



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

## COMO CONFIGURAR UMA VPN AZURE “POINT TO SITE”



*Cristiano Ribeiro*

Com a pandemia e a popularização do home office, se tornou cada vez mais comum pessoas conseguirem acessar os recursos da empresa de qualquer lugar do mundo. Isso acontece graças a tecnologias como a **VPN Azure**, que é um túnel criptografado que faz conexão entre sua rede privada e aos recursos do Azure tais como Máquinas Virtuais, Bancos de Dados SQL, Armazenamentos de dados e outras aplicações.

Existem três tipos de VPN Azure, são eles:



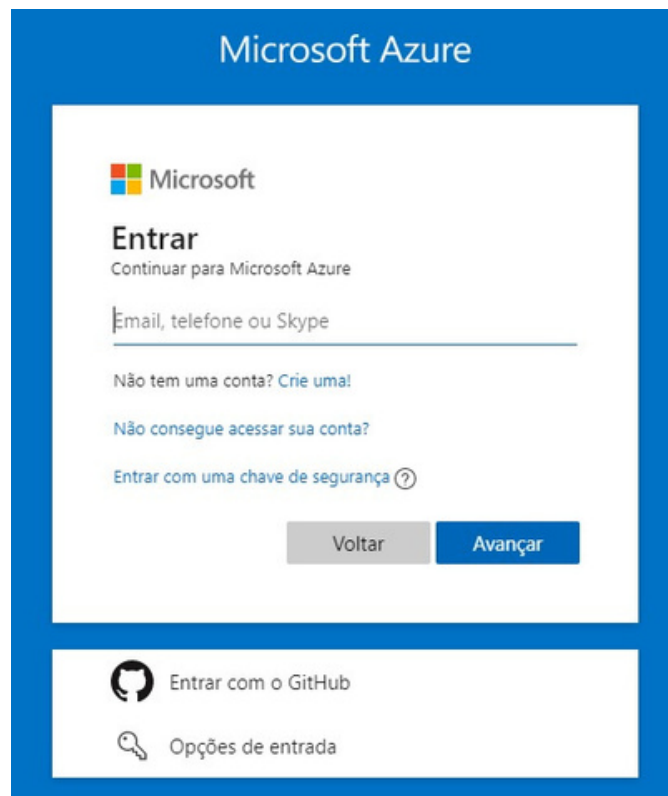
<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

## Pré-requisito

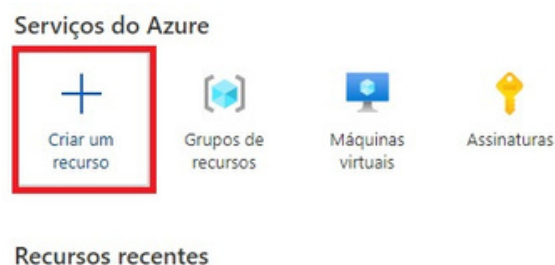
– Assinatura do Azure

## Criando uma VPN no Azure - Passo 1: Criar uma rede virtual

1 – Acesse o site <https://portal.azure.com/> e insira as suas credenciais.



2 – No portal do Azure, clique em “Criar um recurso”.



3 – Pesquise por “Rede Virtual” na barra de pesquisa e clique em “Criar”.



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

Implantar com Gerenciador de Recursos (mudar para Clássico)

Visão geral Planos Informações de Uso + Suporte Revisões

Crie uma seção logicamente isolada no Microsoft Azure com esse serviço de rede. Você pode usando uma conexão IPsec. As Redes virtuais facilitam que você aproveite a infraestrutura aplicativos locais, incluindo sistemas sendo executados no Servidor Windows, mainframes

Use uma Rede virtual para:

4 – Essa é a tela de início para criarmos nossa Rede Virtual. De na o Grupo de Recursos, Nome, região e clique no botão “Avançar: Endereços IP”.

