kullanılabilir. Önceden yapılandırılmış bir VM imajı seçildiğinde dakikalar içinde bir VM oluşturulabilir.

#### Scale VMs in Azure

Test, geliştirme ve küçük görevler için tek bir sanal makine çalıştırılabilir ya da yüksek kullanılabilirlik, ölçeklenebilirlik ve yedeklilik sağlamak için VM’ler birlikte gruplandırılabilir.

Sanal makine ölçek kümeleri bir grup aynı, yük dengeli sanal mkaine oluşturmaya ve yönetmeye olanak tanır. Aynı amaçla oluşturulan birden çok VM’nin aynı şekilde yapılandırıldığından emin olmak ve verimliliği sağlamak gerekir. Bunun yerine, sanal makine ölçek kümeleri ile Azure bu işlerin çoğunu otomatikleştirir. Sanal makine ölçek setleri ayrıca kaynaklarınızın verimli bir şekilde kullanıldığından emin olmak için otomatik olarak bir yük dengeleyici dağıtır.

Sanal makine kullanılabilirlik setleri, daha esnek ve yüksek oranda kullanılabilir bir ortam oluşturmaya yardımcı olacak bir başka araçtır. Kullanılabilirlik kümeleri, VM'lerin güncellemeleri kademelendirmesini ve çeşitli güç ve ağ bağlantılarına sahip olmasını sağlamak için tasarlanmıştır, böylece tek bir ağ veya güç kesintisi ile tüm VM'lerin kaybedilmesini önler.

### Describe Azure Virtual Desktop

Azure Sanal Masaüstü, bulut üzerinde çalışan bir masaüstü ve uygulama sanallaştırma hizmetidir. Herhangi bir konumdan Windows'un bulutta barındırılan bir sürümünün kullanılmasını sağlar. Azure Sanal Masaüstü, Microsoft Entra ID ile kullanıcıların masaüstleri için merkezi güvenlik yönetimi sağlar.

Azure Sanal Masaüstü ile veriler ve uygulamalar yerel donanımdan ayrılır. Gerçek masaüstü ve uygulamalar bulutta çalıştığından, gizli verilerin kişisel bir cihazda bırakılma riski azalır. Ayrıca, kullanıcı oturumları hem tekli hem de çoklu oturum ortamlarında izole edilir.

### 2.2.3 Describe Azure Containers

Sanal makineler, fiziksel donanım için gerekli olan yatırımlara kıyasla maliyetleri düşürmenin mükemmel bir yolu olsa da, yine de sanal makine başına tek bir işletim sistemiyle sınırlıdırlar. Bir uygulamanın birden fazla örneğini tek bir ana makinede çalıştırmak istiyorsanız, konteynerler mükemmel bir seçimdir.

Konteynerler bir sanallaştırma ortamıdır. Tek bir fiziksel ana bilgisayarda birden fazla sanal makine çalıştırmaya benzer şekilde, tek bir fiziksel veya sanal ana bilgisayarda birden fazla kapsayıcı çalıştırılabilir. Konteynerler hafiftir ve dinamik olarak oluşturulmak, ölçeklendirilmek ve durdurulmak üzere tasarlanmıştır. Konteynerler, talep üzerine değişikliklere yanıt vermenize olanak tanıyacak şekilde tasarlanmıştır. Kapsayıcılarla, bir çökme veya donanım kesintisi olduğunda hızlı bir şekilde yeniden başlşatılabilir. En popüler kapsayıcı motorlarından biri Docker'dır ve Azure Docker'ı destekler.

#### Azure Container Instances

Azure Container Instances, herhangi bir sanal makineyi yönetmek veya herhangi bir ek hizmet benimsemek zorunda kalmadan Azure'da bir kapsayıcı çalıştırmanın en hızlı ve en basit yolunu sunar. Azure Container Instances bir hizmet olarak platform (PaaS) teklifidir. Azure Container Instances, kapsayıcılarınızı yüklemenize olanak tanır ve ardından hizmet kapsayıcıları sizin için çalıştırır.

#### Azure Container Apps

Azure Container Apps birçok yönden bir kapsayıcı örneğine benzer. Hemen çalışmaya başlamayı sağlarlar, kapsayıcı yönetimi kısmını ortadan kaldırırlar ve bir PaaS teklifidirler. Konteyner Uygulamaları, yük dengeleme ve ölçeklendirme gibi ekstra avantajlara sahiptir. Bu diğer işlevler tasarımında daha esnek olmayı sağlar.

#### Azure Kubernetes Service

Azure Kubernetes Service (AKS) bir kapsayıcı düzenleme hizmetidir. Orkestrasyon hizmeti, kapsayıcıların yaşam döngüsünü yönetir. Bir kapsayıcı filosu dağıtırken AKS, filo yönetimini daha basit ve verimli hale getirebilir.

### Describe Azure Functions

Azure İşlevleri, sanal makinelerin veya kapsayıcıların bakımını gerektirmeyen, olay güdümlü, sunucusuz bir işlem seçeneğidir. Azure İşlevleri ile bir olay işlevi uyandırır ve olay olmadığında kaynak sağlama ihtiyacını ortadan kaldırır.

Azure İşlevlerini kullanmak, altta yatan platform veya altyapıyla değil, yalnızca hizmetinizi çalıştıran kodla ilgilendiğinizde idealdir. İşlevler genellikle bir olaya (genellikle REST isteği aracılığıyla), zamanlayıcıya veya başka bir Azure hizmetinden gelen iletiye yanıt olarak iş gerçekleştirmeniz gerektiğinde ve bu işin saniyeler veya daha kısa sürede hızlı bir şekilde tamamlanabileceği durumlarda kullanılır.

İşlevler durumsuz veya durumlu olabilir. Durumsuz olduklarında (varsayılan), bir olaya her yanıt verdiklerinde yeniden başlatılıyorlarmış gibi davranırlar. Durumlu olduklarında (Dayanıklı İşlevler olarak adlandırılır), önceki etkinliği izlemek için işlevden bir bağlam geçirilir.

### Describe Application Hosting Options

Uygulamayı Azure’da barındırmak gerekiyorsa, başlangıçta bir VM veya kapsayıcılara yönelinebilir. Hem VM’ler hem de kapsayıcılar mükemmel barındırma çözümleri sunar. VM’ler kullanıcıya barındırma ortamı üzerinde maksimum kontrol sağlar. Azure ile kullanılabilecek başka barındırma seçenekleri de vardır.

#### Azure App Service

App Service, altyapıyı yönetmeden istenilen programlama dilinde web uygulamaları, arka plan işleri, mobil arka uçlar ve RESTful API'ler oluşturmaya ve barındırmaya olanak tanır. App Service Windows ve Linux'u destekler. Sürekli dağıtım modelini desteklemek için GitHub, Azure DevOps veya herhangi bir Git deposundan otomatik dağıtımlar sağlar. Azure App Service, uygulamaları Azure'da barındırmak için kullanılan sağlam bir barındırma seçeneğidir. App Service ile barındırılabilen en yaygın uygulama hizmeti stilleri şunlardır;

* Web Apps: App Service, ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP veya Python kullanarak web uygulamalarını barındırmak için tam destek içerir. Ana işletim sistemi olarak Windows veya Linux'u seçilebilir.
* API Apps: Bir web sitesini barındırmak gibi, seçilen dili ve çerçeveyi kullanarak REST tabanlı web API'leri oluşturulabilir. Tam Swagger desteği ve API'nizi Azure Marketplace'te paketleyip yayınlama olanağı elde edilir. Üretilen uygulamalar herhangi bir HTTP veya HTTPS tabanlı istemciden tüketilebilir.
* WebJobs: Bir programı (.exe, Java, PHP, Python veya Node.js) veya betiği (.cmd, .bat, PowerShell veya Bash) bir web uygulaması, API uygulaması veya mobil uygulama ile aynı bağlamda çalıştırmak için kullanılabilir. Zamanlanabilir veya bir tetikleyici tarafından çalıştırılabilirler. WebJobs genellikle uygulama mantığının bir parçası olarak arka plan görevlerini çalıştırmak için kullanılır.
* Mobile Apps: iOS ve Android uygulamaları için hızlı bir şekilde arka uç oluşturmak üzere App Service'in Mobil Uygulamalar özelliği kullanılır.

