

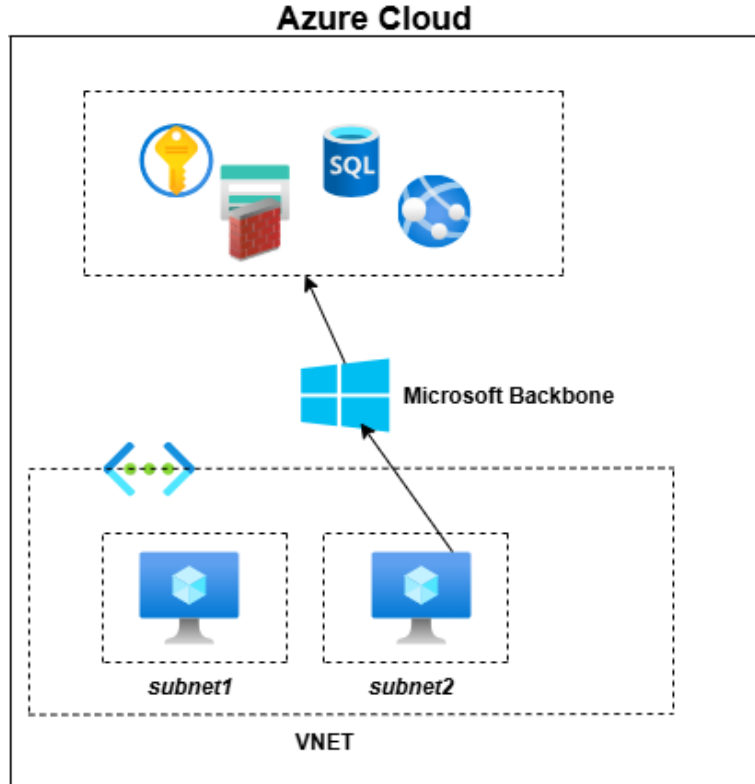
Azure Service Endpoint Kavramı ve Dağıtımı

Azure Service Endpoint yani **Hizmet Uç Noktaları** olarak anılmaktadır.

Service Endpoint'ler Ortamımızdaki virtual network'lerimizdeki kaynaklarımızın Azure servislerine güvenli ve özel erişim sağlamak için kullanılmaktadır. Bir anlama bu servislere erişim için güvenli ve özel erişim sağlayabilmek hedefiyle custom route yani özel bir rota oluşturmuş oluyoruz. Virtual Network'e bağlı olan kaynaklarımızdan inbound yani gelen trafik , herkese açık olmayan sadece bizim erişimimizi sağlayan daha güvenli özel Microsoft Backbone'larından geçmektedir. Azure Cloud ortamında her servisiniz dışarıya açık olmak zorunda değildir. Kurumsal ortamda zaten normal şartlar altında bu mümkün olmamaktadır. Genellikle kritik servislerimizi internete dış dünyaya açmamamız önerilmektedir yada bunu sınırlandırmamız istenebilmektedir. Bu sayede üst düzey ve servislerimizin iletişimini internete dışarıya çıkarmadan güvenli ve özel iletişim kurmasını sağlayabiliriz. Bir de Firewall yani Güvenlik Duvarı da işin içine girdiğinde daha çok secure connection dediğimiz güvenli bir bağlantı oluşacaktır.

Bu servisi özetleyecek bir diyagram çizdim. Bu diyagram içerisinde Azure Cloud ortamındaki servislerim ve kaynaklarım mevcut. Fakat genelde Azure Key Vault , Storage Account yada App Servis gibi Azure hizmetlerini test veya geliştirme ortamı şeklinde dışarıya açmayı tercih edebiliriz. Fakat canlı ortamda tutacağımız veriler kritik olduğundan dolayı bunları güvenli ve internete çıkmadan azure servisleriyle birbirleriyle haberleştirmem gerekiyor pek tabikide. Bunu da en iyi gerçekleştireceğim Servis ise Service Endpoint....

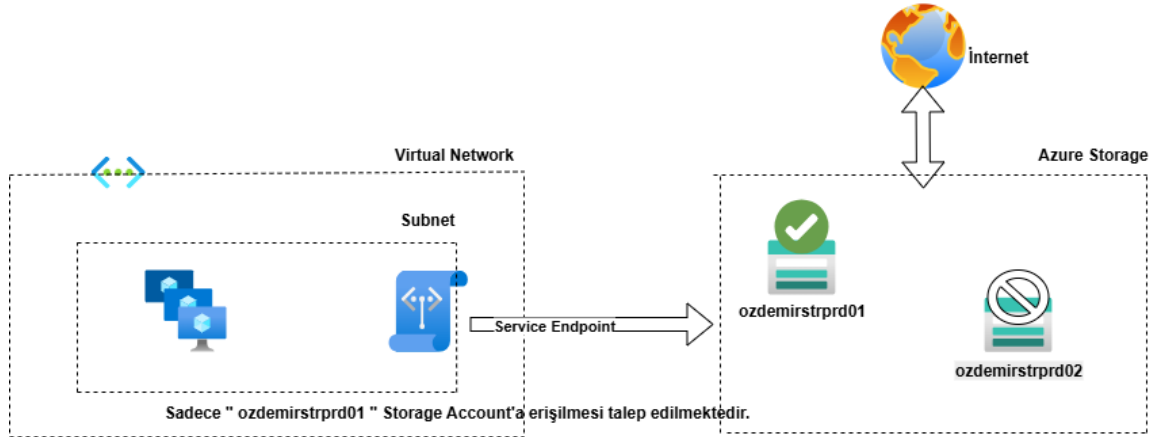
Diyagramda da gösterildiği gibi ben bunları prod bir ortamda internete dış dünyaya çıkmadan haberleştirmek istiyorsam böyle bir mimaride ilerlemem şarttır. Aynı vnet'te olan Azure Sanal Makineleri ayrı ayrı subnet'e ayırarak ; bir subnet'i farklı ortama diğer subnet'i ise Microsoft Backbone aracılığıyla birebir servislere erişecek şekilde özel bir rotadan haberleştirebilirim ve güvenli hale getirebilirim.



Service Endpoint'i nasıl tanıyacağız ? Tabiki de uygulayarak ve yaptığımız işlemleri adım adım sizlere anlatarak.... Peki ne yapacağız ?

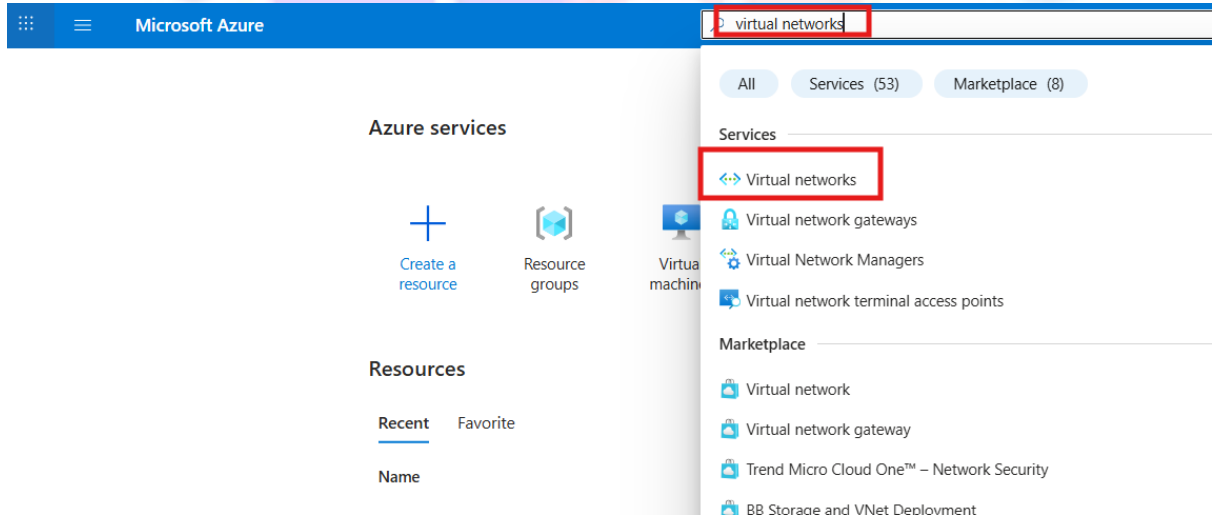
Bu uygulamada ;

- 2 Adet Azure VM
- 2 Adet Storage Account (Birisine erişim gerçekleştirilir. Birisine erişim yapılması istenmemektedir. Burada servisi daha iyi tanıyabilmemiz için Diğerine erişim Service Endpoint ile dışarıya açık olmamasını sağlamak yani erişimi kısıtlamak)
- 1 Virtual Network- 2 Subnet (Private – Public)
- 1 Service Endpoint

