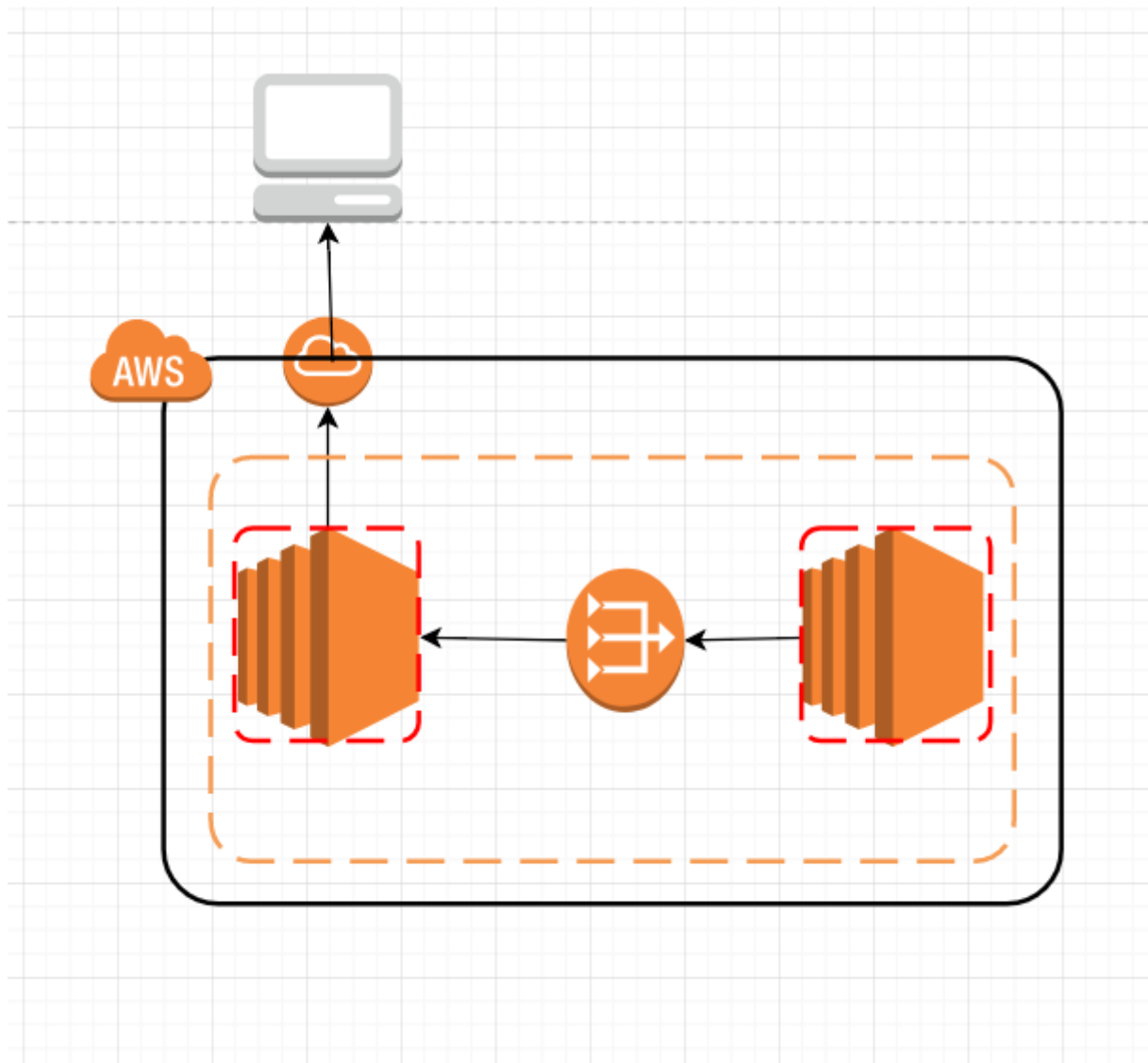


## CREATION OF BASTION (PUBLIC EC2) TO ALLOW A PING WITH A PRIVATE EC2

Diagram of the implementation :



### TASK 1 : Create a VPC with a public and a private subnets

1/ In the **AWS Management Console**, On **services** Menu, Click **VPC**

2/ Click **Start VPC Wizard**

3/ In the navigation pane, click **VPC with Public and Private Subnets**.