Básico Endereços IP Segurança Marcas Revisar + criar

A VNet (Rede Virtual) do Azure é o bloco de construção fundamental para a sua rede privada no Azure. A VNet habilita muitos tipos de recursos do Azure, como as VMs (Máquinas Virtuais) do Azure, para se comunicar com segurança entre si, a Internet e redes locais. A VNet é semelhante a uma rede tradicional que você operaria no seu próprio data center, mas traz os benefícios adicionais da infraestrutura do Azure, como escala, disponibilidade e isolamento. Saiba mais sobre a rede virtual

**Detalhes do projeto**

Assinatura \* ⓘ Azure para Estudantes

Grupo de recursos \* ⓘ RG\_EmpresaVPN  
[Criar novo](#)

**Detalhes da instância**

Nome \* RG\_Empresa\_Vnet

Região \* (US) Centro-Sul dos EUA

Revisar + criar < Anterior Avançar: Endereços IP > Baixar um modelo para automação

5 – Aqui você pode escolher os endereços IPs disponíveis na sua rede virtual e o número de sub-redes que deseja. Para este exemplo escolhemos o espaço 172.16.0.0/16 e o intervalo de endereço de sub-rede 172.16.0.0/24. Depois de escolher o “Espaço de endereço IP”, clique em “Avançar: Segurança”.



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

+ Adicionar sub-rede    - Remover sub-rede

<input type="checkbox"/> Nome da sub-rede	Intervalo de endereço de sub-rede	Gateway NAT
<input type="checkbox"/> empresa-vnet	172.16.0.0/24	-

**i** É recomendável o uso de um gateway da NAT para o acesso de saída da Internet a partir de uma sub-rede. Você pode implantar um gateway da NAT e atribuí-lo a uma sub-rede depois de criar a rede virtual. [Saiba mais](#)

[Revisar + criar](#)    < Anterior    **Avançar: Segurança >**    [Baixar um modelo para automação](#)

6 – Na guia “Segurança”, temos 3 opções disponíveis:

**Bastionhost:** Fornece conexão SSH/RDP para a sua máquina virtual via Portal do Azure.

**DDos:** Funcionalidade que protege a sua rede virtual de ataques DDos.

**Firewall:** Recurso baseado em nuvem que protege os recursos da sua rede virtual.

Como estamos fazendo uma implantação simples, manteremos o padrão. Clique em “Revisar + Criar > Criar”.



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

DDoS ⓘ	<input type="radio"/> Habilitar
Firewall ⓘ	<input checked="" type="radio"/> Desabilitar
	<input type="radio"/> Habilitar

<b>Revisar + criar</b>	< Anterior	Avançar: Marcas >
------------------------	------------	-------------------

**7** – O processo de implantação pode levar alguns minutos. Para acompanhar o processo de implantação, clique no ícone do sino e quando a implantação terminar, clique em “Ir para o recurso”.

Pesquisar recursos, serviços e documentos (G+/)

| Visão Geral ↗ ...

Anterior ↻ Atualizar

→

Concluída

Notificações

Mais eventos no log de atividades →

✔ Implantação bem-sucedida

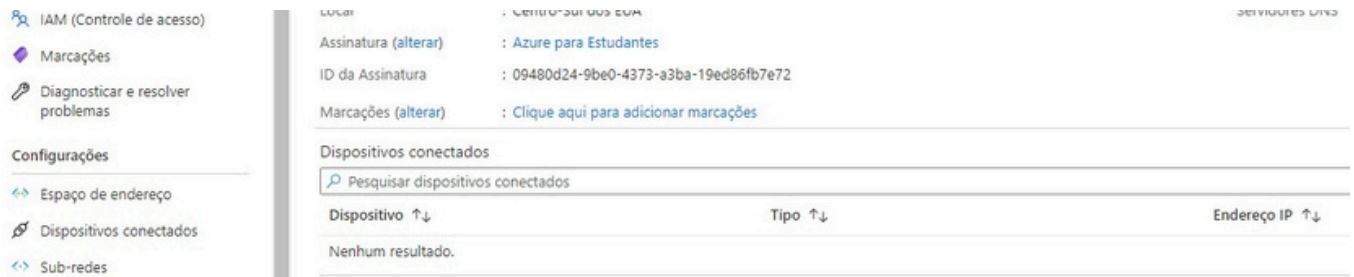
Êxito ao implantar 'Microsoft.VirtualNetwork-20210 recursos 'RG\_EmpresaVPN'.

