

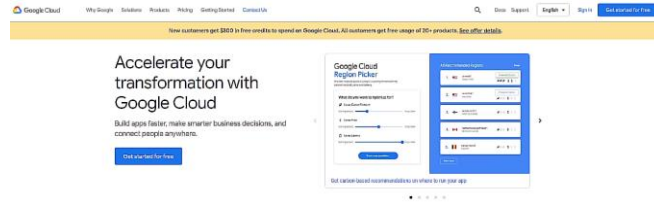
Özel Server Kurma – Self Hosted – Google Cloud

1)Google Cloud – Server kurma ve ilk bağlantı

-Kendi özel serverımızı photon kurulumunu yapacağız.

1-Google Cloud gidip server işlemlerimizi yapacağız. Online oyunumuzda server kiralarken, local bir noktadan kiralamak daha önemli olacaktır. Biz bu dersimizde Google Cloud ile server kurma işlemlerimizi gerçekleştireceğiz.

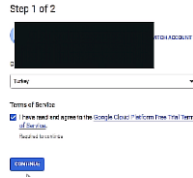
Eğer istersen Amazon veya Microsoft gibi şirketlerin cloud yapısını da kullanabilirsin. Ya da bir hosting firmasından server kiralayabilirsin.



2-Get started for free butonuna tıklıyoruz. Ve karşımıza gelen giriş yap panelinden gmail adresimiz ile giriş işlemlerimizi yapıyoruz.

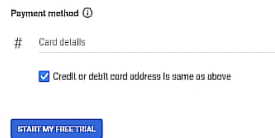


3-Sonrasında ülke seçimini yapıp, sözleşmeyi kabul ediyoruz.

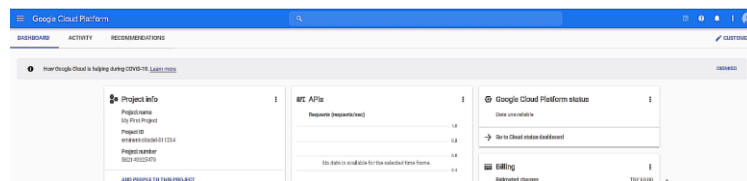


4-Adreslerimizi, kişisel bilgilerimizi vs. tamamladıktan sonra, kendimize ait bir kredi kartı girip sembolik birkaç dolar çekip, daha sonrasında iade ediyor. Eğer 90 günlük deneme sürecini tamamlarsan ve devam etmek istersen bu kredi kartı ile devam ediyorsun.

!Kredi kartı kısmında sanal kredi kartı kullanmanı tavsiye ederim.

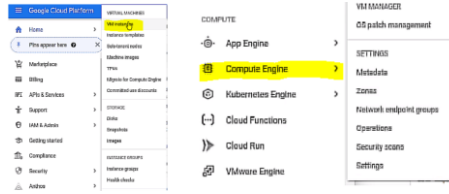


5-Sonrasında Google Cloud arayüzü karşımıza geliyor.



6-!Photon sdk dosyamız Windows serverlar ile çalışır. Eğer free hesap kullanıyorsan, sana Windows server kullandırtmıyor.

Sonrasında sanal makine kurulumuna gidiyoruz.



7-Compute Engine aktifleştirelim mi? sorusu karşına gelebilir. Aktifleştirme işlemini tamamladıktan sonra aşağıdaki gibi bir sayfa karşına gelecek.



8-Bir server oluşturmak için Create Instance butonuna tıklıyoruz. Ve karşımıza bir form geliyor.



9-Formumuzu dolduruyoruz. Ve formu doldururken hepsinde küçük harf kullanmalıyız.

Server ismimizi giriyoruz.

Name ⓘ
Name is permanent
photonosistem

Labels ⓘ (Optional)
+ Add label

Region ⓘ
Region is permanent
us-central1 (Iowa)

Zone ⓘ
Zone is permanent
us-central1-a

Kurmak istediğimiz işletim sistemini seçiyoruz. Default olarak Linux işletim sistemi karşımıza geliyor, ancak ilk başta dediğim gibi Photon Windows üzerinde çalışıyor. İşletim sistemimizi değiştiriyoruz.

!Windows minimum 2012 kullanmalıyız. Önerilen 2019.