4/ Click **Select**

5/ Configure following Settings

**IPv4 CIDR block** : Type : 10.0.0.0/16

**VPC name** : Type : My Work VPC

**Public subnet's IPv4 CIDR** : Type 10.0.1.0/24

**Availability Zone** : click the first availability zone

**Public subnet name** : Public subnet work

**Private subnet's IPv4 CIDR** : Type 10.0.3.0/24

**Availability Zone** : click the first availability zone

**Private subnet name** : Private subnet work

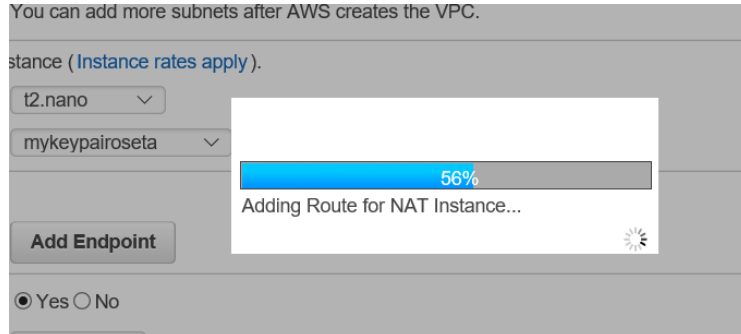
**Specify the details of your Nat Gateway** :

Go to look on the Elastic IP : (as example 34.247.209.197)

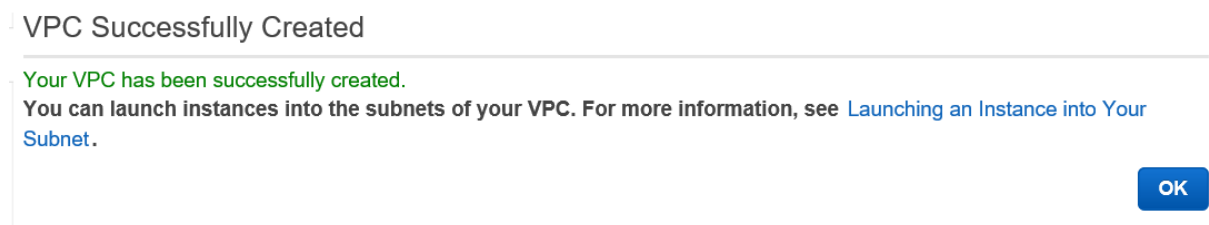
**Key pair name** : Click the key pair.

6/ Click **Create VPC**

You will need to wait



7/ Click **OK** when the VPC is successfully created like below



## TASK 2 : Create Route table for subnets

1/ In the navigation pane, click **Route Tables**.

2/ Select the route table **My Work VPC** and yes under **Main**

- 3/ double click the **Name** for this route table type : Private route table
- 4/ In the lower pane click the **routes** and note that EniXXX is selected
- 5/ Click **Subnet association** and then click **Edit**
- 6/ Select **Private subnet Work**
- 7 / click Save
- 8/ Select the route table **My Work VPC** and no under **Main**
- 9/ double click the **Name** for this route table type : Public route table
- 10/ In the lower pane click the **routes** and note that igwxxx is selected
- 11/ Click **Subnet association** and then click **Edit**
- 12/ Select **Public subnet Work**
- 13/ click Save

### TASK 3 : Create a VPC security group

- 1/ In the navigation pane, click **Security group**
- 2/ Click **Create Security Group**
- 3/ In the Create Security Group


**Name Tag** : work security group

**Group name** : work security group

**Description** : Enable HTTP access







**VPC** : select WORK

- 4/ Click on the new work security group

	work security group	sg-63f5811e	work security group	vpc-95d0a3f3   WORK	Enable HTTP access
---	---------------------	-------------	---------------------	---------------------	--------------------

- 5/ click the **Inbound Rules tab**


- 6/ Click **Edit**

Type	Protocol	Port Range	Source	Description
HTTP (80) 	TCP (6) 	80	0.0.0.0/0 	
RDP (3389) 	TCP (6) 	3389	0.0.0.0/0 	
Add another rule				

### TASK 4 LAUNCH THE INSTANCE :

1/ On the Services menu Console, Select EC2 and click **Launch Instance**

And select the Microsoft Server 2016

**Microsoft Windows Server 2016 Base** - ami-894c7bf0

Windows

Free tier eligible

Microsoft Windows 2016 Datacenter edition. [English]  
Root device type: ebs    Virtualization type: hvm    ENA Enabled: Yes

Select

64-bit

Select the following line (should be the default)

<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
-------------------------------------	-----------------	--------------------------------	---	---	----------	---	-----------------	-----