App Service, web erişimli uygulamaları barındırırken kullanıcının uğraştığı altyapı kararlarının çoğunu ele alır;

* Dağıtım ve yönetim platforma entegre edilmiştir.
* Uç noktalar güvence altına alınabilir.
* Siteler, yüksek trafik yükleriyle başa çıkmak için hızla ölçeklendirilebilir.
* Yerleşik yük dengeleme ve trafik yöneticisi yüksek kullanılabilirlik sağlar.

Tüm bu uygulama stilleri aynı altyapıda barındırılır ve bu avantajları paylaşır. Bu esneklik, App Service'i web odaklı uygulamaları barındırmak için ideal seçim haline getirir.

### Describe Azure Virtual Networking

Azure sanal ağları ve sanal alt ağları; VM’ler, web uygulamaları ve Veritabanları gizi kaynakların birbirleriyle, internetteki kullanıcılarla ve şirket içi istemci bilgisayarlarla iletişim kurmasını sağlar. Azure VN aşağıdaki temel ağ oluşturma özelliklerini sağlar;

* Yalıtım ve Segmentasyon: Azure VN birden çok yalıtılmış sanal ağ oluşturmaya olanak tanır. Sanal ağ kurulduğunda genel veya özel IP adresi aralıkları kullanarak özel bir IP adresi alanı tanımlanır. Bu IP adresi alt ağlara bölünebilir ve tanımlanan alanın bir kısmı her bir adlandırılmış alt ağa tahsis edilebilir.
* İnternet İletişimi: Bir Azure kaynağına genel bir IP adresi atanarak veya kaynağı genel bir yük dengeleyicinin arkasına konularak internetten gelen bağlantılar etkinleştirilebilir.
* Azure Kaynakları Arası İletişim Kurma: Azure kaynaklarının birbirleriyle güvenli iletişim kurmasını isteyeceksiniz. Hizmet uç noktaları, Azure SQL veritabanları ve depolama hesapları gibi diğer Azure kaynak türlerine bağlanabilir. Bu yaklaşım, güvenliği artırmak ve kaynaklar arasında en uygun yönlendirmeyi sağlamak için birden çok Azure kaynağını sanal ağlara bağlamanıza olanak tanır.
* Şirket içi Kaynaklarla İletişim Kurma: Azure VN şirket içi ortamlardaki kaynakları birbirine bağlamaya da yarar. Hem yerel hem bulut ortamını kapsayan bir ağ da oluşturulabilir.
* Ağ Trafiği Yönlendirme: Varsayılan olarak Azure bağlı tüm sanal ağlardaki alt ağlar, şirket içi ağlar ve internet arasındaki trafiği yönlendirir. Rota tabloları, trafiğin nasıl yönlendirilmesi gerektiğine ilişkin kuralları tanımlamanıza olanak tanır.
* Ağ Trafiği Filtreleme: Ağ güvenlik grupları, birden çok gelen ve giden güvenlik kuralı içerebilen Azure kaynaklarıdır. Bu kurallar, kaynak ve hedef IP adresi, bağlantı noktası ve protokol gibi faktörlere göre trafiğe izin verecek veya trafiği engelleyecek şekilde tanımlanabilir.
* Sanal Ağları Bağlama: Sanal ağ eşleştirmesini kullanarak sanal ağları birbirine bağlanabilir. Eşleme, iki sanal ağın doğrudan birbirine bağlanmasını sağlar. Eşlenen ağlar arasındaki ağ trafiği özeldir ve Microsoft omurga ağı üzerinde hareket eder, asla genel internete girmez.

### Describe Azure Virtual Private Networks

Sanal özel ağ (VPN), başka bir ağ içinde şifrelenmiş bir tünel kullanır. VPN'ler genellikle iki veya daha fazla güvenilir özel ağı güvenilmeyen bir ağ (tipik olarak genel internet) üzerinden birbirine bağlamak için kullanılır. Trafik, gizli dinleme veya diğer saldırıları önlemek için güvenilmeyen ağ üzerinden seyahat ederken şifrelenir. VPN'ler ağların hassas bilgileri güvenli ve emniyetli bir şekilde paylaşmasını sağlayabilir.

#### VPN Gateways

VPN ağ geçidi, bir tür sanal ağ geçididir. Azure VPN Ağ Geçidi örnekleri, sanal ağın ayrılmış bir alt ağında dağıtılır ve aşağıdaki bağlantıyı etkinleştirir:

* Şirket içi veri merkezlerini siteden siteye bağlantı yoluyla sanal ağlara bağlamak
* Noktadan siteye bağlantı aracılığıyla bireysel cihazları sanal ağa bağlamak
* Ağdan ağa bağlantı aracılığıyla sanal ağları diğer sanal ağlara bağlamak

Tüm veri aktarımı, internet üzerinden geçerken özel bir tünel içinde şifrelenir. Her sanal ağa yalnızca bir VPN ağ geçidi dağıtabilirsiniz. Ancak, diğer sanal ağları veya şirket içi veri merkezlerini içeren birden fazla konuma bağlanmak için bir ağ geçidi kullanabilirsiniz. Politika tabanlı VPN ağ geçitleri, her bir tünel üzerinden şifrelenmesi gereken paketlerin IP adreslerini statik olarak belirtir. Rota tabanlı ağ geçitlerinde, IPSec tünelleri bir ağ arayüzü veya sanal tünel arayüzü olarak modellenir.

#### High-Availability Scenarios

Bilgileri güvende tutmak için bir VPN yapılandırılıyorsa, bunun yüksek düzeyde kullanılabilir ve hata toleranslı bir VPN olduğundan emin olunmalıdır. VPN ağ geçidinin esnekliğini en üst düzeye çıkarmanın birkaç yolu vardır.

##### 2.2.7.2.1 Active/Standby

Varsayılan olarak, Azure’da yalnızca bir VPN ağ geçidi kaynağı görülse bile VPN ağ geçitleri etkin/yedek yapılandırmada iki örnek olarak dağıtılır. Planlı bakım veya planlanmamış kesinti etkin örneği etkilediğinde, yedek örnek herhangi bir kullanıcı müdahalesi olmadan bağlantıların sorumluluğunu otomatik olarak üstlenir.

##### 2.2.7.2.2 Active/Active

BGP yönlendirme protokolü desteğinin sunulmasıyla birlikte VPN ağ geçitlerini aktif/aktif yapılandırmada da dağıtabilirsiniz. Bu yapılandırmada, her örneğe benzersiz bir genel IP adresi atarsınız. Daha sonra şirket içi cihazdan her IP adresine ayrı tüneller oluşturursunuz. Şirket içinde ek bir VPN cihazı dağıtarak yüksek kullanılabilirliği genişletebilirsiniz.

##### 2.2.7.2.3 ExpressRoute Failover

ExpressRoute devreleri yerleşik esnekliğe sahiptir. Ancak, bağlantı sağlayan kabloları etkileyen fiziksel sorunlara veya ExpressRoute konumunun tamamını etkileyen kesintilere karşı bağışık değildirler. Bir ExpressRoute devresinin kesintiye uğramasıyla ilişkili risklerin olduğu yüksek kullanılabilirlik senaryolarında, alternatif bir bağlantı yöntemi olarak interneti kullanan bir VPN ağ geçidi de sağlayabilirsiniz. Bu şekilde, sanal ağlara her zaman bir bağlantı olmasını sağlayabilirsiniz.

##### 2.2.7.2.4 Zone-Redundant Gateways

Kullanılabilirlik bölgelerini destekleyen bölgelerde, VPN ağ geçitleri ve ExpressRoute ağ geçitleri bölge yedekli bir yapılandırmada dağıtılabilir. Bu yapılandırma, sanal ağ geçitlerine esneklik, ölçeklenebilirlik ve daha yüksek kullanılabilirlik sağlar. Ağ geçitlerini Azure kullanılabilirlik bölgelerinde dağıtmak, bir bölgedeki ağ geçitlerini fiziksel ve mantıksal olarak ayırırken Azure'a olan şirket içi ağ bağlantınızı bölge düzeyindeki arızalardan korur. Bu ağ geçitleri farklı ağ geçidi stok tutma birimleri (SKU'lar) gerektirir ve Temel genel IP adresleri yerine Standart genel IP adreslerini kullanır.