**Ir para o recurso** ⚙ Fixar no painel

**8** – A rede virtual foi criada com sucesso.

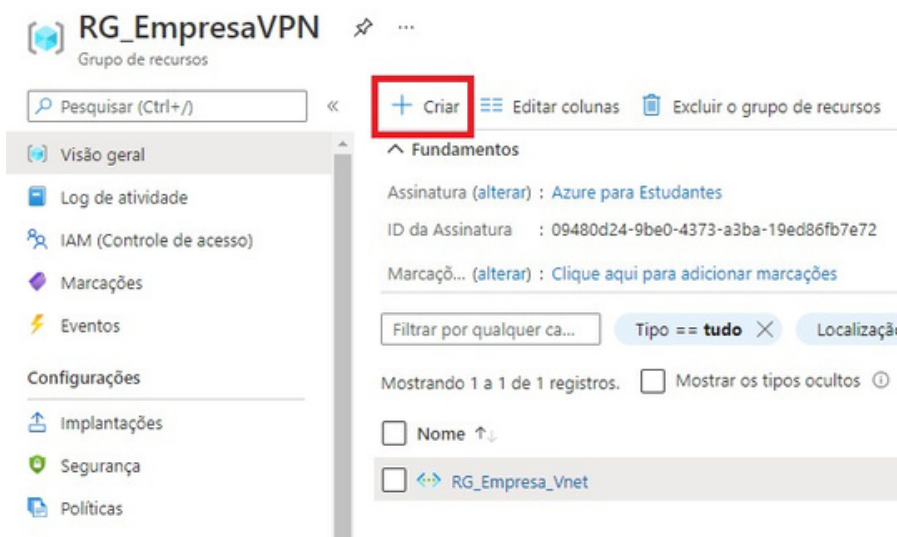


<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>



## Passo 2: Criar uma Gateway de Rede Virtual

9 – Precisaremos de um Gateway de Rede virtual para que a nossa rede virtual seja acessível por meio da VPN. Dentro do nosso grupo de recursos, clique em “Criar” para criarmos mais um recurso.



10 – Procure pelo recurso “Virtual Network Gateway” ou “Gateway de Rede Virtual” e quando encontrar e clique em “Criar”.



11 – Aqui definiremos alguns parâmetros para nosso gateway. Obs: A região do gateway deve ser a mesma região da rede virtual criada anteriormente. Caso contrário, não será possível ligar o gateway a nossa rede virtual.

**Nome:** Definiremos um nome do recurso.

**Região:** Definiremos a região do recurso.



**Tipo de Gateway:** Utilizaremos o “VPN” pois não temos um circuito ExpressRoute.

**Tipo de VPN:** Como não estamos criando um gateway para coexistir com um gateway do ExpressRoute e nem utilizaremos IKEv2, escolheremos o “Baseado em rota”.

**SKU:** Essa opção define as funcionalidades do gateway de VPN. Utilizaremos o “VpnGw1” que permite 30 túneis de site a site e 650Mbps de taxa de transferência.

**Rede Virtual:** Nesse campo utilizaremos a rede virtual que criamos para associá-la ao gateway.

**Intervalo de endereços de sub-rede do gateway:** Essa parte apenas aparece se você não tiver um gateway de sub-rede. Seguiremos a recomendação da microsoft e utilizaremos um CIDR /27.

## Criar gateway de rede virtual ...

Básico Marcas Revisar + criar

O Azure forneceu um guia de planejamento e design para ajudar você a configurar as diversas opções de gateway de VPN. [Saiba mais.](#)

### Detalhes do projeto

Selecione a assinatura para gerenciar os custos e os recursos implantados. Use grupos de recursos como pastas para organizar e gerenciar todos os seus recursos.