2/ Click next configure instance details

Network : WORK

Subnet : Public

Auto assign : Enable


3/ click **Review and Launch**

4/ click **Launch**

5/ Select the Keypair with tick I acknowledge

6/ On the Services menu Console, Select EC2 and click **Launch Instance**

And select the Microsoft Server 2016

**Microsoft Windows Server 2016 Base** - ami-894c7bf0

Windows

Free tier eligible

Microsoft Windows 2016 Datacenter edition. [English]  
Root device type: ebs    Virtualization type: hvm    ENA Enabled: Yes

Select

64-bit

Select the following line (should be the default)

<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
-------------------------------------	-----------------	--------------------------------	---	---	----------	---	-----------------	-----

7/ Click next configure instance details

Network : WORK

Subnet : Private

Auto assign : Disable

3/ click **Review and Launch**

4/ click **Launch**

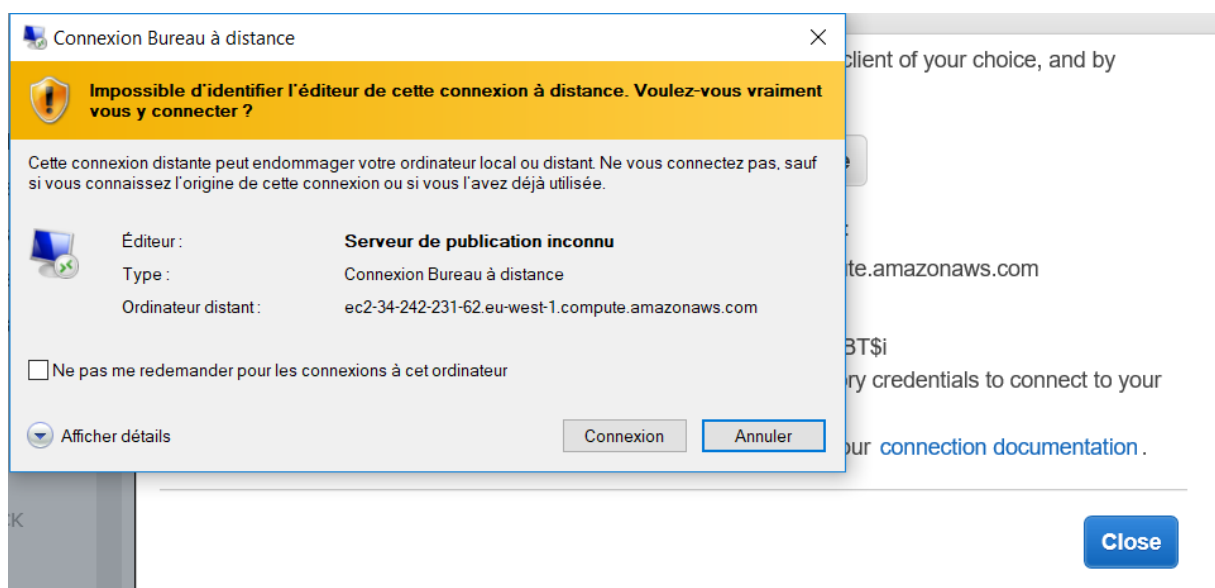
5/ Select the Keypair with tick I acknowledge