### Describe Azure ExpressRoute

Azure ExpressRoute, bir bağlantı sağlayıcısının yardımıyla şirket içi ağlarınızı özel bir bağlantı üzerinden Microsoft bulutuna genişletmenize olanak tanır. Bu bağlantıya ExpressRoute Devresi adı verilir. Bağlantı, herhangi birinden herhangi birine (IP VPN) ağdan, noktadan noktaya Ethernet ağından veya bir ortak yerleşim tesisindeki bir bağlantı sağlayıcısı aracılığıyla sanal bir çapraz bağlantıdan olabilir. ExpressRoute bağlantıları genel İnternet üzerinden gitmez. Bu, ExpressRoute bağlantılarının İnternet üzerinden tipik bağlantılara göre daha fazla güvenilirlik, daha yüksek hızlar, tutarlı gecikme süreleri ve daha yüksek güvenlik sunmasını sağlar. ExpressRoute kullanmanın çeşitli avantajları vardır;

* Jeopolitik bölgedeki tüm bölgelerde Microsoft bulut hizmetlerine bağlanabilirlik.
* ExpressRoute Global Reach ile tüm bölgelerde Microsoft hizmetlerine küresel bağlantı.
* Border Gateway Protocol (BGP) aracılığıyla ağınız ve Microsoft arasında dinamik yönlendirme.
* Daha yüksek güvenilirlik için her eşleme konumunda yerleşik yedeklilik.

ExpressRoute ile verileriniz genel internet üzerinden seyahat etmez, bu nedenle internet iletişimiyle ilişkili potansiyel risklere maruz kalmaz. ExpressRoute, şirket içi altyapınızdan Azure altyapınıza giden özel bir bağlantıdır. ExpressRoute bağlantınız olsa bile DNS sorguları, sertifika iptal listesi denetimi ve Azure Content Delivery Network istekleri yine de genel internet üzerinden gönderilir.

### Describe Azure DNS

Azure DNS, Microsoft Azure altyapısını kullanarak ad çözümlemesi sağlayan DNS etki alanları için bir barındırma hizmetidir. Etki alanlarınızı Azure'da barındırarak DNS kayıtlarınızı diğer Azure hizmetlerinizle aynı kimlik bilgilerini, API'leri, araçları ve faturalandırmayı kullanarak yönetebilirsiniz. Azure DNS’in birçok avantajı vardır;

* Güvenilirlik ve performans
* Güvenlik
* Kullanım Kolaylığı
* Özelleştirilebilir sanal ağlar
* Takma ad kayıtları

## 2.3 Describe Azure Storage Services

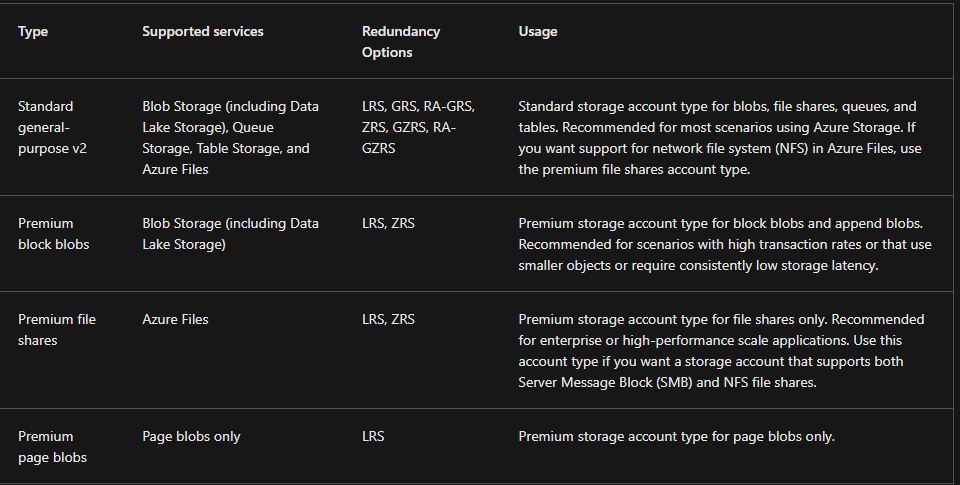
Farklı depolama türleri ve dağıtılmış bir altyapının verileri nasıl daha esnek hale getirebileceği gibi Azure’da depolamayı tanıtan modüldür. Modülün öğrenme hedefleri şunlardır;

* Azure depolama hizmetlerini karşılaştırma (Compare Azure storage services)
* Depolama katmanlarını tanımlama (Describe storage tiers)
* Yedeklilik seçeneklerini tanımlama (Describe redundancy options)
* Depolama hesabı seçeneklerini ve depolama türlerini tanımlama (Describe storage account options and storage types)
* AzCopy, Azure Depolama Gezgini ve Azure File Sync dahil olmak üzere dosya taşıma seçeneklerini tanımlama (Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync)
* Azure Geçişi ve Azure Data Box dahil olmak üzere geçiş seçeneklerini açıklama (Describe migration options, including Azure Migrate and Azure Data Box)

### 2.3.1 Describe Azure Storage Accounts

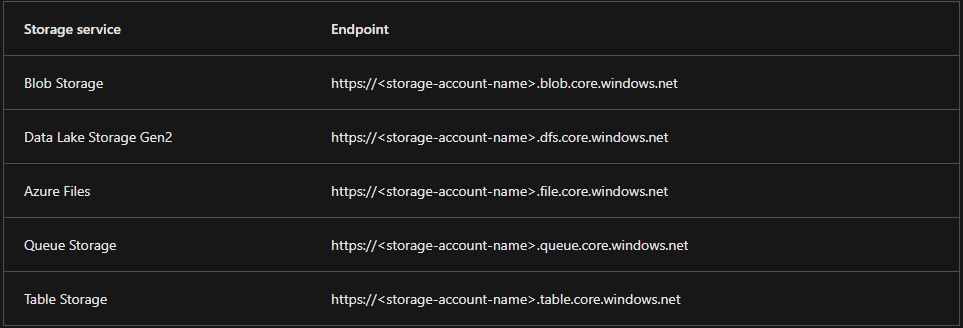
Bir depolama hesabı Azure depolama verileri için dünyanın her yerinden HTTP veya HTTPS üzerinden erişilebilen benzersiz bir ad alanı sağlar. Bu hesaptaki veriler güvenli, yüksek oranda kullanılabilir, dayanıklı ve büyük ölçüde ölçeklenebilirdir. Hesap türü, depolama hizmetlerini ve artıklık seçeneklerini belirler ve kullanım durumları üzerinde etkisi vardır. Aşağıda, bu modülün ilerleyen bölümlerinde ele alınacak olan yedeklilik seçeneklerinin bir listesi bulunmaktadır;

* Yerel olarak yedekli depolama (LRS)
* Coğrafi yedekli depolama (GRS)
* Okuma erişimli coğrafi yedekli depolama (RA-GRS)
* Bölge yedekli depolama (ZRS)
* Jeo-bölge-yedekli depolama (GZRS)
* Okuma erişimli coğrafi bölge yedekli depolama (RA-GZRS)



Azure depolama hesabı kullanmanın avantajlarından biri veriler için Azure’da benzersiz bir ad alanına sahip olmaktır. Bunu yapabilmek için Azure'daki her depolama hesabının Azure içinde benzersiz bir hesap adına sahip olması gerekir. Hesap adı ve Azure Depolama hizmeti uç noktasının birleşimi, depolama hesabınızın uç noktalarını oluşturur.

* Depolama hesabı adlarının uzunluğu 3 ila 24 karakter arasında olmalıdır ve yalnızca sayılar ve küçük harfler içerebilir.
* Depolama hesabı adınız Azure içinde benzersiz olmalıdır. İki depolama hesabı aynı ada sahip olamaz. Bu, Azure'da benzersiz, erişilebilir bir ad alanına sahip olma özelliğini destekler.
* Aşağıdaki tabloda Azure Depolama hizmetleri için uç nokta biçimi gösterilmektedir.