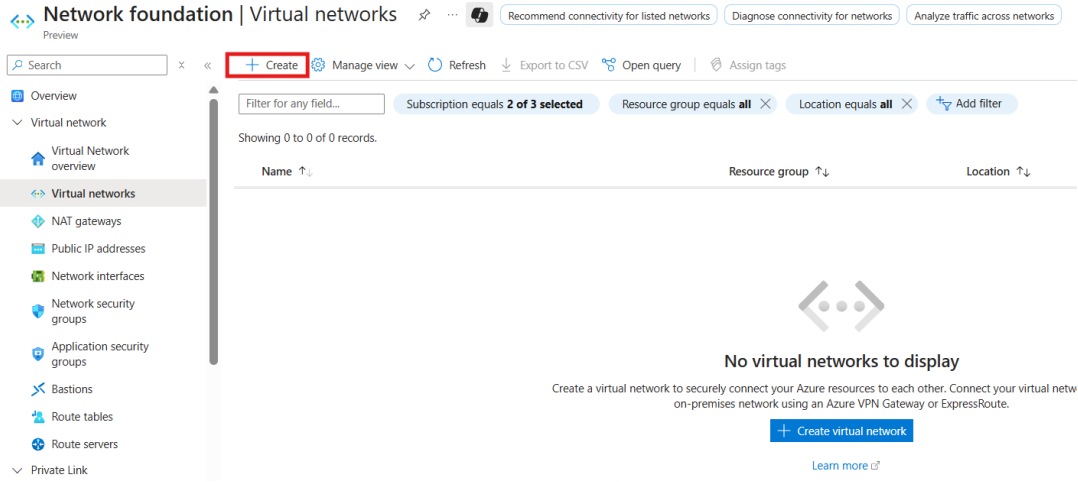


Azure Portal'da bu servisi oluşturmaya ve deneyimleye başlayalım. Haydi 😊

İlk öncelik klasik olarak; Azure Portala giriş yapıyoruz. Ardından arama kutucuğuna “ **Virtual Networks** ” yazarız.



“ Virtual Network ” dağıtımını gerçekleştirmek için “ Create ” seçeneğini seçeriz.



“ Basics ” bölümünde kaynağımızı dağıtmak istediğimiz “ Resource Group ” seçeriz. Eğer ortamınızda Resource Group mevcut değilse “ Create new ” seçeneğini seçerek dağıtım işlemi gerçekleştirebilirsiniz. Var olan Private adındaki Resource Group seçimimi gerçekleştirdim.

“ Virtual Network Name ” olarak “ Prod-coreServicesVNET ” isimlendirmesi gerçekleştiririz.

“ Region ” seçimi olarak “ East US ” bölgesini seçeriz. Ardından “ Next : Security ” seçeneğini seçerek bir sonraki adıma devam ederiz.

Create virtual network ...

Basics Security IP addresses Tags Review + create

Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Visual Studio Enterprise Aboneliği

Resource group * Private

Create new

Instance details

Virtual network name * Prod-CoreServicesVNET

Region * (US) East US

Deploy to an Azure Extended Zone

Previous Next : Security Review + create

“ **Security** ” adımımda herhangi bir özellik ihtiyacım olmadığı içi seçim ve aktifleştirme işlemi gerçekleştirmeyeceğiz. “ **Next : IP addresses** ” seçeneğini seçerek devam ederiz.

Create virtual network ...

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

Enhance the security of your virtual network with these additional paid security services. [Learn more](#)

Virtual network encryption

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more](#)

Virtual network encryption ☐

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more](#)

Enable Azure Bastion ☐

Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. [Learn more](#)

[Previous](#) **Next : IP addresses** [Review + create](#)

Ortamanızdaki IP Adres Havuzuna göre de yapılandırma yapabilirsiniz. Ben varolan varsayılan olan adres havuzundan ilerliyorum. “ **Subnets** ” bölümündeki “ **default** ” isminde olan Subnet’i erişim yapılacak şekilde public ve bir subnet daha konfigüre ederek onuda private olarak isimlendireceğiz.

Create virtual network ...

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

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

☐ Allocate using IP address pools. [Learn more](#)

+ Add a subnet

10.0.0.0/16 [Delete address space](#)

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

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

“Name” değerini Public olarak değiştiririz. Ardından “Save” seçeneğini seçeriz.

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose ⓘ Default

Name * ⓘ Public

IPv4

Include an IPv4 address space ☒

IPv4 address range ⓘ 10.0.0.0/16
10.0.0.0 - 10.0.255.255

Starting address * ⓘ 10.0.0.0

Size ⓘ /24 (256 addresses)

Subnet address range ⓘ 10.0.0.0 - 10.0.0.255

IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Save Cancel [Give feedback](#)

“Review + create” seçeneğini seçerek Virtual Network dağıtımına devam ederiz.

Create virtual network

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

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

☐ Allocate using IP address pools. [Learn more](#)

+ Add a subnet

10.0.0.0/16 [Delete address space](#)

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
Public	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

Add IPv4 address space

Previous Next : Tags Review + create

Dağıtım doğrulandı. “Create” seçeneğini seçerek kaynak dağıtımına başlarız.

Create virtual network ...

Validation passed

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription

Visual Studio Enterprise Aboneliği

Resource Group

Private

Name

Prod-CoreServicesVNET

Region

East US

Security

Azure Bastion

Disabled

Azure Firewall

Disabled

Azure DDoS Network Protection

Disabled

IP addresses

Address space

10.0.0.0/16 (65,536 addresses)

Subnet

Public (10.0.0.0/24) (256 addresses)

Previous

Next

Create

[Download a template for automation](#)

Dağıtım gerçekleştirilme aşamasındadır.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home >

Prod-CoreServicesVNET-1755003709323 | Overview

Deployment

Search

Delete

Cancel

Redeploy

Download

Refresh

Overview

Inputs

Outputs

Template

Deployment is in progress

Deployment name : Prod-CoreServicesVNET-1755003709323

Subscription : Visual Studio Enterprise Aboneliği

Resource group : Private

Start time : 8/12/2025, 4:01:55 PM

Correlation ID : d98cf4ee-02df-4a8a-b2c4-645b83bb2a42

Deployment details

Resource	Type	Status	Operation details
Prod-CoreServicesVNET	Virtual network	OK	Operation details

Give feedback

[Tell us about your experience with deployment](#)

Virtual Network dağıtımımız gerçekleştirildi.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home >

Prod-CoreServicesVNET-1755003709323 | Overview

Deployment

Search

Delete

Cancel

Redeploy

Download

Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name : Prod-CoreServicesVNET-1755003709323

Subscription : Visual Studio Enterprise Aboneliği

Resource group : Private

Start time : 8/12/2025, 4:01:56 PM

Correlation ID : d98cf4ee-02df-4a8a-b2c4-645b83bb2a42

Deployment details

Next steps

Go to resource

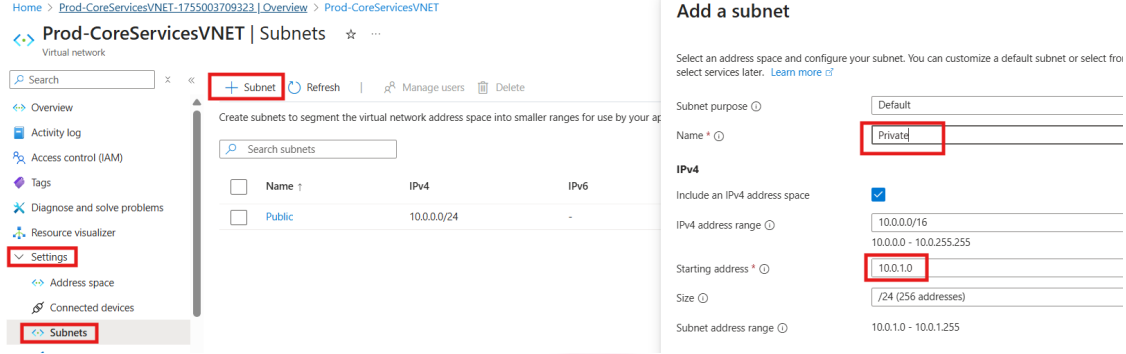
Give feedback

[Tell us about your experience with deployment](#)

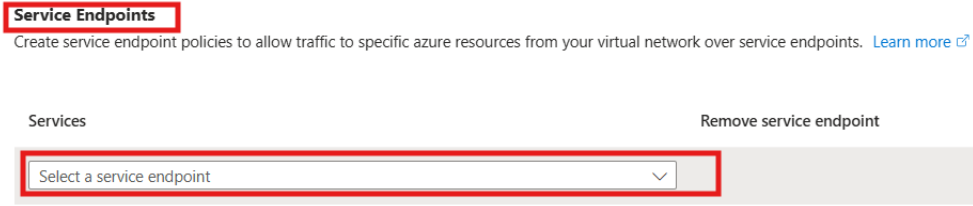
VNet dağıtma işlemi gerçekleştirdikten sonra sıra geldi Service Endpoint dağıtımını gerçekleştirmemiz gerekmektedir. Şimdi ilk olarak dağıtmış olduğumuz Virtual Network'e girerek

“ **Settings** ” adından “ **Subnets** ” seçeneğini seçerek Service Endpoint aktifleştireceğimiz “ **Private** ” adında farklı bir subnet ekleyeceğiz.