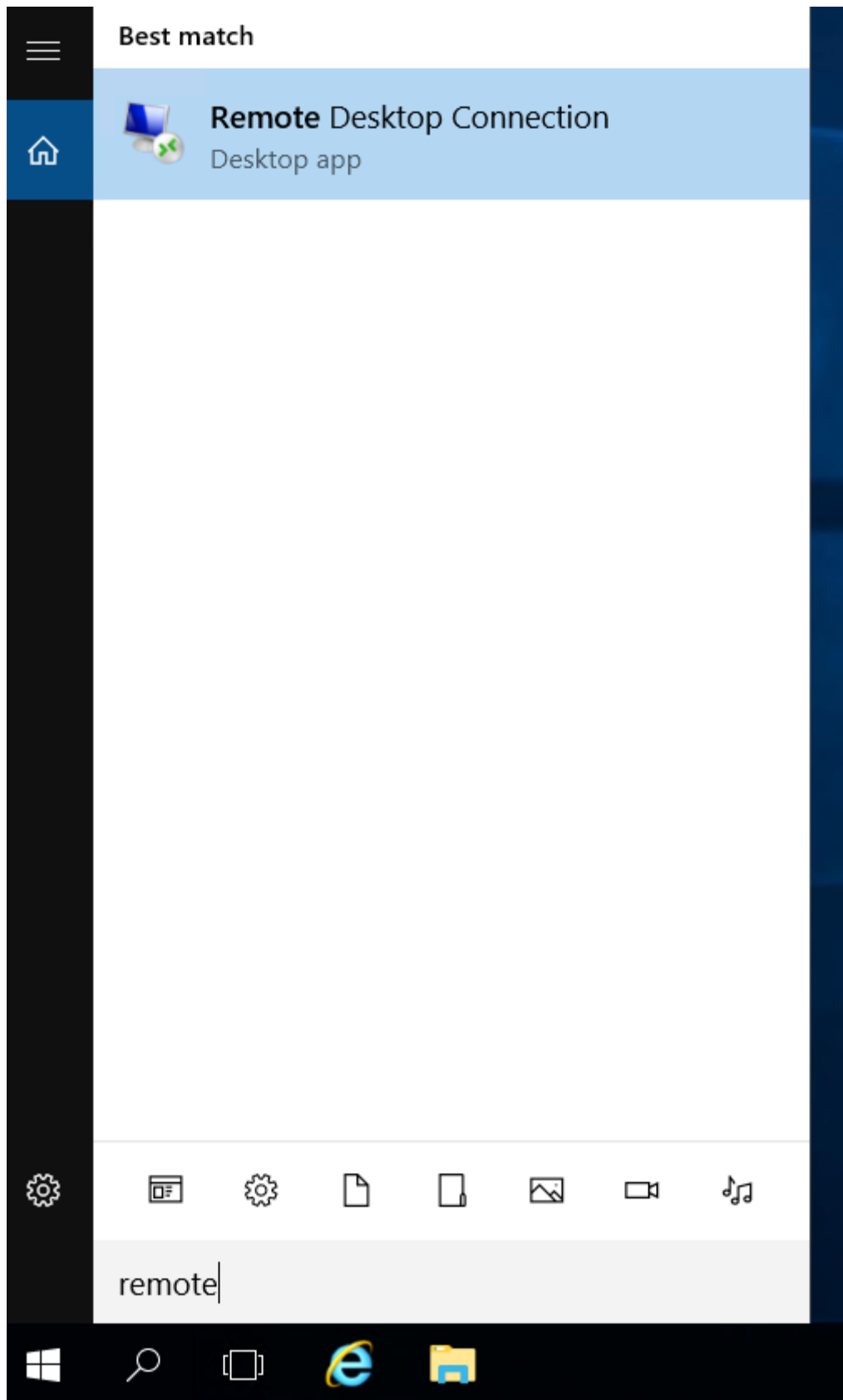
## TASK 5 CONNECT TO THE INSTANCE

1/ In The EC2 select the public Instance and Click on **Connect**

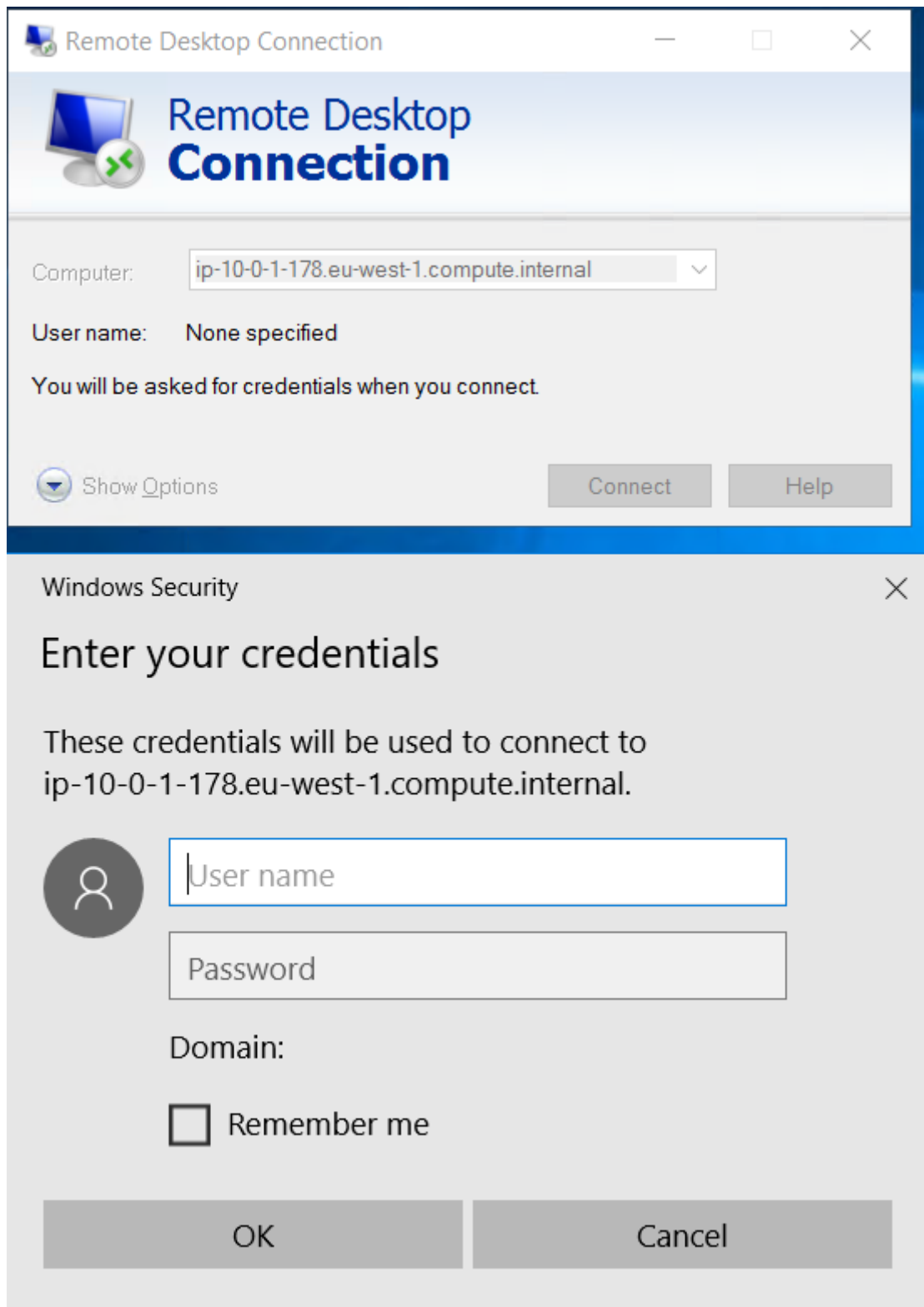
2/ Select the Keyfile and Get the password copy the password.

3/ click on Connection





1/ Do the same operation



The image shows two overlapping Windows dialog boxes. The top box is the 'Remote Desktop Connection' window, which has a title bar with standard Windows window controls. It features a blue header with a computer icon and the text 'Remote Desktop Connection'. Below the header, there is a 'Computer:' label followed by a text box containing 'ip-10-0-1-178.eu-west-1.compute.internal'. Underneath, the 'User name:' is set to 'None specified'. A message states 'You will be asked for credentials when you connect.' At the bottom, there are three buttons: 'Show Options' (with a dropdown arrow), 'Connect', and 'Help'.

The bottom box is a 'Windows Security' dialog titled 'Enter your credentials'. It informs the user that the provided credentials will be used to connect to the same IP address. It contains a user icon, a 'User name' text box, a 'Password' text box, and a 'Domain:' label. There is an unchecked checkbox for 'Remember me'. At the bottom are 'OK' and 'Cancel' buttons.

Remote Desktop Connection