Assinatura \* Azure para Estudantes

Grupo de recursos ① RG\_EmpresaVPN (derivado do grupo de recursos da rede virtual)

### Detalhes da instância

Nome \* RG\_Empresa\_Vnet\_GW ✓

Região \* Centro-Sul dos EUA

Tipo de gateway \* ① ☒ VPN ☐ ExpressRoute

Tipo de VPN \* ① ☒ Baseado em rota ☐ Baseado em política

SKU \* ① VpnGw1

Geração ① Generation1

Rede virtual \* ① RG\_Empresa\_Vnet

[Criar rede virtual](#)

① São listadas apenas as redes virtuais na assinatura e na região selecionadas no momento.

Intervalo de endereços de sub-rede do gateway \* ① 172.16.1.0/27 ✓

172.16.1.0- 172.16.1.31 (32 endereços)

**12 –** Após o campo “intervalo de endereços de sub-rede do gateway” criaremos um novo IP público para o nosso gateway. Manteremos o padrão no restante das opções.

Clique em “Revisar + criar” e depois em “Criar”.

*Obs: Um gateway de rede virtual pode levar até 40 minutos para ser criado.*



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

Habilitar o modo ativo-ativo \* ⓘ

☐ Habilitado ☒ Desabilitado

Configurar BGP \* ⓘ

☐ Habilitado ☒ Desabilitado

O Azure recomenda o uso de um dispositivo VPN validado com o seu gateway de rede virtual. Para ver uma lista de dispositivos validados e instruções de configuração, consulte o [documentação](#) do Azure sobre dispositivos VPN validados.

Revisar + criar

Anterior

Avançar: Marcas >

Baixar um modelo para automação

13 – Com a implantação concluída, clique em “Ir para o recurso”.

### ✓ A implantação foi concluída



Nome da implantação: Microsoft.VirtualNetworkGateway-2021080...  
Assinatura: Azure para Estudantes  
Grupo de recursos: RG\_EmpresaVPN

Hora de início: 08/08/2021 19:24:19  
ID de Correlação: 465dac92-79ad-478a-a323-42e2313a8771

▼ Detalhes de implantação (Baixar)

▲ Próximas etapas

Ir para o recurso

14 – Dentro do recurso, vá na opção “Configuração de ponto a site” no menu a esquerda. Nosso ponto a site ainda não está configurado, clique em “configurar agora” para configurar.



15 – Nessa configuração temos as seguintes opções:

**Pool de endereços:** Aqui definiremos a faixa de endereços IPs que os dispositivos irão utilizar ao se conectar na VPN.

**Tipo de túnel:** Aqui você poderá escolher o protocolo para o túnel VPN. Você tem as seguintes opções disponíveis.

ACEITO  
OpenVPN (SSL)



SSTP (SSL)

IKEv2





IKEv2 e OpenVPN (SSL)



IKEv2 e SSTP (SSL)


Utilizaremos o “SSTP (SSL)”. Cada protocolo necessita de uma liberação de porta específica no firewall. A opção que escolhemos utiliza a porta 443 que normalmente já está liberada nos firewalls.

**Tipo de autenticação:** Utilizaremos a opção “Certificado Azure”. Nos próximos passos, geraremos certificados no host cliente para fazer a autenticação na VPN.


 Salvar  Descartar  Excluir  Baixar cliente VPN

---


Pool de endereços \*

10.0.0.0/24 


Tipo de túnel

SSTP (SSL) 