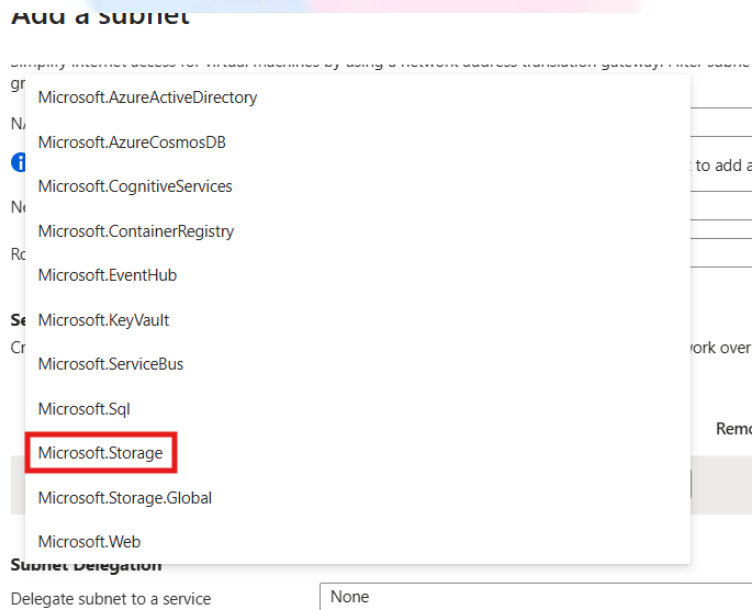
“ **Settings** ” altından “ **Subnets** ” seçeneğini seçeriz. “ **Name** ” kısmına “ **Private** ” yazarak “ **Starting address** ” kısmına Public adındaki Subnet'ten farklı bir ip adres tanımı yapılır.



Biraz aşağı indikten sonra ; “ **Service Endpoint** ” bölümünden “ **Services** ” seçeneğinde seçmiş olduğunuz servis ile Virtual Network'ten Service Endpoint üzerinden belirli Azure kaynaklarına trafiği izin vermek için servis seçimi yapmamızı istemektedir.



“ **Select a service endpoint** ” seçeneğini seçeriz. Ardından bu projemiz özelinde “ **Microsoft.Storage** ” seçeneğini seçeriz.



Services bölümüne eklendiğini gördük. “Add” seçeneğini seçeriz.

Add a subnet

Network security group ⓘ

None

Route table

None

Service Endpoints
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services

Remove service endpoint

Microsoft.Storage

Select a service endpoint

Service endpoint policies

None

Policy

Status

No service endpoint policies selected

Subnet Delegation
Delegate subnet to a service

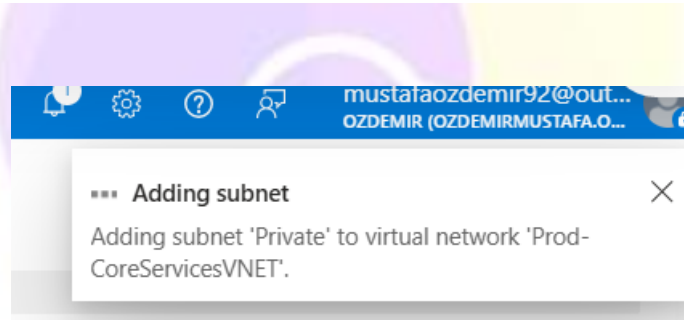
None

Add

Cancel

Give feedback

Subnet ekleniyor.



Public ve Private şeklinde Subnet oluşturma işlemlerini gerçekleştirdik.

Prod-CoreServicesVNET | Subnets

Virtual network

Search

+ Subnet Refresh Manage users Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Address space

Connected devices

Subnets

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

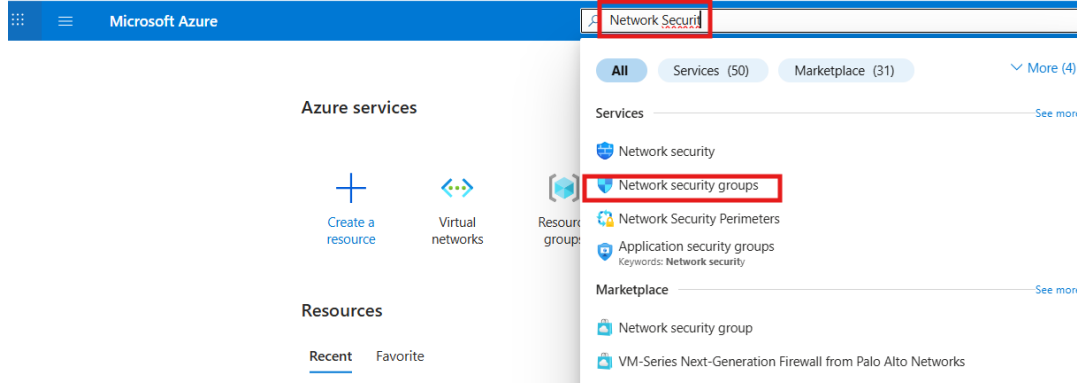
Search subnets

	Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
<input type="checkbox"/>	Public	10.0.0.0/24	-	251	-	-	-
<input type="checkbox"/>	Private	10.0.1.0/24	-	251	-	-	-

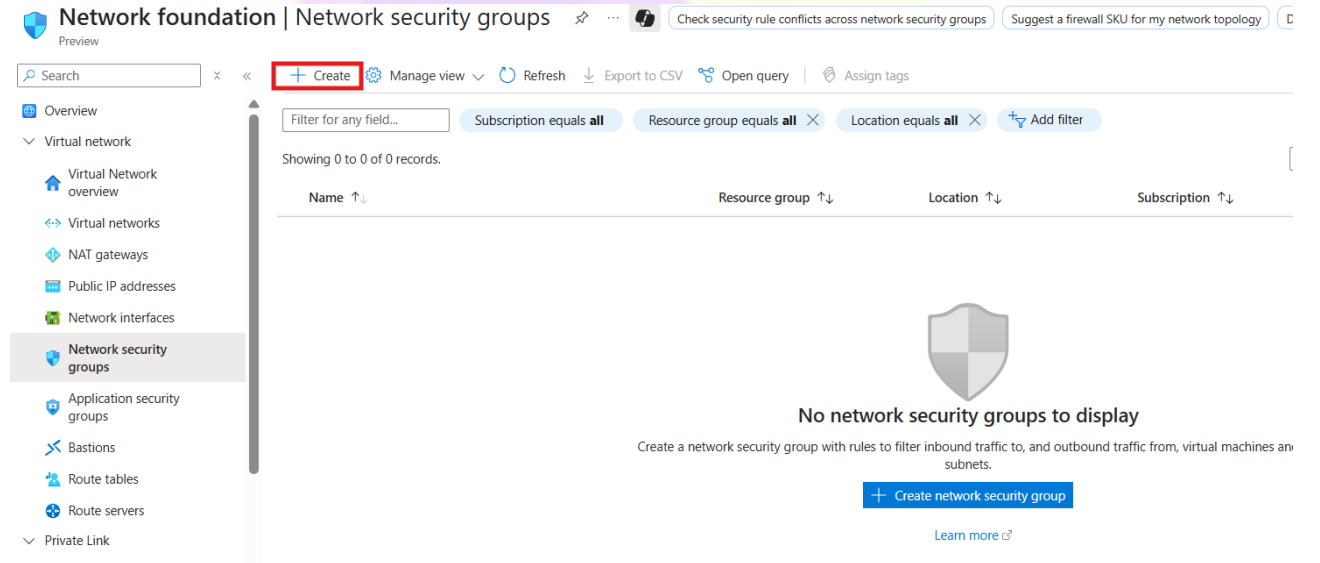
Şimdi sırada Bir Subnet'i network erişimini kısıtlama işlemini gerçekleştirmek. Haydi Ona da hemen başlayalım 😊 Normalde Subnet'lerdeki tüm Azure Sanal Makineler tüm kaynaklarla iletişim kurabilir. Projeye göre iletişim kurmasını istemiyorum. Bunu kısıtlayabilmek için **“ Network Security Group ”** dağıtımı gerçekleştirerek , Bunu Subnet'e associate yani atama yaparak bir subnet'teki tüm kaynaklarla iletişimi sınırlandıracağız.

Haydi Network Security Group oluşturalım :

Yeniden arama kısmına **“ Network Security Group ”** olarak servis aratırız.



NSG dağıtmak için **“ Create ”** seçeneğini seçeriz.



Önceden dağıtmış olduğumuz Private adındaki Resource Group'a dağıtım gerçekleştiriyoruz. “ **Name** ” bölümüne NSG'yi hatırlayabileceğim isimlendirme gerçekleştiriyor. Bölge seçimini de gerçekleştirdikten sonra NSG Dağıtımlarına başlarız. “ **Review + Create** ” seçeneğini seçeriz.