### 2.3.2 Describe Azure Storage Redundancy

Azure depolama, geçici donanım arızaları, ağ veya elektrik kesintileri ve doğal afetler gibi planlı ve plansız olaylardan korunmak için verilerinizin her zaman birden çok kopyasını depolar. Yedeklilik, depolama hesabınızın arızalar karşısında bile kullanılabilirlik ve dayanıklılık hedeflerini karşılamasını sağlar. Hangi yedekleme seçeneğini seçmeniz gerektiğini belirlemeye yardımcı olan faktörler şunlardır;

* Verilerinizin birincil bölgede nasıl çoğaltıldığı.
* Bölgesel felaketlere karşı koruma sağlamak için verilerinizin birincil bölgeye coğrafi olarak uzak olan ikinci bir bölgeye replike edilip edilmediği.
* Birincil bölgenin kullanılamaz hale gelmesi durumunda uygulamanızın ikincil bölgedeki çoğaltılmış verilere okuma erişimi gerektirip gerektirmediği.

#### 2.3.2.1 Redundancy in the Primary Region

Bir Azure Depolama hesabındaki veriler her zaman birincil bölgede üç kez çoğaltılır. Azure Depolama, verilerinizin birincil bölgede nasıl çoğaltılacağına ilişkin iki seçenek sunar:

* Yerel olarak yedekli depolama (LRS): Yerel olarak yedekli depolama (LRS), verilerinizi birincil bölgedeki tek bir veri merkezinde üç kez çoğaltır. LRS, belirli bir yıl boyunca nesneler için en az 11 dokuzluk dayanıklılık (%99,999999999) sağlar. LRS en düşük maliyetli yedekleme seçeneğidir ve diğer seçeneklere kıyasla en az dayanıklılığı sunar. LRS verilerinizi sunucu rafı ve sürücü arızalarına karşı korur. Ancak, veri merkezinde yangın veya sel gibi bir felaket meydana gelirse, LRS kullanan bir depolama hesabının tüm kopyaları kaybolabilir veya kurtarılamayabilir.
* Bölge olarak yedekli depolama (ZRS): Kullanılabilirlik Bölgesi özellikli Bölgeler için bölge yedekli depolama (ZRS), Azure Depolama verilerinizi birincil bölgedeki üç Azure kullanılabilirlik bölgesinde eşzamanlı olarak çoğaltır. ZRS, Azure Depolama veri nesneleri için belirli bir yıl boyunca en az 12 dokuz (%99,9999999999) dayanıklılık sunar. ZRS ile, bir bölge kullanılamaz hale gelse bile verilerinize hem okuma hem de yazma işlemleri için erişilebilir. Bağlı istemcilerden Azure dosya paylaşımlarının yeniden bağlanması gerekmez. Bir bölge kullanılamaz hale gelirse Azure, DNS yeniden atama gibi ağ güncelleştirmelerini üstlenir. Microsoft, yüksek kullanılabilirlik gerektiren senaryolar için birincil bölgede ZRS kullanılmasını önerir.

#### 2.3.2.2 Redundancy in a Secondary Region

Yüksek dayanıklılık gerektiren uygulamalar için, depolama hesabınızdaki verileri ek olarak birincil bölgeden yüzlerce kilometre uzaklıktaki ikincil bir bölgeye kopyalamayı seçebilirsiniz. Depolama hesabınızdaki veriler ikincil bir bölgeye kopyalanırsa, birincil bölgedeki verilerin kurtarılmasını engelleyen yıkıcı bir arıza durumunda bile verileriniz dayanıklı olur. Azure Depolama, verilerinizi ikincil bir bölgeye kopyalamak için iki seçenek sunar: coğrafi olarak yedekli depolama (GRS) ve coğrafi bölge olarak yedekli depolama (GZRS). GRS, LRS'yi iki bölgede çalıştırmaya benzer ve GZRS, ZRS'yi birincil bölgede ve LRS'yi ikincil bölgede çalıştırmaya benzer.

Coğrafi yedekli depolama (GRS veya GZRS ile), bölgesel kesintilere karşı koruma sağlamak için verilerinizi ikincil bölgedeki başka bir fiziksel konuma kopyalar. Ancak, bu veriler yalnızca müşteri veya Microsoft birincil bölgeden ikincil bölgeye bir yük devretme başlatırsa okunabilir.

### Describe Azure Storage Services

Azure Depolama platformu aşağıdaki veri hizmetlerini içerir:

* Azure Blobs: Metin ve ikili veriler için büyük ölçüde ölçeklenebilir bir nesne deposu. Ayrıca Data Lake Storage Gen2 aracılığıyla büyük veri analizi için destek içerir.
* Azure Files: Bulut veya şirket içi dağıtımlar için yönetilen dosya paylaşımları.
* Azure Queues: Uygulama bileşenleri arasında güvenilir mesajlaşma için bir mesajlaşma deposu.
* Azure Disks: Azure VM'leri için blok düzeyinde depolama birimleri.
* Azure Tables: Yapılandırılmış, ilişkisel olmayan veriler için NoSQL tablo seçeneği.

Azure Depolama hizmetleri, uygulama geliştiricileri ve BT uzmanları için aşağıdaki avantajları sunar:

* **Dayanıklı ve yüksek oranda kullanılabilir.** Yedeklilik, geçici donanım arızaları meydana geldiğinde verilerinizin güvende olmasını sağlar. Yerel felaketlere veya doğal afetlere karşı ek koruma sağlamak için verileri veri merkezleri veya coğrafi bölgeler arasında çoğaltmayı da tercih edebilirsiniz. Bu şekilde çoğaltılan veriler, beklenmedik bir kesinti meydana gelmesi durumunda yüksek oranda kullanılabilir kalır.
* **Güvenli.** Bir Azure depolama hesabına yazılan tüm veriler hizmet tarafından şifrelenir. Azure Depolama, verilerinize kimlerin erişebileceği konusunda size ayrıntılı denetim sağlar.
* **Ölçeklenebilir.** Azure Depolama, günümüz uygulamalarının veri depolama ve performans ihtiyaçlarını karşılamak için büyük ölçüde ölçeklenebilir olacak şekilde tasarlanmıştır.
* **Yönetilir.** Azure donanım bakımını, güncelleştirmeleri ve kritik sorunları sizin için yönetir.
* **Erişilebilir.** Azure Depolama'daki verilere dünyanın her yerinden HTTP veya HTTPS üzerinden erişilebilir. Microsoft, Azure Depolama için .NET, Java, Node.js, Python, PHP, Ruby, Go ve diğerleri dahil olmak üzere çeşitli dillerde istemci kitaplıklarının yanı sıra gelişmiş bir REST API sağlar. Azure Depolama, Azure PowerShell veya Azure CLI'da komut dosyası oluşturmayı destekler. Ayrıca Azure Portal ve Azure Depolama Gezgini, verilerinizle çalışmak için kolay görsel çözümler sunar.

#### 2.3.3.1 Azure Blobs

Azure Blob depolama, bulut için bir nesne depolama çözümüdür. Metin veya ikili veriler gibi büyük miktarda veri depolayabilir. Azure Blob depolama yapılandırılmamıştır, yani tutabileceği veri türlerinde herhangi bir kısıtlama yoktur. Blob depolama binlerce eşzamanlı yüklemeyi, büyük miktarda video verisini, sürekli büyüyen günlük dosyalarını yönetebilir ve internet bağlantısı olan her yerden erişilebilir. Blob depolama şunlar için idealdir:

* Görüntüleri veya belgeleri doğrudan bir tarayıcıya sunma.
* Dağıtılmış erişim için dosyaları depolama.
* Video ve ses akışı.
* Yedekleme ve geri yükleme, olağanüstü durum kurtarma ve arşivleme için veri depolama.
* Şirket içi veya Azure tarafından barındırılan bir hizmet tarafından analiz için veri depolama.