Tipo de Autenticação

Certificado do Azure 

Certificados raiz

Nome	Dados de certificado público
<input type="text"/>	<input type="text"/> 

Certificados revogados

Nome	Impressão digital
<input type="text"/>	<input type="text"/> 

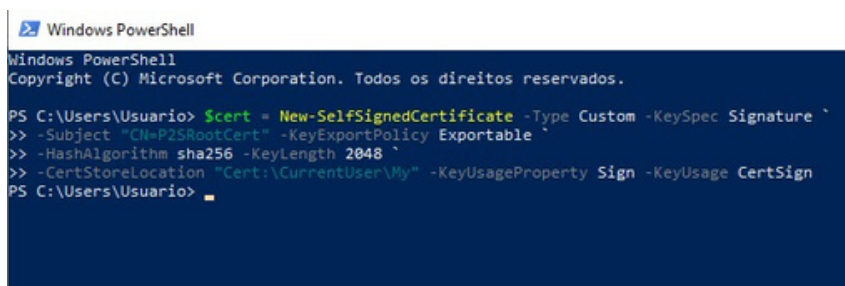
### Passo 3: Geração de Certificados

**16** – Os certificados são necessários para que haja uma autenticação em uma conexão ponto a site. Na máquina local com um Windows 10, entre no Windows Powershell. Geraremos dois certificados, um certificado raiz autoassinado e um certificado do cliente.

Começaremos criando o certificado de raiz autoassinado. Cole o comando:

```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

E dê “Enter”.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

PS C:\Users\Usuario> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Users\Usuario>
```

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
` -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"
```

E dê "Enter".

```
PS C:\Users\Usuario> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $cert -TextExtension @"(2.5.29.37={text}1.3.6.1.5.5.7.3.2)"

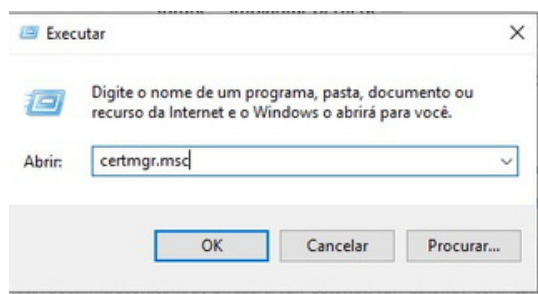
PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                               Subject
-----
4EC031FE8C4959CF4B46E8C3C36A7B2D9421D981 CN=P2SChildCert