Create network security group ...

Basics Tags Review + create

Project details

Subscription *

Visual Studio Enterprise Aboneliği

Resource group *

Private

Create new

Instance details

Name *

ProdPrivateNSG

✓

Region *

East US

✓

Review + create

< Previous

Next : Tags >

[Download a template for automation](#)

“ **Create** ” seçeneğini seçeriz.

Create network security group ...

✓ Validation passed

Basics Tags **Review + create**

Basics

Subscription

Visual Studio Enterprise Aboneliği

Resource group

Private

Region

East US

name

ProdPrivateNSG

Tags

None

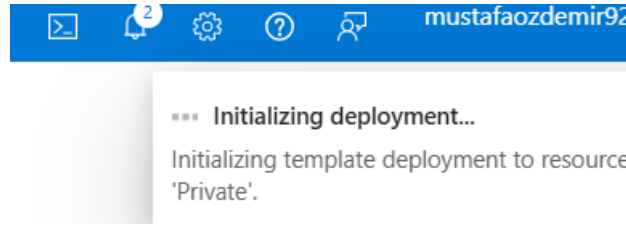
Create

< Previous

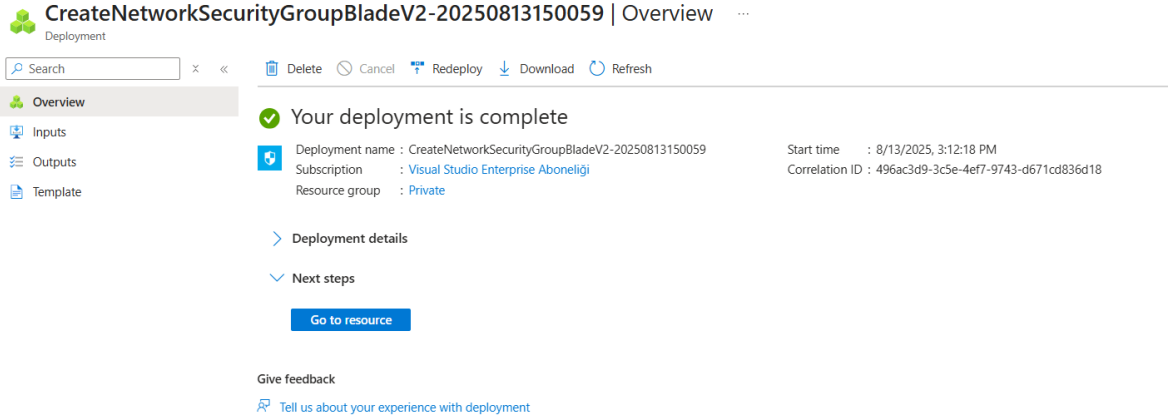
Next >

[Download a template for automation](#)

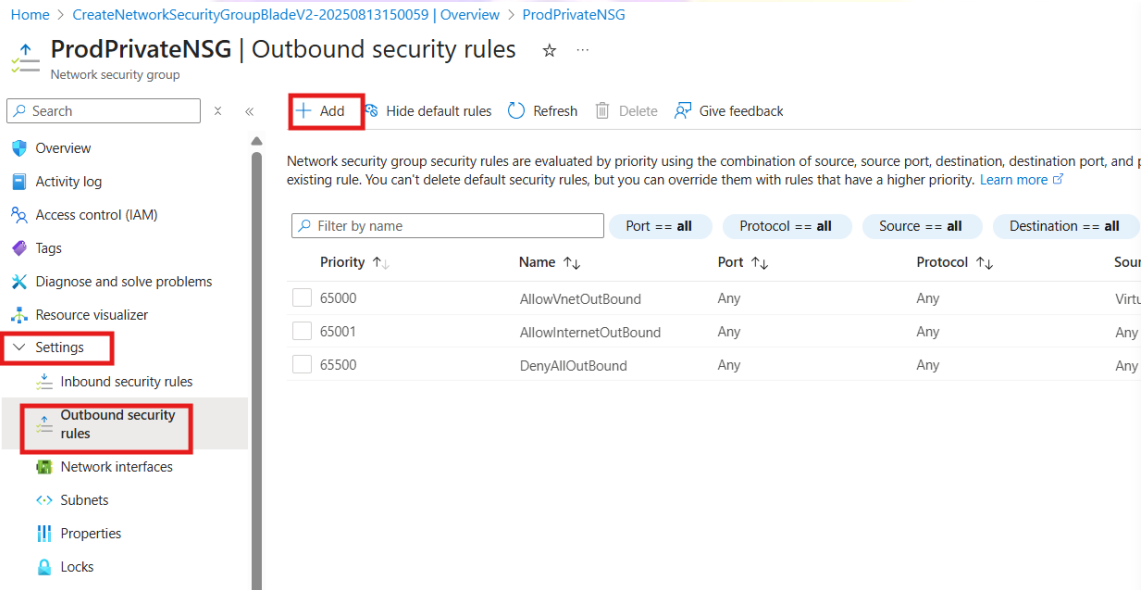
Dağıtım işlemi başladı.



NSG Dağıtım işlemi tamamlandı.



NSG dağıtımını gerçekleştirildi. “Settings” bölümü altından “Outbound Security Rules” seçeneğini seçerek kural oluşturmak için “Add” seçeneğini seçeriz.



“ **Source** ” bölümünde kaynak bölümünde hangi kaynaktan gelecek trafiği “ **IP Address Service vb.** ” bazda yapılandırma yapıyoruz. “ **Source Port Ranges** ” bölümünde kaynak kapsamına alınacak IP Aralığı yazılır yada bir aralık belirtilmek istenmiyorsa “ * ” şeklinde tanımlanır.

“ **Destination** ” bölümünde “ **Service tag** ” seçilir. Hedef servis olarak “ **Storage** ” seçeriz. “ **Destination Port Ranges** ” için yine “ * ” tanımlaması yaparız. “ **Protocol** ” Any tanımlaması yaparız. “ **Action** ” olarak bu kurala “ **Allow** ” yani izin vereceğim.

Add outbound security rule
ProdPrivateNSG

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Service Tag

Destination service tag ⓘ
Storage

Service ⓘ
Custom

Destination port ranges * ⓘ
*

Protocol
☒ Any
☐ TCP
☐ UDP
☐ ICMPv4
☐ ICMPv6

Action
☒ Allow
☐ Deny

Add Cancel Give feedt

“ **Priority** ” seçeneğinde ise belirli bir sayı veririz. Bu sayı kuralın önceliklendireceğini belirlemektedir. “ **Name** ” seçeneğinde ise kuralı neden yazdığım ve kural isimlendirmesi gerçekleştiriyorum. Ardından “ **Add** ” seçeneğini seçeriz.

Priority * ⓘ
100

Name *
Allow-Storage-All

Description

Add Cancel Give feedback

Kuralı eklemiş oluruz.

oupBladeV2-20250813150059 | Overview > ProdPrivateNSG

| Outbound security rules ☆ ...

<< + Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
<input checked="" type="checkbox"/> 100	Allow-Storage-All	Any	Any	Any	Storage	✓ Allow
<input type="checkbox"/> 65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
<input type="checkbox"/> 65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
<input type="checkbox"/> 65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

✓ Created security rule

Successfully created security rule 'Allow-Storage-A

Yeni bir kural daha oluşturuyoruz. Bu yeni oluşturacağımız kural ise internete iletişimi engellemek içindir. Bu kural herhangi bir trafiği internete çıkarmamaktadır.



Add outbound security rule

ProdPrivateNSG

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Service Tag

Destination service tag ⓘ

Internet

Service ⓘ

Custom

Destination port ranges * ⓘ

*

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMPv4

☐ ICMPv6

Action

☐ Allow

☒ Deny

Add

Cancel

Give

Priority * ⓘ
110

Name *
Deny-Internet-All ✓

Description

Add Cancel

Give feedback

Kuralları oluşturun. “Add” seçeneğini seçeriz.

ProdPrivateNSG | Outbound security rules ☆ ...

Network security group

Search x << + Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	Allow-Storage-All	Any	Any	Any	Storage	Allow
110	Deny-Internet-All	Any	Any	Any	Internet	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Şimdi 2 adet NSG Kuralı oluşturmuş olduk.

100 Priority değerine sahip kuralda Depolama alanına iletişim izni vermek için kullanılacaktır.

110 Priority değerine sahip kuralda her türlü internet erişimini reddetmek için kullanılacaktır.

Şimdi geldik Makinelerimize erişim için “Inbound Rule” yapılandırmak rule olarak “RDP” izni veriyoruz. “Settings” bölümü altından “Inbound Security Rules” seçeneğini seçerek “Add” seçeneği ile kural ekleme işlemini gerçekleştiriyoruz.

Microsoft Azure

Home > CreateNetworkSecurityGroupBladeV2-20250813150059 | Overview > ProdPrivateNSG

ProdPrivateNSG | Inbound security rules ☆ ...