Bulutta depolanan veriler üstel bir hızla büyüyebilir. Genişleyen depolama ihtiyaçlarınızın maliyetlerini yönetmek için verilerinizi erişim sıklığı ve planlanan saklama süresi gibi özelliklere göre düzenlemek faydalı olacaktır. Azure Depolama, blob depolama alanınız için farklı erişim katmanları sunarak nesne verilerini en uygun maliyetli şekilde depolamanıza yardımcı olur. Kullanılabilir erişim katmanları şunları içerir:

* **Hot Access Tier:** Sık erişilen verileri depolamak için iyileştirilmiştir (örneğin, web siteniz için görüntüler).
* **Cool Access Tier:** Seyrek olarak erişilen ve en az 30 gün boyunca saklanan veriler için optimize edilmiştir (örneğin, müşterileriniz için faturalar).
* **Cold Access Tier:** Seyrek olarak erişilen ve en az 90 gün boyunca saklanan verileri depolamak için optimize edilmiştir.
* **Archive Access Tier:** Nadiren erişilen ve en az 180 gün boyunca depolanan, esnek gecikme süresi gereksinimleri olan veriler için uygundur (örneğin, uzun vadeli yedeklemeler).

#### 2.3.3.2 Azure Files

Azure Dosya depolama, bulutta endüstri standardı Sunucu İleti Bloğu (SMB) veya Ağ Dosya Sistemi (NFS) protokolleri aracılığıyla erişilebilen tam olarak yönetilen dosya paylaşımları sunar. Azure Files dosya paylaşımları, bulut veya şirket içi dağıtımlar tarafından eşzamanlı olarak bağlanabilir.

Azure Files temel avantajları:

* Paylaşılan erişim: Azure dosya paylaşımları endüstri standardı SMB ve NFS protokollerini destekler, yani uygulama uyumluluğu konusunda endişelenmeden şirket içi dosya paylaşımlarınızı sorunsuz bir şekilde Azure dosya paylaşımlarıyla değiştirebilirsiniz.
* Tam olarak yönetilir: Azure dosya paylaşımları, donanım veya işletim sistemi yönetmeye gerek kalmadan oluşturulabilir. Bu, sunucu işletim sistemine kritik güvenlik yükseltmeleri eklemek veya arızalı sabit diskleri değiştirmekle uğraşmak zorunda kalmayacağınız anlamına gelir.
* Komut dosyası oluşturma ve araçlar: PowerShell cmdlet'leri ve Azure CLI, Azure uygulamalarının yönetiminin bir parçası olarak Azure dosya paylaşımları oluşturmak, bağlamak ve yönetmek için kullanılabilir. Azure portal ve Azure Depolama Gezgini'ni kullanarak Azure dosya paylaşımları oluşturabilir ve yönetebilirsiniz.
* Esneklik: Azure Dosyaları, her zaman kullanılabilir olacak şekilde sıfırdan oluşturulmuştur. Şirket içi dosya paylaşımlarını Azure Dosyalar ile değiştirmek, yerel elektrik kesintileri veya ağ sorunlarıyla uğraşmak için gecenin bir yarısı uyanmak zorunda kalmayacağınız anlamına gelir.
* Tanıdık programlanabilirlik: Azure'da çalışan uygulamalar, paylaşımdaki verilere dosya sistemi I/O API'leri aracılığıyla erişebilir. Bu nedenle geliştiriciler, mevcut uygulamaları geçirmek için mevcut kodlarını ve becerilerini kullanabilir. Sistem IO API'lerine ek olarak Azure Depolama İstemci Kitaplıkları'nı veya Azure Depolama REST API'sini kullanabilirsiniz.

#### 2.3.3.3 Azure Queues

Azure Queue depolama, çok sayıda iletiyi depolamaya yönelik bir hizmettir. İletiler depolandıktan sonra, HTTP veya HTTPS kullanarak kimliği doğrulanmış çağrılar aracılığıyla dünyanın her yerinden bunlara erişebilirsiniz. Kuyruk depolama, bir ileti alındığında eylem gerçekleştirmek için Azure İşlevleri gibi işlem işlevleriyle birleştirilebilir. Örneğin, bir müşteri web sitenize bir form yükledikten sonra bir eylem gerçekleştirmek istiyorsunuz. Web sitesindeki gönder düğmesinin Kuyruk depolama alanına bir ileti tetiklemesini sağlayabilirsiniz. Ardından, ileti alındıktan sonra bir eylemi tetiklemek için Azure İşlevleri'ni kullanabilirsiniz.

#### 2.3.3.4 Azure Disks

Azure Disk depolama veya Azure tarafından yönetilen diskler, Azure VM'leriyle kullanılmak üzere Azure tarafından yönetilen blok düzeyinde depolama birimleridir. Kavramsal olarak fiziksel disklerle aynıdır ancak sanallaştırıldıkları için fiziksel disklere kıyasla daha fazla esneklik ve kullanılabilirlik sunarlar. Yönetilen disklerle tek yapmanız gereken diski sağlamaktır, gerisini Azure halleder.

#### 2.3.3.5 Azure Tables

Azure Tablo depolama, büyük miktarda yapılandırılmış veriyi depolar. Azure tabloları, Azure bulutunun içinden ve dışından kimliği doğrulanmış çağrıları kabul eden bir NoSQL veri deposudur. Bu sayede hibrit veya çoklu bulut çözümünüzü oluşturmak için Azure tablolarını kullanabilir ve verilerinizin her zaman kullanılabilir olmasını sağlayabilirsiniz. Azure tabloları yapılandırılmış, ilişkisel olmayan verileri depolamak için idealdir.

### Identify Azure Data Migration Options

Azure Geçişi, şirket içi ortamdan buluta geçiş yapmanıza yardımcı olan bir hizmettir. Azure Geçişi, şirket içi veri merkezinizin değerlendirmesini ve Azure'a geçişini yönetmenize yardımcı olan bir merkez işlevi görür. Aşağıdakileri sağlar:

* Birleşik geçiş platformu: Azure'a geçişinizi başlatmak, çalıştırmak ve izlemek için tek bir portal.
* Çeşitli araçlar: Değerlendirme ve geçiş için çeşitli araçlar. Azure Geçişi araçları Azure Geçişi'ni içerir: Keşif ve değerlendirme ve Azure Geçişi: Sunucu Geçişi. Azure Geçişi ayrıca diğer Azure hizmetleri ve araçlarıyla ve bağımsız yazılım satıcısı (ISV) teklifleriyle tümleştirilir.
* Değerlendirme ve geçiş: Azure Geçişi hub'ında, şirket içi altyapınızı değerlendirebilir ve Azure'a geçirebilirsiniz.

ISV'lerin araçlarıyla çalışmanın yanı sıra Azure Geçişi hub'ı, geçişe yardımcı olmak için aşağıdaki araçları da içerir:

* **Azure Migrate: Discovery and assessment**. Azure'a geçişe hazırlanmak için VMware, Hyper-V ve fiziksel sunucularda çalışan şirket içi sunucuları keşfedin ve değerlendirin.
* **Azure Migrate: Server Migration.** VMware VM'lerini, Hyper-V VM'lerini, fiziksel sunucuları, diğer sanallaştırılmış sunucuları ve genel bulut VM'lerini Azure'a geçirin.
* **Data Migration Assistant**. Data Migration Assistant, SQL Sunucularını değerlendirmek için bağımsız bir araçtır. Geçişi engelleyen olası sorunların belirlenmesine yardımcı olur. Desteklenmeyen özellikleri, geçişten sonra size fayda sağlayabilecek yeni özellikleri ve veritabanı geçişi için doğru yolu tanımlar.
* **Azure Database Migration Service**. Şirket içi veritabanlarını SQL Server, Azure SQL Veritabanı veya SQL Yönetilen Örnekleri çalıştıran Azure VM'lerine geçirin.
* **Azure App Service migration assistant.** Azure App Service geçiş yardımcısı, Azure App Service'e geçiş için şirket içi web sitelerini değerlendirmeye yönelik bağımsız bir araçtır. .NET ve PHP web uygulamalarını Azure'a geçirmek için Geçiş Yardımcısı'nı kullanın.
* **Azure Data Box.** Büyük miktarda çevrimdışı veriyi Azure'a taşımak için Azure Data Box ürünlerini kullanın.