Boot disk ⓘ
New 10 GB balanced persistent disk
Image
Debian GNU/Linux 10 (buster) [Change]

Boot disk ⓘ
Size (GB) ⓘ
SSD persistent disk 50

Operating system
Windows Server

Version
Windows Server 2019 Datacenter

Server with Desktop Experience, x64 built on 20210413, supports Shielded VM features ⓘ

Locasyon ayarlarımız. Dünyada herkesin bağlantısının kolay olabileceği bir noktada bağlantı yapmak daha iyi olacaktır.

Region Region is permanent
europa-west4 (Netherlands)

Zone Zone is permanent
europa-west4-a

Makine ayarlarımızı yapıyoruz.

Machine configuration

Machine family
General-purpose Compute-optimized GPU

Machine types for common workloads, optimized for cost and flexibility

Series
n2

Powered by Intel Cascade Lake CPU platform

Machine type
n2-standard-2 (2 vCPU, 6 GB memory)

vCPU 2 Memory 6 GB GPUs -

Diğer ayarlarımız

If you are using Windows and intend to run additional Microsoft software, please fill out the [License Verification Form](#)
[Learn more about Microsoft license mobility requirements](#)

Identity and API access

Service account
Compute Engine default service account

Access scopes
☒ Allow default access
☐ Allow full access to all Cloud APIs
☐ Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☒ Allow HTTP traffic
☒ Allow HTTPS traffic
[Management, security, disks, networking, sole tenancy](#)

En son olarak Create diyerek serverımızı kuruyoruz.

You will be billed for this instance. [Compute Engine pricing](#)

Create Cancel

Bu ayarlar ile maliyetimiz aylık 132 dolar olarak gözüküyor.

\$131.51 monthly estimate

Artık serverımız istediğimiz ayarlar ile kuruldu. Sonrasında istediğin değişikliği arttırıp, azaltma işlemlerini rahatça yapabilirsin.

Compute Engine

VM Instances

CREATE INSTANCE

IMPORT VM

REFRESH

START / RESUME

STOP

SUSPEND

RESET

DELETE

CREATE SCHEDULE

Virtual machines

VM Instances

Instance templates

Subnetworks

INSTANCES

INSTANCE SCHEDULE

Filter

Enter property name or value

1041 Instance is running

plus

phoenixlab01

example-vm-01-a

Is state by

Internal IP

External IP

Current

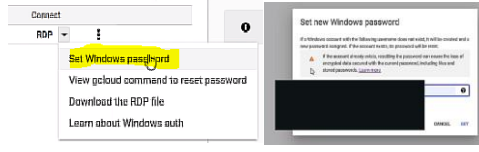
10.144.0.2

34.90.154.24028

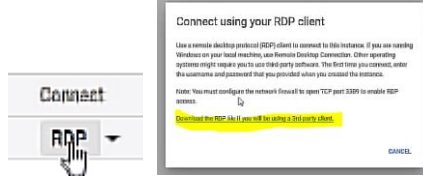
STOP

11-Bizim bu sisteme bağlanıp, server ile ilgili işlemlerimizi yapmamız gerekecek. Biz hazırladığımız servera bağlanabilmek için bir kullanıcı adı ve şifre belirlememiz gerekiyor.

Kullanıcı adı ve şifre oluşturuyoruz. !küçük harfler ile giriş yapıyoruz.

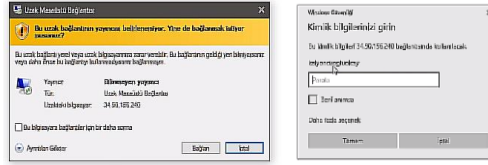


12-Bağlantıyı sağlayabilmek için ise, bize bir dosya verecek ve uzak masaüstüne rahatça bağlanabileceğiz.

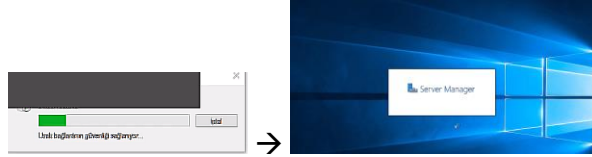


13-İndirmiş olduğumuz dosyaya tıklıyoruz. Ve bize uzak masaüstü bağlantısı olarak karşımıza geliyor. Bağlan diyoruz ve sonrasında kullanıcı adı ve şifremizi giriyoruz.