Network security group


Search x << + Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of : existing rule. You can't delete default security rules, but you can override them with rules

Filter by name Port == all Protocol ==

Priority ↑↓	Name ↑↓	Port ↑↓
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBalancerInBo...	Any
65500	DenyAllInBound	Any

“ Destination port ranges ” ile “ 3389 ” girişı yaparız.

 **Add inbound security rule**
ProdPrivateNSG

Source ⓘ

Source port ranges * ⓘ

Destination ⓘ

Service ⓘ

Destination port ranges * ⓘ

Protocol
☒ Any
☐ TCP
☐ UDP
☐ ICMPv4
☐ ICMPv6

Action
☒ Allow
☐ Deny

Priority * ⓘ


Name veriyoruz. Ardından “ Add ” seçeneğini seçeriz.

Action
☒ Allow
☐ Deny

Priority * ⓘ
 ✓

Name *
 ✓

Description

 [Give feedback](#)

Inbound Rule ekleme işlemi tamamlandı.

ProdPrivateNSG | Inbound security rules

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
120	RDP-Allow-Rule	3389	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

İşlemler için gerekli kuralları oluşturduğumuza göre gidip bu kuralı Subnet'e atayalım. Bunun için Subnet'e atama işlemi gerçekleştiririz. Bu atama işlemi için ilgili NSG'den "Settings" bölümünden "Subnet" seçeneğini seçerek "Associate" seçeneğini seçeriz.

ProdPrivateNSG | Subnets

Network security group

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties

Associate

Search subnets

Name	Address range
No results.	

Kuralları atayacağımız Virtual Network'ü seçeriz. “ **Subnet** ” bölümünde ise “ **Private** ” seçeneğini seçerek atama işlemini gerçekleştiririz. Ardından “ **OK** ” seçeneğini seçeriz.

Associate subnet

ProdPrivateNSG

Virtual network ⓘ

Prod-CoreServicesVNET (Private)

Subnet * ⓘ

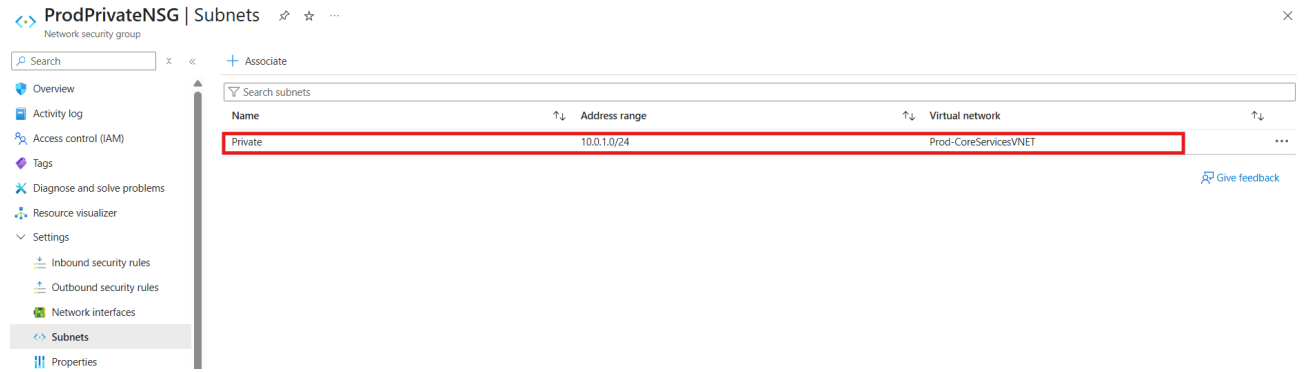
Private

OK

Subnet atama işlemi gerçekleştirilmektedir.



Subnet atama işlemi gerçekleştirdik.



Şimdi geldik bir Kaynağa ağ erişimi sınırlandırmaya haydi gerçekleştirelim. Bundan dolayı Bir Storage Account oluşturacağız. Ardından bu Storage Account'a erişimi sınırlandıracağız.

Bundan önce storage Account nasıl oluşturulur ? Detaylıca incelemek isterseniz. Aşağıdaki makalemde faydalanabilirsiniz :

[Azure Storage Account - Blob Storage Kavramı ve Oluşturma işlemleri - ÇözümPark](#)

“ Azure Storage Account ” dağıtmak için gerekli konfigürasyonları gerçekleştiriz. Ardından bu adımları tamamlayarak **“ Next ”** seçeneğini seçeriz.

Create a storage account ...

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *

Resource group * [Create new](#)

Instance details

Storage account name *

Region * [Deploy to an Azure Extended Zone](#)

Primary service

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

Redundancy *

[Previous](#)

[Next](#)

[Review + create](#)

İkinci adımda ayarları ve konfigürasyonları varsayılan olarak konfigüre ederiz. “ **Next** ” seçeneğini seçeriz.

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ☒

Allow enabling anonymous access on individual containers ☐

Enable storage account key access ☒

Default to Microsoft Entra authorization in the Azure portal ☐

Minimum TLS version

Permitted scope for copy operations (preview)

Hierarchical Namespace

Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs) [Learn more](#)

Enable hierarchical namespace ☐

Access protocols

Blob and Data Lake Gen2 endpoints are provisioned by default [Learn more](#)

“ **Networking** ” adımımda ayarları ve konfigürasyonları varsayılan olarak gerçekleştiririz.

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

Public access

Access your resource from anywhere through a public network.

Note: Allowing access to your resource through a public network increases security risk. [Learn more](#)

Public network access *

☒ Enable
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.

☐ Disable
Restrict inbound access while allowing outbound access.

☐ Secure by perimeter (Most restricted)
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

Public network access scope *

☒ Enable from all networks

☐ Enable from selected virtual networks and IP addresses

▲ Enabling public network access will make this resource available publicly. Unless public access is required, consider using the most restricted access configurations.

Private endpoint

Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be

“ Data Protection ” bölümünü de varsayılan olarak konfigüre ederiz. “ Next ” seçeneğini seçeriz.

Create a storage account ...

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

Recovery

Protect your data from accidental or erroneous deletion or modification.

- ☐ Enable point-in-time restore for containers
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
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)
- ☐ Enable soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)
Enabling soft delete for frequently overwritten data may result in increased storage costs [Learn more](#)
- ☐ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)

Tracking

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

- ☐ Enable versioning for blobs
Use versioning to automatically maintain previous versions of your blobs. [Learn more](#)
Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. [Learn more](#)

Previous **Next** Review + create

“ Encryption ” bölümündeki konfigürasyonları varsayılan olarak konfigüre ederek “ Review + create ” seçeneğini seçeriz.

Create a storage account ...

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

- Encryption type * ⓘ
- ☒ Microsoft-managed keys (MMK)
 - ☐ Customer-managed keys (CMK)
- Enable support for customer-managed keys ⓘ
- ☒ Blobs and files only
 - ☐ All service types (blobs, files, tables, and queues)
- ⚠ This option cannot be changed after this storage account is created.
- Enable infrastructure encryption ⓘ
- ☐

Previous Next **Review + create**

Storage Account dağıtımına başlamak için “Create” seçeneğini seçeriz.

[Home](#) > [Storage accounts](#) >

Create a storage account ...

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

[View automation template](#)

Basics

Subscription	Visual Studio Enterprise Aboneliği
Resource group	Private
Location	East US
Storage account name	prodstraccfile
Primary service	Azure Blob Storage or Azure Data Lake Storage Gen 2
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

Security

Secure transfer	Enabled
-----------------	---------

Previous

Next

Create

Kaynak dağıtımı gerçekleştiriliyor.

Submitting deployment...

Submitting the deployment template for resource group 'Private'.

Kaynak Dağıtımı devam ediyor.

prodstraccfile_1755254011423 | Overview

Deployment

Search x < Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Deployment is in progress

Deployment name: prodstraccfile_1755254011423
Subscriptions: Visual Studio Enterprise Aboneliği
Resource group: Private

Start time: 8/15/2025, 1:34:41 PM
Correlation ID: cd71fe5a-2c33-4de3-b9cb-ea0fa83229d4

Deployment details

Resource	Type	Status	Operation details
No results.			

Give feedback

Tell us about your experience with deployment



Microsoft Defender for Cloud
Secure your apps and infrastructure
[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
[Find an Azure expert >](#)

Kaynak dağıtımı tamamlandı. “Go to resource” seçeneğini seçeriz.

Home > prodstraccfile_1755254011423 | Overview

Deployment

Search x « Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name: prodstraccfile_1755254011423
Subscription: Visual Studio Enterprise Aboneliği
Resource group: Private

Start time: 8/15/2025, 1:34:41 PM
Correlation ID: cd71fe5a-2c33-4de3-b9cb-ea0fa83229d4

Deployment details

Next steps

[Go to resource](#)

Give feedback

[Tell us about your experience with deployment](#)

Ve storage account dağıtımımız gerçekleştirildi.