PS C:\Users\Usuario>
```

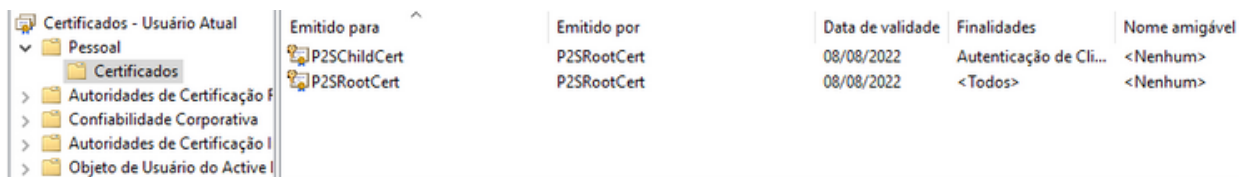
Os dois certificados foram criados com sucesso.

**18** – Precisaremos exportar o certificado para o Azure. Use o atalho "Bandeira + R" e digite "certmgr.msc".



**19** – Vá em "Pessoal > Certificados". Exportaremos o certificado "P2SRootCert".

Para fazer isso, clique com o botão direito no certificado "P2SRootCert" > "Todas as tarefas > Exportar".



**20** – Clique em "Avançar".



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

Um certificado, que é emitido por uma autoridade de certificação, é uma confirmação de sua identidade e contém informações usadas para proteger dados ou estabelecer conexões de rede seguras. Um repositório de certificados é a área do sistema em que os certificados são mantidos.

Para continuar, clique em Avançar.

Avançar

Cancelar

**21** – Não vamos exportar a chave privada. Clique em “Avançar”.

← Assistente para Exportação de Certificados

#### Exportar Chave Privada

Você pode optar por exportar a chave privada com o certificado.

As chaves privadas são protegidas por senha. Para exportar a chave privada com o certificado, você deverá digitar uma senha em uma página mais adiante.

Deseja exportar a chave privada com o certificado?

- ☐ Sim, exportar a chave privada
- ☒ Não, não exportar a chave privada

Avançar

Cancelar

**22** – Escolha a opção “X.509 codificado na base 64 (\*.cer)” e clique em “Avançar”.



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

☐ Arquivo binário codificado por DER (\*.cer)  
☒ X.509 codificado na base 64 (\*.cer)  
☐ Padrão de Sintaxe de Mensagens Criptografadas - Certificados PKCS n°7 (\*.p7b)  
☐ Incluir todos os certificados no caminho de certificação, se possível  
☐ Troca de Informações Pessoais - PKCS n° 12 (.PFX, .P12)  
☐ Incluir todos os certificados no caminho de certificação, se possível  
☐ Excluir a chave privada se a exportação tiver êxito  
☐ Exportar todas as propriedades estendidas  
☐ Habilitar privacidade de certificados  
☐ Repositório de Certificados Serializado da Microsoft (.SST)

Avançar Cancelar

**23** – Aqui escolheremos o nome do arquivo e onde vamos salvá-lo. Clique em “Procurar” para especificar o local que você deseja salvar. Após ter feito isso, clique em “Avançar”.

Assistente para Exportação de Certificados

**Arquivo a Ser Exportado**  
Especifique o nome do arquivo que você deseja exportar