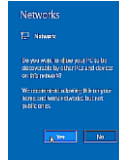
Eğer bilgisayarında bağlı olan hesap gelirse, daha fazla seçeneğe tıklıyorsun, başka bir hesap kullanmak istediğini belirtip, kullanıcı adı ve şifreni giriş yapıyorsun. Ve işlemleri tamamlamış oluyorsun.



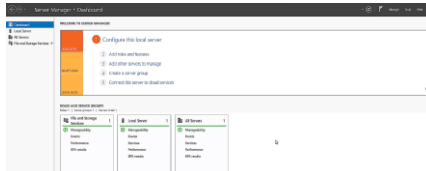
Tamam dedikten sonra kurmuş olduğumuz servera bağlanıyoruz.



14- Kurmuş olduğun pc, internete çıkmasını istiyor musun sorusu karşımıza geliyor. Evet dedikten sonra işlemlerimize devam ediyoruz.

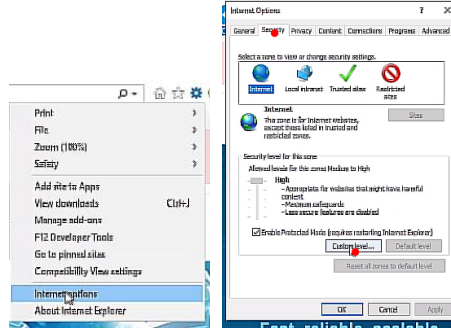


15-Server Manager Dashboard sayfamız ise bizim analiz yaptığımız makine kullanımları hakkında tüm bilgileri sağlayan ara yüzümüzdür.



2)Photon SDK indirme ve yükleme | Lisans işlemleri | Powershell portlarını açma

16-Java vs. gibi internet girişlerimizi yapmamız gerekiyor. Serverımızdan Explorer açtıktan sonra aşağıdaki işlemleri yapıp gerekli aktifleştirmeleri yapıyoruz.



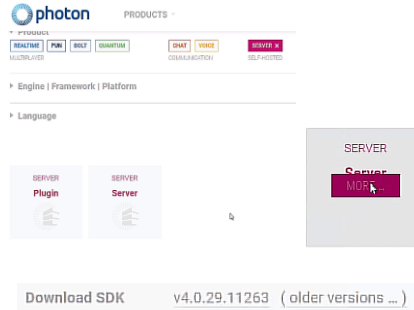
Dosya indirme ve js ayarlarını etkinleştiriyoruz.



17-Sonrasında, serverımıza Google Chrome indiriyoruz. Sürekli bir işlem yapacaksa ve internete çıkacaksa Google Chrome kullanmamız daha hızlı olacaktır. !Tercihe bağlı istediğin tarayıcıyı kullanabilirsin.

18- Google Chrome açtıktan sonra, photon sayfasına gidiyoruz. Photon üyeliğimiz ile giriş yaptıktan sonra, server kısmına gidiyoruz.

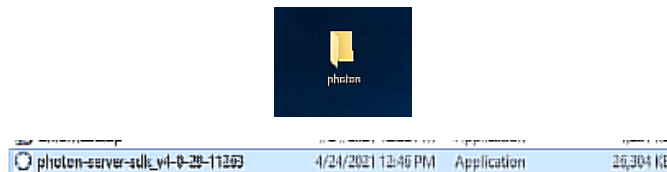
SDK dosyamızı indiriyoruz.



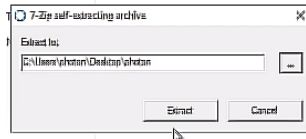
19-Takıldığın noktalarda, server dokümanından da yararlanabilirsin.



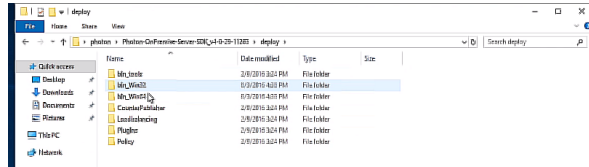
20-Server masaüstünde bir klasör oluşturuyoruz. Sonrasında server için indirdiğimiz sdk dosyamıza tıklıyoruz.