Home > prodstraccfile_1755254011423 | Overview

prodstraccfile Storage account

Search x « Upload Open in Explorer Delete Move Refresh Open in mobile CLI / PS Feedback

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Containers

File shares

Queues

Tables

Security + networking

Essentials

Resource group (move): Private

Location: eastus

Subscription (move): Visual Studio Enterprise Aboneliği

Subscription ID: a47bb4d7-2dab-4dd5-9011-ab81ddf0681c

Disk state: Available

Tags (edit): Add tags

Performance: Standard

Replication: Locally-redundant storage (LRS)

Account kind: StorageV2 (general purpose v2)

Provisioning state: Succeeded

Created: 8/15/2025, 1:34:46 PM

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Blob service

Hierarchical namespace: Disabled

Default access tier: Hot

Blob anonymous access: Disabled

Blob soft delete: Disabled

Container soft delete: Disabled

Versioning: Disabled

Change feed: Disabled

NFS v3: Disabled

Allow cross-account replication: Disabled

Security

Require secure transfer for REST API operations: Enabled

Storage account key access: Enabled

Minimum TLS version: Version 1.2

Infrastructure encryption: Disabled

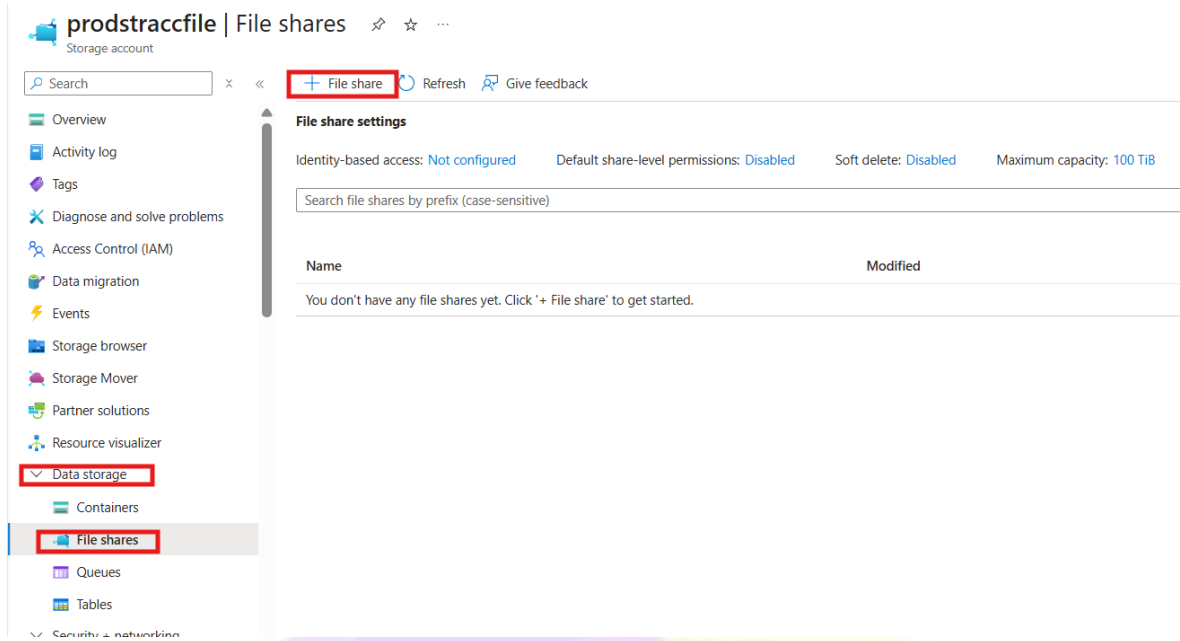
Networking

Public network access: Enabled

Public network access scope: Enable from all networks

Bir sonraki yapacağımız işlem ise dağıttığımız storage account içerisinde “ **File Shares** ” oluşturmak.

Storage Account’a giriş yaparak “ **Data storage** ” bölümü altında “ **File Shares** ” seçeneğini ardından “ **File Share** ” ile bu bölümde Dosya paylaşım oluştururuz.



“ **Name** ” bölümünde isimlendirme yaparız. “ **Access tier** ” bölümünde ise “ **Transaction optimized** ” seçeneğini seçerek devam ederiz. “ **Review + create** ” seçeneğini seçeriz.

New file share

Basics Backup Review + create

Name * prod
Access tier * Transaction optimized

Performance

Maximum IO/s 20000
Maximum capacity 100 TiB

[To use the SMB protocol with this share, check if you can communicate over port 445. These scripts for Windows clients and Linux clients can help. Learn how to circumvent port 445 issues.](#)

Review + create

< Previous

Next : Backup >

“ Create “ seçeneğini seçeriz.

New file share ...

✓ Validation passed

Basics Backup Review + create

Basics

File share name prod
Access Tier TransactionOptimized
Protocol SMB

Create

< Previous

Next >

[Download a template for automation](#)

Ve File Share oluşturma işlemimiz gerçekleşti.

Home > prodstracfile_1755254011423 | Overview > prodstracfile | File shares > New file share >

prod
SMB File share

Search x < > Connect Upload Refresh Add directory Delete share Change tier Edit quota Give feedback

Overview

Diagnose and solve problems

Access Control (IAM)

Browse

Operations

Snapshots

Backup

Enable Backup for file share "prod" to protect your data. [Learn more](#)

Essentials

Storage account	: prodstracfile	Share URL	: https://prodstracfile.file.core.windows.net/prod
Resource group (move)	: Private	Redundancy	: Locally-redundant storage (LRS)
Location	: East US	Configuration modified	: 8/15/2025, 1:47:23 PM
Subscription (move)	: Visual Studio Enterprise Aboneliği		
Subscription ID	: a47bb4d7-2dab-4dd5-9011-ab81ddf0681c		

Properties Capabilities (2) Tutorials

Size

Maximum storage (GiB)	102400
Used storage capacity (GiB)	0
Access tier	Transaction optimized

Performance

IOPS	Varies by region. Learn more
Throughput (MiB/sec)	Varies by region. Learn more