#### Azure Data Box

Azure Data Box, büyük miktarda verinin hızlı, ucuz ve güvenilir bir şekilde aktarılmasına yardımcı olan bir fiziksel geçiş hizmetidir. Veri Kutusu, bölgesel bir taşıyıcı aracılığıyla veri merkezinize ve veri merkezinizden taşınır. Sağlam bir kılıf, Veri Kutusunu taşıma sırasında hasara karşı korur ve sabitler.

Data Box'ın Azure'a veri aktarmak için kullanılabileceği çeşitli senaryolar;

* Bir kerelik geçiş - büyük miktarda şirket içi veri Azure'a taşındığında.
* Çevrimiçi bir medya kitaplığı oluşturmak için bir medya kitaplığını çevrimdışı bantlardan Azure'a taşıma.
* VM grubunuzu, SQL sunucunuzu ve uygulamalarınızı Azure'a geçirme.
* HDInsight kullanarak derinlemesine analiz ve raporlama için geçmiş verileri Azure'a taşıma.
* İlk toplu aktarım - Data Box (tohum) kullanılarak ilk toplu aktarım yapıldığında ve ardından ağ üzerinden artımlı aktarımlar yapıldığında.
* Periyodik yüklemeler - periyodik olarak büyük miktarda veri üretildiğinde ve Azure'a taşınması gerektiğinde.

### Azure File Movement Options

Azure Geçişi ve Azure Veri Kutusu gibi hizmetleri kullanarak büyük ölçekli geçiş yapmanın yanı sıra Azure, tek tek dosyaları veya küçük dosya gruplarını taşımanıza veya bunlarla etkileşim kurmanıza yardımcı olmak için tasarlanmış araçlara da sahiptir. Bu araçlar arasında AzCopy, Azure Depolama Gezgini ve Azure Dosya Eşitleme yer alır.

* AzCopy: AzCopy, blobları veya dosyaları depolama hesabınıza veya hesabınızdan kopyalamak için kullanabileceğiniz bir komut satırı yardımcı programıdır. AzCopy ile dosya yükleyebilir, dosya indirebilir, depolama hesapları arasında dosya kopyalayabilir ve hatta dosyaları senkronize edebilirsiniz.
* Azure Storage Explorer: Azure Depolama Gezgini, Azure Depolama Hesabınızdaki dosyaları ve blobları yönetmek için grafiksel bir arabirim sağlayan bağımsız bir uygulamadır.
* Azure File Sync: Azure File Sync, dosya paylaşımlarınızı Azure Files'ta merkezileştirmenizi ve Windows dosya sunucusunun esnekliğini, performansını ve uyumluluğunu korumanızı sağlayan bir araçtır.

## 2.4 Describe Azure Identity, Access and Security

Azure ile kullanılabilen bazı yetkilendirme ve kimlik doğrulama yöntemlerini kapsayan bölümdür. Modülün öğrenme hedefleri şunlardır;

* Microsoft Entra ID ve Microsoft Entra Domain Services dahil olmak üzere Azure'daki dizin hizmetlerini tanımlama (Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services)
* Çoklu oturum açma (SSO), çok faktörlü kimlik doğrulama (MFA) ve parolasız dahil olmak üzere Azure'daki kimlik doğrulama yöntemlerini tanımlama (Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication (MFA), and passwordless)
* Azure'da dış kimlikleri ve konuk erişimini tanımlama (Describe external identities and guest access in Azure)
* Microsoft Entra Koşullu Erişim'i tanımlama (Describe Microsoft Entra Conditional Access)
* Azure Rol Tabanlı Erişim Denetimi'ni (RBAC) tanımlama (Describe Azure Role Based Access Control (RBAC))
* Sıfır Güven kavramını tanımlayın (Describe the concept of Zero Trust)
* Derinlemesine savunma modelinin amacını açıklayın (Describe the purpose of the defense in depth model)
* Bulut için Microsoft Defender'ın amacını açıklayın (Describe the purpose of Microsoft Defender for Cloud)

### 2.4.1 Describe Azure Directory Services

#### 2.4.1.1 Microsoft Entra ID

Microsoft Entra ID, hem Microsoft bulut uygulamalarında hem de kendi geliştirdiğiniz bulut uygulamalarında oturum açmanızı ve bunlara erişmenizi sağlayan bir dizin hizmetidir. Microsoft Entra ID, Microsoft'un bulut tabanlı kimlik ve erişim yönetimi hizmetidir. Microsoft Entra ID ile kimlik hesaplarını siz kontrol edersiniz, ancak Microsoft hizmetin küresel olarak kullanılabilir olmasını sağlar.

* BT yöneticileri. Yöneticiler, iş gereksinimlerine göre uygulamalara ve kaynaklara erişimi denetlemek için Microsoft Entra ID'yi kullanabilir.
* Uygulama geliştiricileri. Geliştiriciler, bir uygulamaya SSO işlevselliği eklemek veya bir uygulamanın kullanıcının mevcut kimlik bilgileriyle çalışmasını sağlamak gibi, oluşturdukları uygulamalara işlevsellik eklemek için standartlara dayalı bir yaklaşım sağlamak üzere Microsoft Entra ID'yi kullanabilir.
* Kullanıcılar. Kullanıcılar kimliklerini yönetebilir ve self servis parola sıfırlama gibi bakım işlemlerini gerçekleştirebilir.
* Çevrimiçi hizmet aboneleri. Microsoft 365, Microsoft Office 365, Azure ve Microsoft Dynamics CRM Online aboneleri, hesaplarında kimlik doğrulaması yapmak için Microsoft Entra ID'yi zaten kullanıyor.

Microsoft Entra ID aşağıdaki gibi hizmetler sağlar:

* Kimlik doğrulama: Bu, uygulamalara ve kaynaklara erişmek için kimlik doğrulamayı içerir. Ayrıca self servis parola sıfırlama, çok faktörlü kimlik doğrulama, özel bir yasaklı parola listesi ve akıllı kilitleme hizmetleri gibi işlevler sağlamayı da içerir.
* Çoklu oturum açma: Çoklu oturum açma (SSO), birden fazla uygulamaya erişmek için yalnızca bir kullanıcı adı ve bir parola hatırlamanızı sağlar. Bir kullanıcıya tek bir kimlik bağlanır ve bu da güvenlik modelini basitleştirir. Kullanıcılar rol değiştirdikçe veya bir kuruluştan ayrıldıkça, erişim değişiklikleri bu kimliğe bağlanır, bu da hesapları değiştirmek veya devre dışı bırakmak için gereken çabayı büyük ölçüde azaltır.

#### 2.4.1.2 Microsoft Entra Domain Services

Microsoft Entra Etki Alanı Hizmetleri, etki alanına katılma, grup ilkesi, hafif dizin erişim protokolü (LDAP) ve Kerberos/NTLM kimlik doğrulaması gibi yönetilen etki alanı hizmetleri sağlayan bir hizmettir. Microsoft Entra ID'nin, dizin hizmetlerini destekleyen altyapıyı sürdürmek zorunda kalmadan kullanmanıza izin vermesi gibi, Microsoft Entra Etki Alanı Hizmetleri ile bulutta etki alanı denetleyicileri (DC'ler) dağıtmaya, yönetmeye ve yamalamaya gerek kalmadan etki alanı hizmetlerinden faydalanabilirsiniz. Bir Microsoft Entra Domain Services yönetilen etki alanı oluşturduğunuzda, benzersiz bir ad alanı tanımlarsınız. Bu ad alanı, etki alanı adıdır. Daha sonra iki Windows Server etki alanı denetleyicisi seçtiğiniz Azure bölgesine dağıtılır. DC'lerin bu dağıtımı, çoğaltma kümesi olarak bilinir.

### 2.4.2 Describe Azure Authentication Methods

Kimlik doğrulama, bir kişinin, hizmetin veya cihazın kimliğini belirleme sürecidir. Kişinin, hizmetin veya cihazın kim olduğunu kanıtlamak için bir tür kimlik bilgisi sağlamasını gerektirir. Azure, standart parolalar, çoklu oturum açma (SSO), çok faktörlü kimlik doğrulama (MFA) ve parolasız kimlik doğrulama dahil olmak üzere birden fazla kimlik doğrulama yöntemini destekler. Aşağıdaki diyagramda güvenlik seviyesi ile kolaylık karşılaştırmalı olarak gösterilmektedir. Parolasız kimlik doğrulama yüksek güvenlik ve yüksek kolaylık sağlarken, parolaların tek başına düşük güvenlik ancak yüksek kolaylık sağladığına dikkat edin.