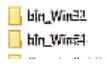
Sonrasında oluşturduğumuz klasörümüzü seçiyoruz. Ve içerisindeki dosyaları photon klasörüne çıkarıyoruz.



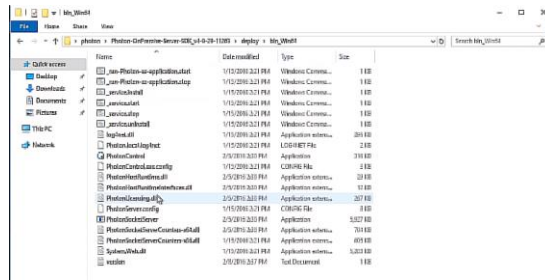
Artık tüm klasör ve dosyaları çıkarmış durumdayız.



!Buradaki önemli olan nokta kurmuş olduğumuz sistemin mimarisi 32 ise 32 olanı 64 ise 64 olan mimariyi kullanacağız.



Bizim kurmuş olduğumuz mimarimiz 64 olduğu için ana dosyalarımız 64 içerisindeki dosyalardır.



21-Biz Photon serverı kullanabilmemiz için bir lisanslama yapmamız gerekiyor. Çünkü pun vs. hazır yapıları kullandığımızda arka planla bize lisanslama işlemlerini yapıyor. Ancak biz özel server kullandığımız için lisans işlemlerini de kendimiz yapmamız gerekiyor.

Photon server dokümanından Operations → Licenses kısmına tıklıyoruz.



Free Lisans almak istediğimizi söylüyoruz.

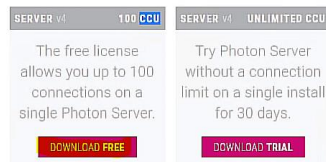
Free License

Photon can be used free of charge for up to 100 concurrent connections (players that are connected at the same time). Note that you may not use free or trial licenses for commercial purposes, if not agreed otherwise. Free and trial licenses each may be used on one (server) machine at a time.

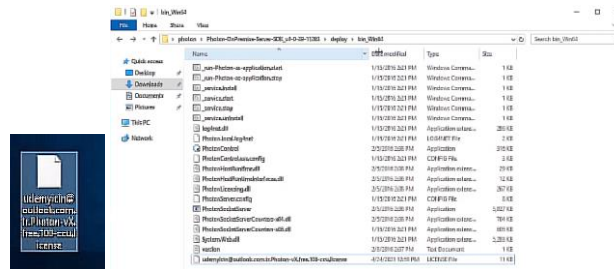
[Get your free license here.](#)

[Back To Top](#)

Free and Trial Licenses

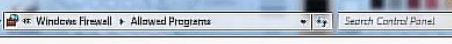


Sistem başladığında ilk önce lisans dosyalarını aradığı için, sürükleyip bırakmamız yeterli.



Bağlantıların yapılabilmesi için gerekli portları açıp ve güvenlik duvarından ise, photon sdk dosyasına izin veriyor olmamız gerekiyor.

- Operations
 - IPv6
 - Debugging
 - Secure WebSockets Setup
 - Photon Server Configuration
 - Photon Server Config Settings
 - TCP and UDP Port Numbers
- Firewall Settings
 - Policy Files
 - Hosting and Requirements
 - Licenses



The screenshot shows the 'Allowed Programs' tab in the Windows Firewall control panel. The title bar reads 'Windows Firewall > Allowed Programs'. Below the title bar is a search bar labeled 'Search Control Panel'. The main content area has the heading 'Allow programs to communicate through Windows Firewall' followed by the instruction 'To add, change, or remove allowed programs and ports, click Change settings.' Below this is a link 'What are the risks of allowing a program to communicate?' and a button 'Change settings...'. A table titled 'Allowed programs and features:' lists the following:

Name	Domain	Home/Work (Private)	Public
<input checked="" type="checkbox"/> Photon Socket Server [Exit Games GmbH I]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

```
$fw = New-Object -ComObject hnetcfg.FwPolicy2
$ruleTcp = New-Object -ComObject HNetCfg.FwRule
$ruleUdp = New-Object -ComObject HNetCfg.FwRule

$ruleTcp.Name = "Photon SocketServer TCP"
$ruleTcp.Protocol = 6 #NET_FW_IP_PROTOCOL_TCP
$ruleTcp.LocalPorts = "80,443,843,943,4520-4522,4530-4533,4540,4541,5060-6063,9080-9093,19090-19093"
$ruleTcp.Enabled = $true

$ruleTcp.Profiles = 7 #all
$ruleTcp.Action = 1 # NET_FW_ACTION_ALLOW

$ruleUdp.Name = "Photon SocketServer UDP"
$ruleUdp.Protocol = 17 #NET_FW_IP_PROTOCOL_UDP
$ruleUdp.LocalPorts = "5055-5058,40001,27000-27003"
$ruleUdp.Enabled = $true

$ruleUdp.Profiles = 7 #all
$ruleUdp.Action = 1 # NET_FW_ACTION_ALLOW

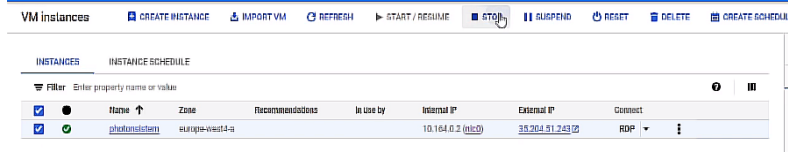
$fw.Rules.Add($ruleTcp)
$fw.Rules.Add($ruleUdp)
```



Kodu çalıştırdıktan sonra makinayı kapatıp, tekrar açmalısın.

3)Google Cloud portlarını açma | Photon sunucuyu çalıştırma

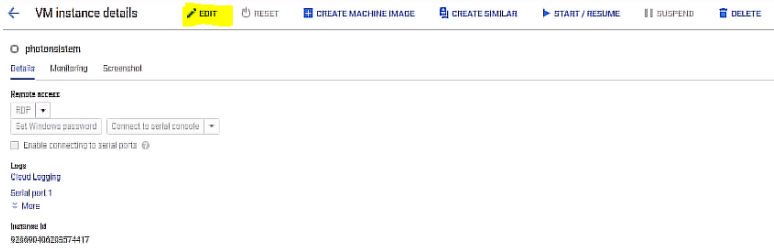
24- Benim server tarafında tanımlamış olduğum portları Google Cloud tarafında da tanımlamış olmam gerekiyor. Bu işlemi yapabilmek için ilk önce makinamızı durdurmamız gerekiyor. Sonrasında f5 ile sayfayı yeniliyoruz.



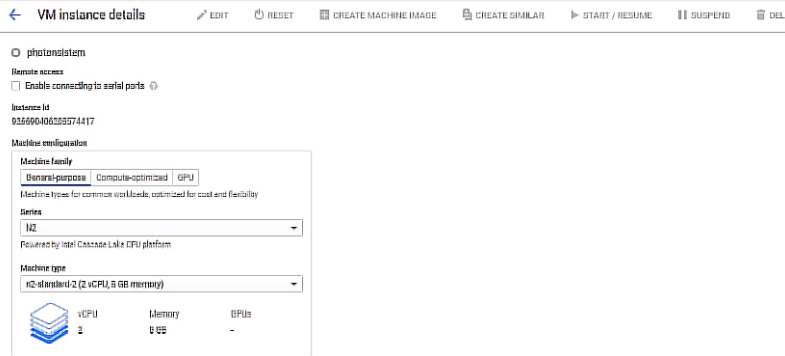
Makinamızın ismine tıklayarak ayarlarına gidiyoruz.



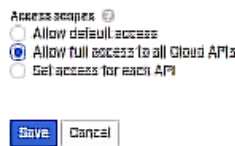
Makinamızı görebiliyoruz. Edit butonu ile de makine ayarlarına geçiyoruz.