Feature status

Soft delete	Disabled
Large file shares	Enabled

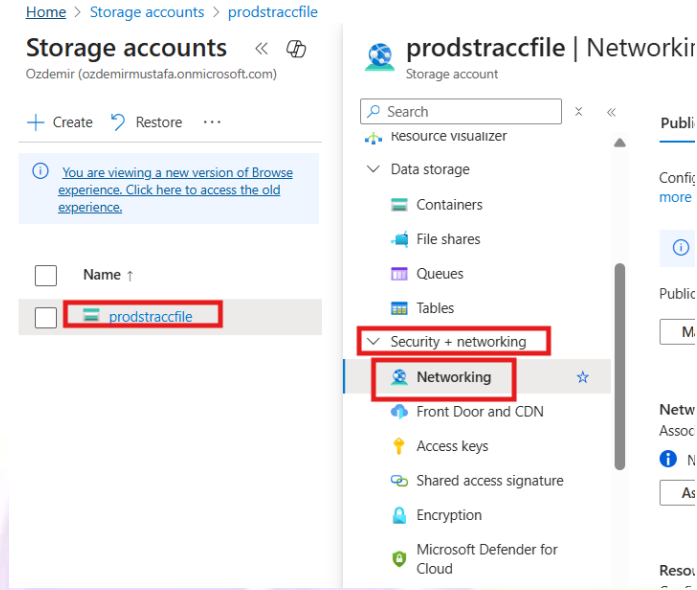
Identity-based access

Directory service	Not configured
Domain	-

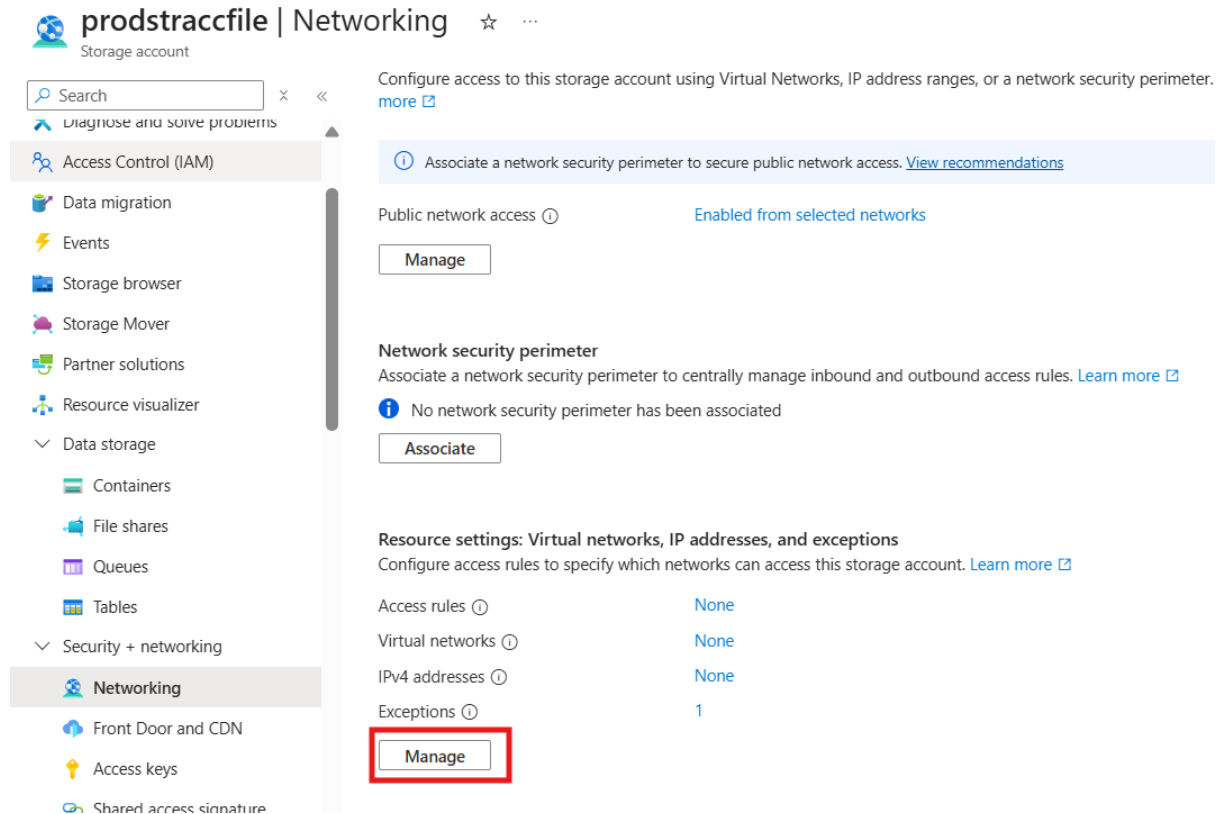
SMB protocol settings

File Share oluşturduk. Şimdi yapacağımız işlem Network erişimini bir subnet'e kısıtlamaktır. Bunu gerçekleştireceğiz. Storage Account'lar genelde default olarak internetten erişim şeklinde konfigüre edilmektedir. Herhangi bir networkten gelen erişimleri Kabul ederler. Ama bizim istediğimiz senaryo bu değil. Subnet'ten gelen erişim hariç diğer tüm Virtual Network'lerden gelen internet ve subnet erişimlerimizi engellememiz gerekmektedir.

Dağıtım gerçekleştirdiğimiz Storage account'umuza erişim gerçekleştiririz. Ardından konfigürasyonları yapabilmemiz için **"Security + networking"** bölümü altında **"Networking"** seçeneğini seçeriz.



"Manage" seçeneğini seçeriz.



“ **Virtual Networks** ” bölümü altından storage account’umuza var olan virtual network’ümüzü eklemek için “ **Add a virtual network** ” seçeneği altından “ **Add existing virtual network** ” seçeneğini seçeriz.

Microsoft Azure

Home > Storage accounts > prodstraccfile | Networking >

Resource access settings

Virtual Networks

Allow select virtual networks to connect to your resource using service endpoints. [Learn more](#)

+ Add a virtual network

Add existing virtual network

Add new virtual network

Subnet	Address Range	Endpoint Status	Resource Group
--------	---------------	-----------------	----------------

IPv4 Addresses

Allow select public internet IP addresses to access your resource. [Learn more](#)

“ **Subscription** ” bölümünde virtual network’ümüzü kapsayan aboneliği seçeriz. Ardından eklemek istediğimiz Virtual Network’ü seçerek , eklemek istediğimiz Subnet’i ekleriz. Ardından “ **Add** ” seçeneğini seçeriz.

Add networks

Subscription *

Virtual networks *

Subnets *

Add

Ardından virtual network'ümüzün ve subnetimizin eklendiğini gördük. Konfigürasyonların kaydedilmesi için "Save" seçeneğini seçeriz.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Storage accounts > prodstraccfile | Networking >

Resource access settings

Virtual Networks

Allow select virtual networks to connect to your resource using service endpoints. [Learn more](#)

+ Add a virtual network

Virtual Network	Subnet	Address Range	Endpoint Status	Resource Group	Subscription
Prod-CoreServicesVNET	1	10.0.0.0/16		private	Visual Studio Enterprise Abor
	Private	-	Enabled	private	Visual Studio Enterprise Abor

IPv4 Addresses

Allow select public internet IP addresses to access your resource. [Learn more](#)

+ Add your client IPv4 address ("178.245.140.252")

IPv4 address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity. [Learn more](#)

Resource type

Instance name

Select a resource type

Select one or more instances

Save Cancel

Kaynak konfigürasyonları kaydediliyor.

mustafaozdemir92@out...
OZDEMIR (OZDEMIRMUSTAFA.O...

Saving resource settings

Kaynak konfigürasyonları kaydedildi.

Resource settings saved

Resource settings have been saved successfully

a few seconds ago

Buraya kadar tüm konfigürasyonları tamamladık. Şimdi geldik. Erişimi test etmeye 😊

Erişimi test etmek için 2 adet Sanal Makine oluşturmam gerekiyor. Bunun için detaylı makalemi inceleyebilirsiniz ;

<https://www.cozumpark.com/azure-ortaminizda-windows-server-2022-isletim-sistemli-virtual-machine-olusturma-islemleri/>

2 Sanal makine oluşturacağım. Bunlardan birisi Service Endpoint'ı test etmek için , diğeri ise public erişim için haydi başlayalım.

Sanal Makine kurulumlarımızı VM-Public adındaki makinede public erişimi test edeceğim subnet public olarak yapılandırıdığım Sanal Makinede internete erişimi olup , storage account'a erişmemesini bekliyeceğiz.

VM-Public olarak oluşturacağım makinede VNET ve Subnet seçimini aşağıdaki gibi seçeriz.

The screenshot shows the Azure portal interface for a virtual machine named 'VMPUBLIC'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Bastion, Windows Admin Center, Networking, Network settings, Load balancing, Application security groups, Network manager, Settings, Disks, and Extensions + applications. The main area displays the 'Overview' tab with the following details:

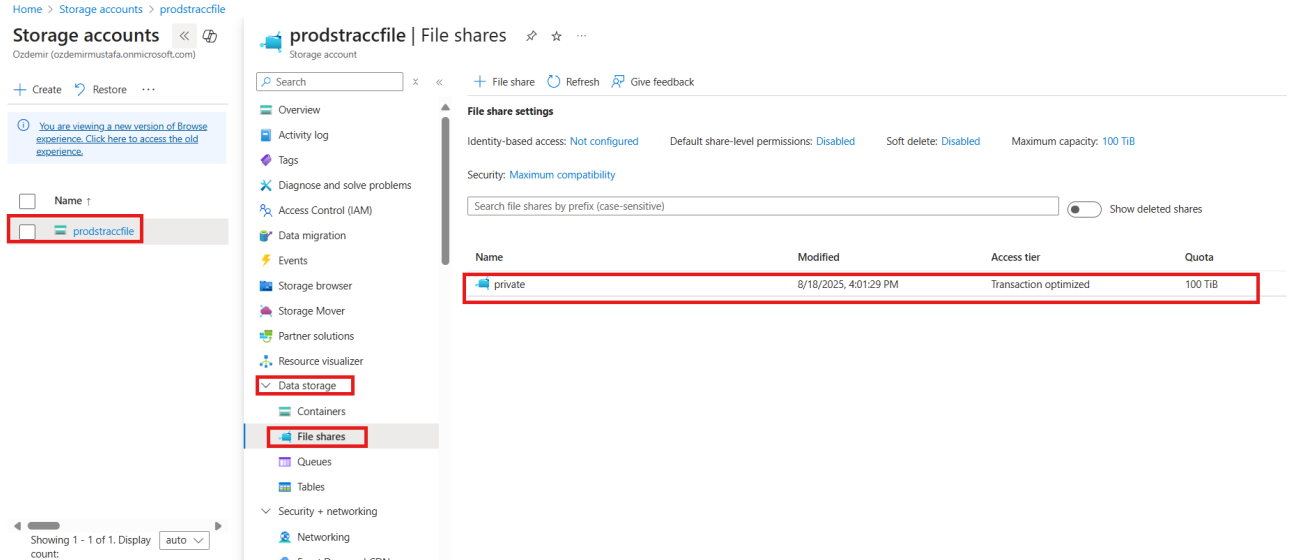
- Essentials:**
 - Resource group (move): Private
 - Status: Running
 - Location: East US
 - Subscription (move): Visual Studio Enterprise Aboneliği
 - Subscription ID: a47bb4d7-2dab-4dd5-9011-ab81dd0681c
- Operating system:** Windows (Windows Server 2025 Datacenter)
- Size:** Standard B2s v2 (2 vcpus, 8 GiB memory)
- Public IP address:** 172.206.198.181
- Virtual network/subnet:** Prod-CoreServicesVNET/Public (highlighted with a red box)
- DNS name:** Not configured
- Health state:** -
- Time created:** 8/18/2025, 9:11 PM UTC

Below the essentials, there are tabs for Properties, Monitoring, Capabilities (8), Recommendations, and Tutorials. The 'Properties' tab is active, showing the following details:

- Virtual machine:**
 - Computer name: VMPUBLIC
 - Operating system: Windows (Windows Server 2025 Datacenter)
 - VM generation: V2
 - VM architecture: x64
 - Agent status: Ready
 - Agent version: 2.7.41491.1172
 - Hibernation: Disabled
 - Host group: -
- Networking:**
 - Public IP address: 172.206.198.181 (Network interface vmpubl)
 - Public IP address (IPv6): -
 - Private IP address: 10.0.0.4
 - Private IP address (IPv6): -
 - Virtual network/subnet: Prod-CoreServicesVNET/Public
 - DNS name: Configure
- Size:** (Icon for size selection)

Sanal Makineye bağlanarak Test işlemlerine başlamak için cmd arayüzünden www.google.com.tr adresine pingleme yapıldığını görürüz.