Nome do arquivo:  
C:\Users\Usuario\Documents\P2SRootCert.cer

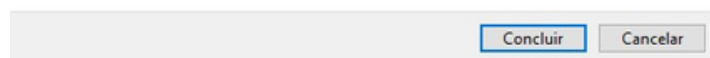
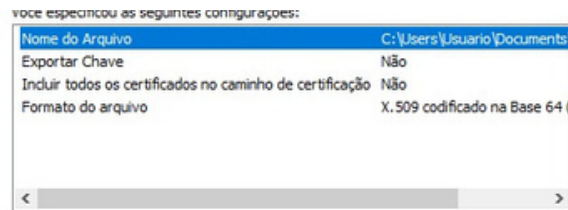
Procurar...

Avançar Cancelar

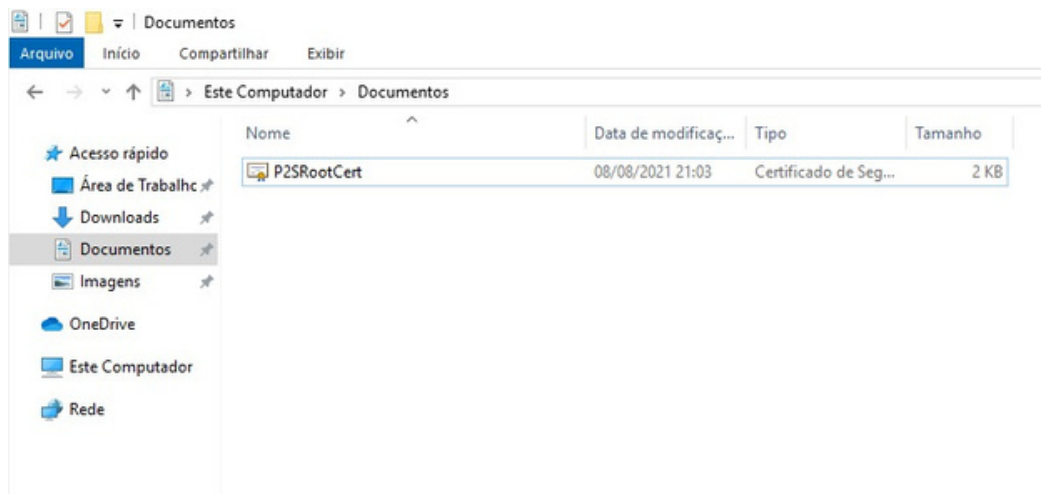
**24** – Aqui você verá um resumo das configurações. Clique em “Concluir”.



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>



25 – Vá até o local onde você salvou o certificado. Na foto abaixo você pode ver como o certificado fica após ser exportado.



26 – Clique com o botão direito no certificado, depois em “Abrir Com > Bloco de notas” e copie o código.



27 – Retorne ao portal do Azure, de uma nova nome para o certificado, cole todo esse código no campo “Dados de certificado público” e clique em “Salvar”. ACEITO



<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>

CERTIFICADO DO AZURE

Certificados raiz

Nome	Dados de certificado público
Empresa_Certificado	MIIC5zCCAc+gAwIBAgIQPSv/2IC+PL9OAT2juNjTsjANBgkqhkiG9w0BAQsFADAU MRQwEgYDVQQDDATQMINSb290Q21 ***

Certificados revogados

Nome	Impressão digital

#### Passo 4: Baixar o cliente VPN na máquina local

28 – Depois de salvar as configurações, clique em “Baixar cliente VPN”.

Salvar Descartar Excluir **Baixar cliente VPN**

Pool de endereços \*

10.0.0.0/24

Tipo de túnel

SSTP (SSL)

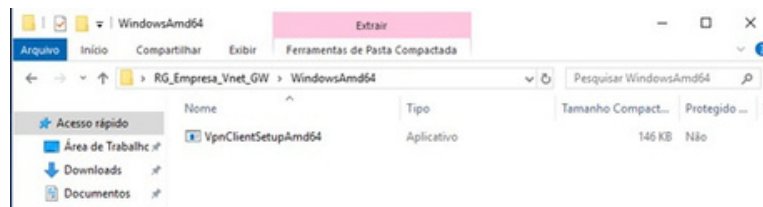
Tipo de Autenticação

Certificado do Azure

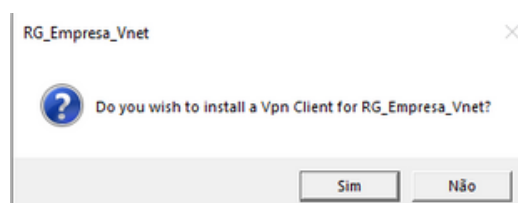
Certificados raiz

Nome	Dados de certificado público
Empresa_Certificado	MIIC5zCCAc+gAwIBAgIQPSv/

29 – Extraia o arquivo baixado, vá em “WindowsAmd64” e clique duas vezes no arquivo executável “VpnClienteSetupAmd64”.



30 – Clique em “Sim” para instalar o cliente VPN.



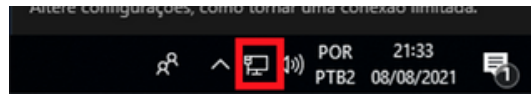
31 – Se você clicar no ícone de rede na barra de tarefas, você vai notar o ícone de VPN. Clique nesse ícone.

Cookie settings





<https://crcloudacademy.herospark.co/p/928c9ab1-3cd3-46b1-8ef5-a4c0e56c0918>



**32** – Você será redirecionado para as configurações. Clique na VPN e depois clique em conectar.

## VPN

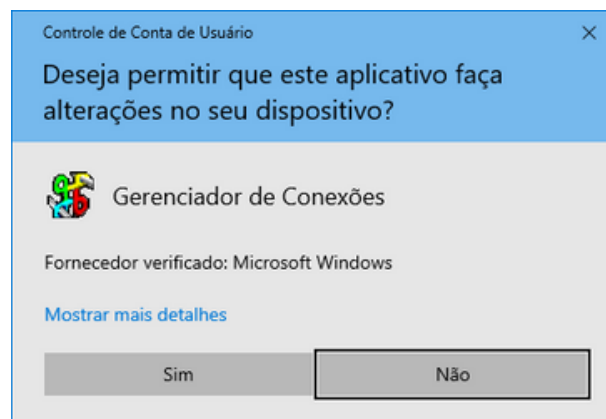


## Opções Avançadas

**33** – Selecione “Não exibir esta mensagem novamente para essa Conexão” e clique em “Continuar”.



**34** – Clique em “Sim” para permitir o gerenciador de conexões.



**35** – O cliente se conectou na VPN com sucesso.