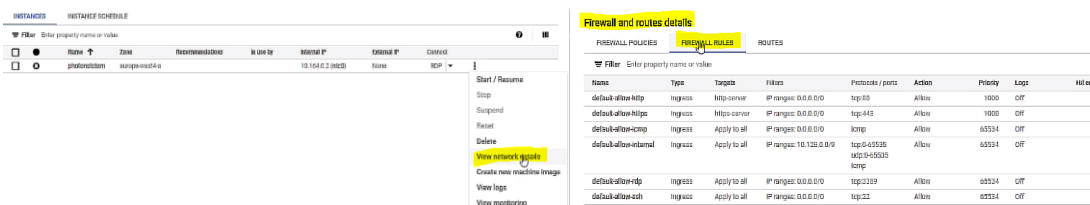
İlk başta yapmış olduğumuz ayarlarımızın olduğu bölüm karşımıza geliyor.



Değişiklik yapacağımız bölüm ise, alt tarafta tüm gelen oturumlara izin verip kayıt işlemimizi yapıyoruz.



25-Bir sonraki yapacağımız işlem ise ağ detayları kısmından güvenlik duvarı ayarlarına giriyoruz.



Burada kendimize bir güvenlik duvarı oluşturup, photonda açtığımız güvenlik duvarlarına yani portlara burada izin vereceğiz.

Yeni kurallar oluşturabilmek için, firewall seçeneğine tıklıyoruz. Artık tüm kuralları görebiliyoruz. İstedığımızı kaldırıp, istediğimizi ekleyebiliriz.

VPC network	Network interface details	Filter
VPC networks	Network interface details	Name Type Targets Filters Protocols / ports Action Priority Network Log
External IP addresses	Network interface details	default-allow-http Ingress http-server IP ranges: 0.0.0.0/0 tcp:80 Allow 1000 default Off
Bring your own IP	Network interface details	default-allow-https Ingress https-server IP ranges: 0.0.0.0/0 tcp:443 Allow 1000 default Off
Private	Network interface details	default-allow-icmp Ingress Apply to all IP ranges: 0.0.0.0/0 icmp Allow 65534 default Off
Routes	Network interface details	default-allow-internal Ingress Apply to all IP ranges: 10.128.0.0/9 tcp:0-65535 udp:0-65535 icmp Allow 65534 default Off
VPC network peering	Network interface details	default-allow-udp Ingress Apply to all IP ranges: 0.0.0.0/0 tcp:3389 Allow 65534 default Off
Shared VPC	Network interface details	default-allow-ssh Ingress Apply to all IP ranges: 0.0.0.0/0 tcp:22 Allow 65534 default Off
Services VPC access	Network interface details	
Packet mirroring	Network interface details	

Yeni bir güvenlik duvarı için üst tarafta bulunan Create Firewall Rule butonuna basıyoruz.



26-Yeni kurallar oluşturma sayfası

Kurallarımıza bir isim veriyoruz.

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *

portlar

Lowercase letters, numbers, hyphens allowed

Sonrasında, öncelik seçeneğimiz default olarak 1000 geliyor biz 999 yaparak daha öncelikli kurallar olduğunu belirtiyoruz.

Priority *

999

CHECK PRIORITY OF OTHER FIREWALL RULES

Priority can be 0 - 65535

Trafiğimizin bir giriş olduğunu ve bütün hepsine izin veriyoruz.

Direction of traffic

☒ Ingress

☐ Egress

Action on match

☒ Allow

☐ Deny

Birden fazla tag oluşturup, iki ayrı makinayı da tag belirterek sistem hangi tagın neyi set edeceğini belirliyoruz. Yani iki ayrı sanal makinamız mevcut biri veri tabanını tutuyor bir diğeri ise oyunumuzun serverı taglar belirterek hangi ayarın hangi makinaya yapılacağını belirleyebiliriz. Ancak bizim tek bir makinamız olduğu için bütün örneklerle set et dememiz yeterli.

Targets

All instances in the network

İp aralığını belirleyerek o ip aralığında gelmesini isteyebiliriz. Ancak oyunumuza herkesin girmesini istediğimiz için her türlü ip'ye izin veriyoruz.

Source IP ranges *

0.0.0.0/0 for example, 0.0.0.0/0, 192.168.2.0/24

Sonrasında photonun bize verdiği tcp ve udp portlarını giriyoruz.

```
$ruleTcp.LocalPorts = "80,443,843,943,4520-4522,4530-4533,4540,4541,6060-6063,9090-9093,19090-19093"  
$ruleUdp.LocalPorts = "5055-5058,40001,27000-27003"
```

!Port açma mantığı şu 80 portu aç, 443 portu aç.. 4520-4522 arasındakiler dahil olmak üzere hepsini aç demek.