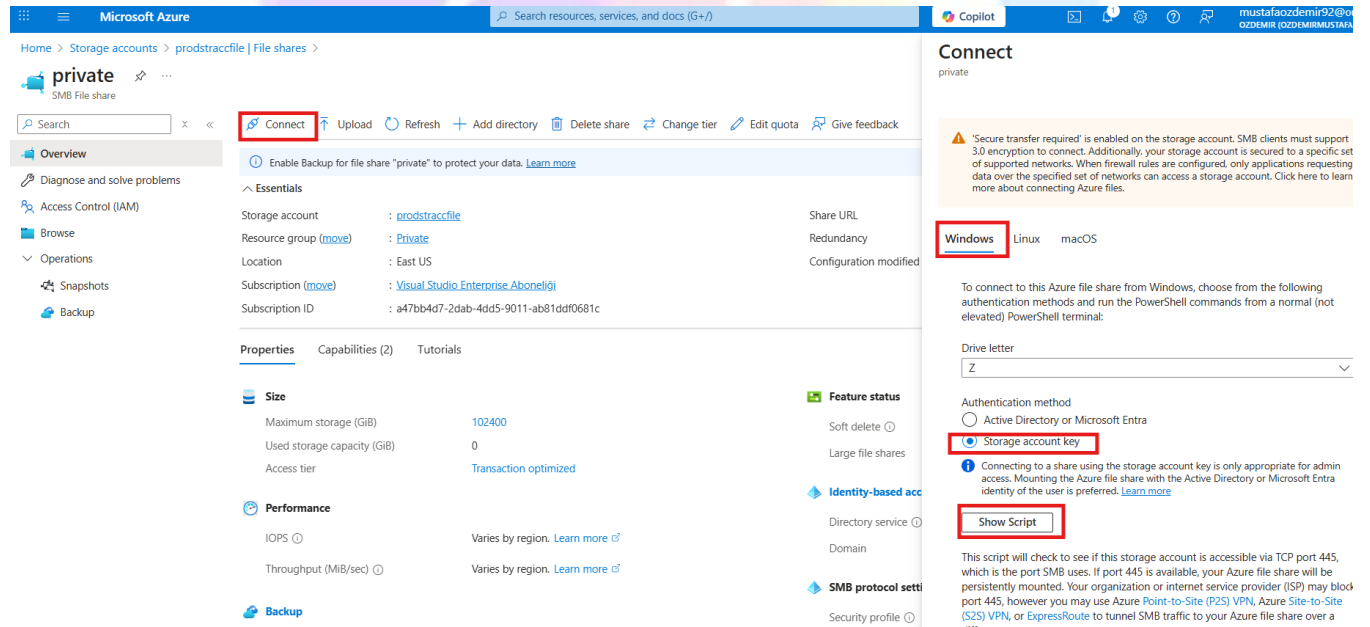
File share erişimi için ise storage account'umuza erişiriz. Ardından storage account içerisinde “ **Data storage** ” bölümünü seçerek “ **File Shares** ” bölümünden “ **private** ” isminde olan paylaşımlımızı seçeriz.



The screenshot shows the Azure portal interface for a storage account named 'prodstraccfile'. The left sidebar has the 'Data storage' section expanded, and 'File shares' is selected. The main area displays the 'File share settings' for the 'private' share. A table lists the shares, with 'private' highlighted. The table has columns for Name, Modified, Access tier, and Quota.

Name	Modified	Access tier	Quota
private	8/18/2025, 4:01:29 PM	Transaction optimized	100 TiB

Ardından file share bağlantı gerçekleştirmek için sunucumuza drive eklememizi ve erişimimizi sağlayan key'leri PowerShell'e kopyalayacağımız script'e erişmek için “ **Connect** ” seçeneğini seçerek işletim sistemi olarak “ **Windows** ” sezeriz. “ **Storage account key** ” seçeneğini seçerek “ **show script** ” ile script konsolunu açarız.



The screenshot shows the 'Connect' page for the 'private' file share. The 'Connect' button is highlighted in the top bar. The 'Windows' tab is selected, and the 'Storage account key' authentication method is chosen. The 'Show Script' button is highlighted.

Authentication method:

- ☐ Active Directory or Microsoft Entra
- ☒ Storage account key

Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory or Microsoft Entra identity of the user is preferred. [Learn more](#)

Show Script

This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), [Azure Site-to-Site \(S2S\) VPN](#), or [ExpressRoute](#) to tunnel SMB traffic to your Azure file share over a...

Ardından Script’i kopyalarak VM-Public adındaki Sanal Makinemizin PowerShell konsoluna yapıştırırız.

Hide Script

```
$connectTestResult = Test-NetConnection -ComputerName
prodstraccfile.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:""prodstraccfile.file.core.windows.net""
/user:""localhost\prodstraccfile""
/pass:""rveQPOcO0USH2DhGHRUfwQtC6mEeaHL07AEekH/0RWssYYfbpBsKa5
x9VMKNyo7rEAbqo1bHEdGM+AStWtPDGg=="`""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\prodstraccfile.file.core.windows.net\private" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port
445. Check to make sure your organization or ISP is not blocking port 445, or
use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic
over a different port."
}
```

This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), Azure [Site-to-Site](#)

Ve bu Sanal Makinemizin istediği gibi public ortama açık olan makinemizin storage account'a erişimi olmadığını görmüş oluruz.İstedığımız bu 😊

```
172.206.198.181 - Remote Desktop Connection
Administrator: Command Prompt x + -
C:\Users\mustafa.ozdemir>ping www.google.com.tr -t

Pinging www.google.com.tr [172.253.115.94] with 32 bytes of data:

Reply from 172.253.115.94: bytes=32 time=3ms TTL=182
Reply from 172.253.115.94: bytes=32 time=9ms TTL=182
Reply from 172.253.115.94: bytes=32 time=5ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=3ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182
Reply from 172.253.115.94: bytes=32 time=3ms TTL=182
Reply from 172.253.115.94: bytes=32 time=5ms TTL=182
Reply from 172.253.115.94: bytes=32 time=2ms TTL=182

Administrator: Windows PowerShell x + -
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> $connectTestResult = Test-NetConnection -ComputerName prodstraccfile.file.core.windows.net -Port 445

PS C:\Windows\system32> if ($connectTestResult.TopTestSucceeded) {
>> # Save the password so the drive will persist on reboot
>> cmd.exe /C "cmdkey /add:"prodstraccfile.file.core.windows.net" /user:"localhos
t\prodstraccfile" /pass:"rveQp0c00USH2DhGhrUfmQtC6mEeaHL07AEekH/0RWssYfvpBsKa5x9VMKNy
o7rEAbqqlbHedGm+ASTwtPDGg=="
>> # Mount the drive
>> New-PSDrive -Name Z -PSProvider FileSystem -Root "\\prodstraccfile.file.core.wind
ows.net\private" -Persist
>> } else {
>> Write-Error -Message "Unable to reach the Azure storage account via port 445. Che
ck to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN,
Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
>> }

CMDKEY: Credential added successfully.
New-PSDrive : Access is denied
At line:5 char:5
+ New-PSDrive -Name Z -PSProvider FileSystem -Root "\\prodstraccfil ...
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (Z:PSDriveInfo) [New-PSDrive], Win32Exce
ption
+ FullyQualifiedErrorId : CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewP
SDriveCommand

PS C:\Windows\system32> |
```

Diğer VM-Private olan Sanal Makinemizin Konfigürasyonu ise aşağıda gösterildiği gibi VNET içerisinde " **Private** " olarak subnet seçimi gerçekleştirilmiştir.

Ve diğer makinemin ise bu senaryoda internete erişmediği ve dışarı çıkmadığı sadece Storage account erişiminde sonlandığını görmüş oluruz.

Hepsi Bu kadar 😊

Makalemi zaman ayırıp okuduğunuz için çok teşekkür ederim. Diğer Makalelerimde görüşmek üzere. Faydalı olması Dileğiyle...