A diagram of a security system

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-azure-identity-access-security/media/passwordless-convenience-security-30321b4d.png>

#### 2.4.2.1 Single Sign-On

Çoklu oturum açma (single sign-on) (SSO) bir kullanıcının bir kez oturum açmasını ve bu kimlik bilgisini farklı sağlayıcılardan birden fazla kaynağa ve uygulamaya erişmek için kullanmasını sağlar. SSO'nun çalışması için farklı uygulamaların ve sağlayıcıların ilk kimlik doğrulayıcıya güvenmesi gerekir. Karmaşıklık gereksinimleri arttıkça, kullanıcıların bunları hatırlaması giderek zorlaşır. Bir kullanıcı ne kadar çok parolayı yönetmek zorunda kalırsa, kimlik bilgileriyle ilgili bir güvenlik olayı riski de o kadar artar. SSO ile yalnızca bir kimlik ve bir parola hatırlamanız gerekir. Uygulamalar arasında erişim, kullanıcıya bağlı tek bir kimliğe verilir ve bu da güvenlik modelini basitleştirir.

#### 2.4.2.2 Multifactor Authentication

Çok faktörlü kimlik doğrulama, oturum açma işlemi sırasında bir kullanıcıdan ekstra bir kimlik formu (veya faktörü) isteme işlemidir. MFA, parolanın ele geçirildiği ancak ikinci faktörün ele geçirilmediği durumlarda parolanın ele geçirilmesine karşı korunmaya yardımcı olur. Çok faktörlü kimlik doğrulama, tam kimlik doğrulaması için iki veya daha fazla unsur gerektirerek kimlikleriniz için ek güvenlik sağlar. Bu unsurlar üç kategoriye ayrılır:

* Kullanıcının bildiği bir şey - bu bir meydan okuma sorusu olabilir.
* Kullanıcının sahip olduğu bir şey - bu, kullanıcının cep telefonuna gönderilen bir kod olabilir.
* Kullanıcının olduğu bir şey - bu genellikle parmak izi veya yüz taraması gibi bir tür biyometrik özelliktir.

Çok faktörlü kimlik doğrulama, kimlik bilgilerinin açığa çıkmasının (örneğin, çalınan kullanıcı adları ve parolalar) etkisini sınırlandırarak kimlik güvenliğini artırır. Çok faktörlü kimlik doğrulama etkinleştirildiğinde, bir kullanıcının parolasına sahip olan bir saldırganın tam kimlik doğrulaması için telefonuna veya parmak izine de sahip olması gerekir.

#### 2.4.2.3 Passwordless Authentication

MFA gibi özellikler kuruluşunuzun güvenliğini sağlamak için harika bir yoldur, ancak kullanıcılar genellikle parolalarını hatırlamak zorunda kalmanın üzerine eklenen ek güvenlik katmanından rahatsız olurlar. Kullanıcılar, kolay ve rahat bir şekilde buna uymaya daha yatkındır. Parolasız kimlik doğrulama yöntemleri daha kullanışlıdır çünkü parola kaldırılır ve yerine sahip olduğunuz bir şey, olduğunuz bir şey veya bildiğiniz bir şey konur.

### 2.4.3 Describe Azure External Identities

Dış kimlik, kuruluşunuzun dışındaki bir kişi, cihaz, hizmet vb. anlamına gelir. Microsoft Entra Dış Kimlik, kurumunuz dışındaki kullanıcılarla güvenli bir şekilde etkileşim kurabileceğiniz tüm yolları ifade eder. İş ortakları, distribütörler, tedarikçiler veya satıcılarla işbirliği yapmak istiyorsanız kaynaklarınızı paylaşabilir ve dahili kullanıcılarınızın harici kuruluşlara nasıl erişebileceğini tanımlayabilirsiniz. Tüketiciye yönelik uygulamalar oluşturan bir geliştiriciyseniz, müşterilerinizin kimlik deneyimlerini yönetebilirsiniz. Aşağıdaki özellikler Dış Kimlikleri oluşturur:

* İşletmeler arası (B2B) işbirliği - Microsoft uygulamalarınızda veya diğer kurumsal uygulamalarda (SaaS uygulamaları, özel geliştirilmiş uygulamalar vb.) oturum açmak için tercih ettikleri kimliği kullanmalarına izin vererek dış kullanıcılarla işbirliği yapın. B2B işbirliği kullanıcıları, dizininizde genellikle konuk kullanıcılar olarak temsil edilir.
* B2B doğrudan bağlantı - Sorunsuz işbirliği için başka bir Microsoft Entra kuruluşuyla karşılıklı, iki yönlü bir güven oluşturun. B2B doğrudan bağlantı şu anda Teams paylaşılan kanallarını destekleyerek dış kullanıcıların kaynaklarınıza kendi Teams örneklerinden erişmesini sağlar. B2B doğrudan bağlantı kullanıcıları dizininizde temsil edilmez, ancak Teams paylaşılan kanalı içinden görülebilir ve Teams yönetim merkezi raporlarında izlenebilir.
* Microsoft Azure Active Directory işletmeden müşteriye (B2C) - Kimlik ve erişim yönetimi için Azure AD B2C'yi kullanırken tüketicilere ve müşterilere modern SaaS uygulamaları veya özel olarak geliştirilmiş uygulamalar (Microsoft uygulamaları hariç) yayımlayın.

Dış kuruluşlarla nasıl etkileşim kurmak istediğinize ve paylaşmanız gereken kaynak türlerine bağlı olarak, bu özelliklerin bir kombinasyonunu kullanabilirsiniz.

### 2.4.4 Describe Azure Conditional Access

Koşullu Erişim, Microsoft Entra ID'nin kimlik sinyallerine dayalı olarak kaynaklara erişime izin vermek (veya erişimi reddetmek) için kullandığı bir araçtır. Bu sinyaller kullanıcının kim olduğunu, kullanıcının nerede olduğunu ve kullanıcının hangi cihazdan erişim talep ettiğini içerir. Koşullu Erişim BT yöneticilerine yardımcı olur:

* Kullanıcıları her yerde ve her zaman üretken olmaları için güçlendirin.
* Kurumun varlıklarını korumak.

Koşullu Erişim ayrıca kullanıcılar için daha ayrıntılı birçok faktörlü kimlik doğrulama deneyimi sağlar. Örneğin, bir kullanıcı bilinen bir konumdaysa ikinci kimlik doğrulama faktörü için sorgulanmayabilir. Ancak, oturum açma sinyalleri olağandışıysa veya beklenmedik bir konumdaysa ikinci bir kimlik doğrulama faktörü için sorgulanabilir. Koşullu Erişim, aşağıdakileri yapmanız gerektiğinde kullanışlıdır:

* Talep edenin rolüne, konumuna veya ağına bağlı olarak bir uygulamaya erişmek için çok faktörlü kimlik doğrulama (MFA) gerektirir. Örneğin, yöneticiler için MFA gerektirebilir ancak normal kullanıcılar veya şirket ağınızın dışından bağlanan kişiler için MFA gerektirmeyebilirsiniz.
* Hizmetlere yalnızca onaylı istemci uygulamaları aracılığıyla erişim talep edin. Örneğin, hangi e-posta uygulamalarının e-posta hizmetinize bağlanabileceğini sınırlayabilirsiniz.
* Kullanıcıların uygulamanıza yalnızca yönetilen cihazlardan erişmesini zorunlu kılın. Yönetilen cihaz, güvenlik ve uyumluluk standartlarınızı karşılayan bir cihazdır.
* Bilinmeyen veya beklenmeyen konumlardan erişim gibi güvenilmeyen kaynaklardan erişimi engelleyin.