Specified protocols and ports

☒ tcp : 80,443,843,943,4520-4522,4530-4533,4540,4541,6060-6063,9090-9093

☒ udp : 5055-5058,40001,27000-27003

İşlemlerimizi yaptık artık create diyerek ayarlarımızın kaydını yapıyoruz. Ayarlarımız yapıldı.

DISABLE RULE

CREATE CANCEL →

portlar	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp: 80,443,843,943,4520-4522,4530-4533,4540,4541,6060-6063,9090-9093	Allow	999	default	Off	--	--
				udp: 5055-5058,40001,27000-27003						

27-Serverımızın içerisinden güvenlik duvarına baktığımızda photon tcp ve udp izin verdiğimizi görüyoruz. Böylelikle işlemimizin başarılı olduğunu anlayabiliriz.

Windows Defender Firewall with Advanced Security

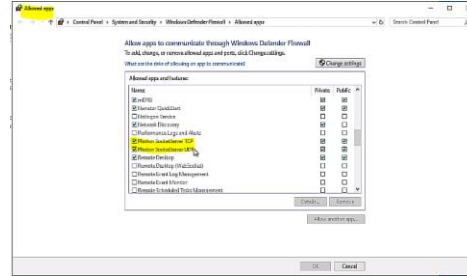
File Action View Help

Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Dir
Allow incoming from OCE metadata server		All	Yes	Allow	Yes
ICMP Allow incoming V4 echo request		All	Yes	Allow	Yes
Photon SocketServer TCP		All	Yes	Allow	Yes
Photon SocketServer UDP		All	Yes	Allow	Yes

28-Güvenlik duvarında izinli olup olmadığının kontrolünü yapıyoruz. Diğer durumlara oyuncular bağlanamayabilir.



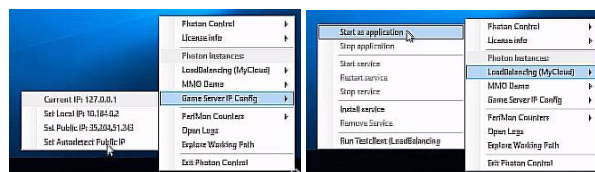
29-Artık uygulamamızı başlatabiliyoruz. Oluşturduğumuz photon klasörüne gidiyoruz ve 64 mimariyi seçiyoruz. PhotonControl tıklıyoruz ve uygulamasını açıyoruz.

PhotonControl	2/5/2016 3:38 PM	Application	316 KB
PhotonControl.exe.config	1/15/2016 3:01 AM	Configuration File	3 KB

Aşağıdaki simge gri bir şekilde. Çalıştırdık ama aktif olmadığını gösteriyor. Biz uygulamayı aktif etmemiz gerekiyor.



İp seçeneklerimizden 4. Seçeneği seçip, start as application diyerek uygulamayı aktifleştiriyoruz.



Artık oyun sunucum çalışıyor demektir.

4)Photon SDK'sını gelen anlatımı | Unity ile sunucumuza bağlanma ve test

!UDP: Geniş alan ağlarında gerçek zamanlı ses ve görüntü gibi veri aktarımlarında kullanılır. UDP –TCP arasındaki en büyük fark gönderilen verinin gidip gitmediğini sorgulamıyor bu nedenle hızlıdır.

Ancak UDP güvenilir olmayan aktarım türüdür. Kontrol olmadığı için.

!TCP: Geniş alan ağlarında gerçek zamanlı ses ve görüntü gibi veri aktarımlarında kontrollü bir şekilde aktarım sağlar. Ve UDP'ye göre daha yavaştır.

UDP daha güvenli hale kendimiz getirerek kullanabiliriz.

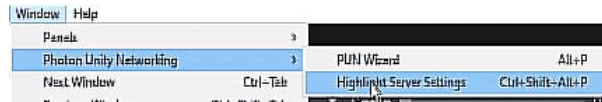
30-Photon başlattığımızda iki sunucu başlar. Biri ana sunucu (Lobby ve oda işlemleri) game sunucu ise oyun işlemlerini yaptığımız sunucudur.

Name	Date modified	Type	Size
GameServer	2/9/2016 3:24 PM	File folder	
Master	2/9/2016 3:24 PM	File folder	

31-Sistem performanslarımızı ise buradan görebiliyoruz

The screenshot shows the Photon Control interface. On the left, there is a menu with options like 'Start Photon', 'Install Counters', 'Remove Counters', 'Create Logging Set', 'Start Logging', 'Stop Logging', and 'Remove Logging Set'. The main window displays a 'System Summary' tab with various performance metrics for the WPHOTONSYSTEM, including memory usage, network interface, physical disk, and processor information.

32-Unity ile bağlanma işlemini görelim.



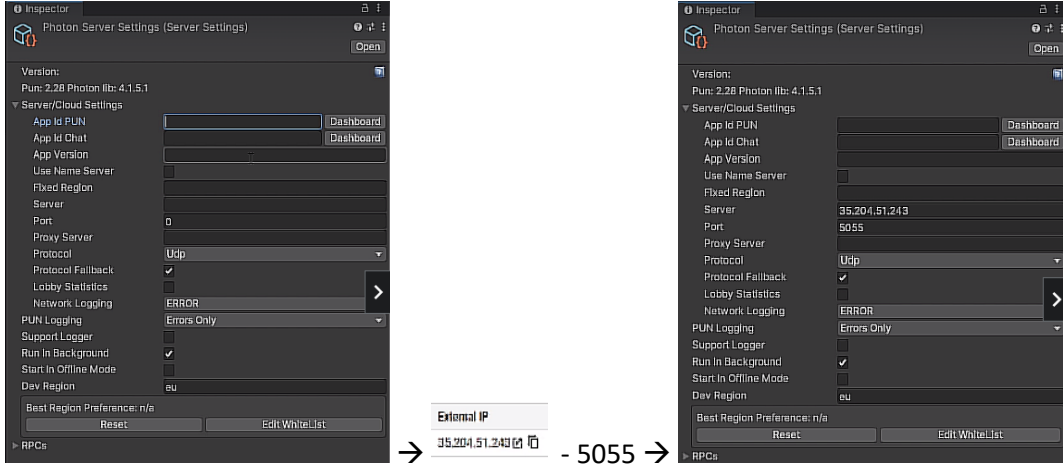
Hiçbir ayar girilmemesi gerekiyor. Sonrasında ip ve portumuzu girip, photon bağlanmış oluyoruz.

Portu nasıl bulacağımızı soruyorsan Photon server dokümantasyonunu açıyoruz. Operations → TCP and UDP Port Numbers seçeneğine tıklıyoruz.

Zaten bizim port ayarlarında yaptığımız port numaramızdır.

Port Number	Protocol	Purpose
4520	TCP	(Internal, 525) Game Server to Master Server
843	TCP	Flash / Unity Polloy
943	TCP	Silverlight Policy
5055	UDP	LoadBalancing: Client to Master Server (UDP)
5056	UDP	LoadBalancing: Client to Game Server (UDP)
4530	TCP	LoadBalancing: Client to Master Server (TCP)
4531	TCP	LoadBalancing: Client to Game Server (TCP)
9090	TCP	LoadBalancing: Client to Master Server (WebSockets)
9091	TCP	LoadBalancing: Client to Game Server (WebSockets)
5055	UDP	MMO Demo (UDP)
4530	TCP	MMO Demo (TCP)
9090	TCP	MMO Demo (WebSockets)

The screenshot shows the Photon Operations menu in the Unity interface. The 'TCP and UDP Port Numbers' option is highlighted, and an arrow points to the table above.



Script tarafında ise herhangi bir farklı bir şey yapmana gerek yok.

!FAZLADAN BİLGİ

```
Unity İletisi | 0 başvuru
private void Update()
{
    Pingdegeri.text = "Ping : " + PhotonNetwork.GetPing().ToString();
    // Debug.Log(PhotonNetwork.NetworkClientState); // Serverin Bağlantı durumunu gösterir.
}
```

!SON OLARAK BİZ HANGİ PROTOKOLDEN BAĞLANICAĞSAK ONU SEÇİYOR OLMAMIZ GEREKİYOR.