### 2.4.5 Describe Azure Role-Based Access Control

En az ayrıcalık ilkesi, yalnızca bir görevi tamamlamak için gereken düzeye kadar erişim izni vermeniz gerektiğini söyler. Bir depolama bloğuna yalnızca okuma erişimine ihtiyacınız varsa, o depolama bloğuna yalnızca okuma erişimi verilmelidir. Ancak, tüm bir ekip için bu düzeyde izinleri yönetmek sıkıcı olacaktır. Her birey için ayrıntılı erişim gereksinimlerini tanımlamak ve ardından yeni kaynaklar oluşturulduğunda veya ekibe yeni kişiler katıldığında erişim gereksinimlerini güncelleştirmek yerine Azure, Azure rol tabanlı erişim denetimi (Azure RBAC) aracılığıyla erişimi denetlemenize olanak tanır. Azure, bulut kaynakları için ortak erişim kurallarını tanımlayan yerleşik roller sağlar. Ayrıca kendi rollerinizi de tanımlayabilirsiniz. Her rol, o rolle ilgili ilişkili bir erişim izinleri kümesine sahiptir. Bireyleri veya grupları bir veya daha fazla role atadığınızda, ilişkili tüm erişim izinlerini alırlar.

A screenshot of a computer screen

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-azure-identity-access-security/media/role-based-access-scope-4b12a8f3.png>

### 2.4.6 Describe Zero Trust Model

Sıfır Güven, en kötü durum senaryosunu varsayan ve kaynakları bu beklentiyle koruyan bir güvenlik modelidir. Sıfır Güven, başlangıçta ihlali varsayar ve ardından her talebi kontrolsüz bir ağdan geliyormuş gibi doğrular. Bu yeni bilgi işlem dünyasını ele almak için Microsoft, aşağıdaki yol gösterici ilkelere dayanan Sıfır Güven güvenlik modelini şiddetle tavsiye etmektedir:

* Açıkça doğrulayın - Her zaman mevcut tüm veri noktalarına dayanarak kimlik doğrulama ve yetkilendirme yapın.
* En az ayrıcalıklı erişimi kullanın - Tam Zamanında ve Yeterince Erişim (JIT/JEA), risk tabanlı uyarlanabilir ilkeler ve veri koruması ile kullanıcı erişimini sınırlandırın.
* İhlali varsayın - Patlama yarıçapını en aza indirin ve erişimi bölümlere ayırın. Uçtan uca şifrelemeyi doğrulayın. Görünürlük elde etmek, tehdit tespitini yönlendirmek ve savunmaları iyileştirmek için analitiği kullanın.

A diagram of a cell with a lock and a padlock

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-azure-identity-access-security/media/zero-trust-cf9202be.png>

### 2.4.7 Describe Defense-in-Depth

Derinlemesine savunmanın amacı bilgiyi korumak ve erişim yetkisi olmayan kişiler tarafından çalınmasını önlemektir. Derinlemesine savunma stratejisi, verilere yetkisiz erişim elde etmeyi amaçlayan bir saldırının ilerlemesini yavaşlatmak için bir dizi mekanizma kullanır. Derinlemesine savunmayı, merkezde güvence altına alınacak veriler ve bu merkezi veri katmanını korumak için işlev gören diğer tüm katmanlar olmak üzere bir dizi katman olarak görselleştirebilirsiniz.

A diagram of a security system

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-azure-identity-access-security/media/defense-depth-486afc12.png>

Her katman koruma sağlar, böylece bir katman ihlal edilirse, daha fazla maruz kalmayı önlemek için sonraki bir katman zaten mevcuttur. Bu yaklaşım, tek bir koruma katmanına olan bağımlılığı ortadan kaldırır. Bir saldırıyı yavaşlatır ve güvenlik ekiplerinin otomatik ya da manuel olarak harekete geçebileceği uyarı bilgileri sağlar.

* Fiziksel güvenlik katmanı, veri merkezindeki bilgi işlem donanımını korumak için ilk savunma hattıdır.
* Kimlik ve erişim katmanı altyapıya erişimi ve değişiklik kontrolünü kontrol eder.
* Çevre katmanı, büyük ölçekli saldırıları kullanıcılar için bir hizmet reddine neden olmadan önce filtrelemek için dağıtılmış hizmet reddi (DDoS) korumasını kullanır.
* Ağ katmanı, segmentasyon ve erişim kontrolleri aracılığıyla kaynaklar arasındaki iletişimi sınırlar.
* Hesaplama katmanı sanal makinelere erişimi güvence altına alır.
* Uygulama katmanı, uygulamaların güvenli ve güvenlik açıklarından arındırılmış olmasını sağlamaya yardımcı olur.
* Veri katmanı, korumanız gereken iş ve müşteri verilerine erişimi kontrol eder.
* Bu katmanlar, uygulamalarınızın tüm katmanlarında güvenlik yapılandırma kararları almanıza yardımcı olacak bir kılavuz sağlar.

### 2.4.8 Describe Microsoft Defender for Cloud

Defender for Cloud, güvenlik duruşu yönetimi ve tehdit koruması için bir izleme aracıdır. Güvenlik duruşunuzu güçlendirmeye yönelik rehberlik ve bildirimler sağlamak için bulut, şirket içi, hibrit ve çoklu bulut ortamlarınızı izler. Bulut için Defender Azure'a özgü bir hizmet olduğundan, birçok Azure hizmeti herhangi bir dağıtıma gerek kalmadan izlenir ve korunur. Ancak, şirket içi veri merkeziniz varsa veya başka bir bulut ortamında da çalışıyorsanız, Azure hizmetlerinin izlenmesi güvenlik durumunuzun tam bir resmini vermeyebilir. Bulut için Defender tüm tehditleri tespit etmenize yardımcı olur:

* Azure PaaS hizmetleri - Azure App Service, Azure SQL, Azure Storage Account ve daha fazla veri hizmeti dahil olmak üzere Azure hizmetlerini hedef alan tehditleri tespit edin. Ayrıca Bulut Uygulamaları için Microsoft Defender (eski adıyla Microsoft Cloud App Security) ile yerel tümleştirmeyi kullanarak Azure etkinlik günlüklerinizde anomali algılama gerçekleştirebilirsiniz.
* Azure veri hizmetleri - Bulut için Defender, Azure SQL'deki verilerinizi otomatik olarak sınıflandırmanıza yardımcı olan özellikler içerir. Ayrıca Azure SQL ve Depolama hizmetlerindeki olası güvenlik açıkları için değerlendirmeler ve bunların nasıl azaltılacağına ilişkin öneriler alabilirsiniz.
* Ağlar - Defender for Cloud, kaba kuvvet saldırılarına maruz kalmayı sınırlamanıza yardımcı olur. Sanal makine bağlantı noktalarına erişimi azaltarak, tam zamanında VM erişimini kullanarak, gereksiz erişimi önleyerek ağınızı sağlamlaştırabilirsiniz. Seçilen bağlantı noktalarında, yalnızca yetkili kullanıcılar için, izin verilen kaynak IP adresi aralıkları veya IP adresleri için ve sınırlı bir süre için güvenli erişim ilkeleri belirleyebilirsiniz.

Azure ortamınızı savunmanın yanı sıra, Azure olmayan sunucularınızı korumak için hibrit bulut ortamınıza Bulut için Defender özelliklerini ekleyebilirsiniz. En önemli konulara odaklanmanıza yardımcı olmak için özelleştirilmiş tehdit istihbaratı ve özel ortamınıza göre önceliklendirilmiş uyarılar alırsınız.

Bulut için Defender, buluttaki ve şirket içindeki kaynaklarınızın ve iş yüklerinizin güvenliğini yönetirken üç hayati ihtiyacı karşılar:

* Sürekli değerlendirme - Güvenlik duruşunuzu bilin. Güvenlik açıklarını belirleyin ve izleyin.
* Güvenli hale getirin - Azure Security Benchmark ile kaynakları ve hizmetleri güçlendirin.
* Savunun - Kaynaklara, iş yüklerine ve hizmetlere yönelik tehditleri tespit edin ve çözün.

A green square with white text

Description automatically generated

<https://learn.microsoft.com/en-us/training/wwl-azure/describe-azure-identity-access-security/media/assess-secure-defend-46228306.png>