Computer: ip-10-0-1-178.eu-west-1.compute.internal

User name: None specified

You will be asked for credentials when you connect.

Show Options Connect Help

Windows Security

Enter your credentials

These credentials will be used to connect to ip-10-0-1-178.eu-west-1.compute.internal.

User name

Password

Domain:

☐ Remember me

OK Cancel

## First Ping in the Public environment in a Cmd.exe

```
ec2-34-245-56-22 - ec2-34-245-56-22.eu-west-1.compute.amazonaws.com - Connexion Bureau à distance
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [216.58.198.78] with 32 bytes of data:
Reply from 216.58.198.78: bytes=32 time=1ms TTL=46
Reply from 216.58.198.78: bytes=32 time=1ms TTL=46
Reply from 216.58.198.78: bytes=32 time=1ms TTL=46
Reply from 216.58.198.78: bytes=32 time=1ms TTL=46

Ping statistics for 216.58.198.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>
```

## Second Ping in the Private environment in a Cmd.exe

```
ec2-34-245-56-22 - ec2-34-245-56-22.eu-west-1.compute.amazonaws.com - Connexion Bureau à distance
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [209.85.203.100] with 32 bytes of data:
Reply from 209.85.203.100: bytes=32 time=1ms TTL=37
Reply from 209.85.203.100: bytes=32 time=1ms TTL=37
Reply from 209.85.203.100: bytes=32 time=1ms TTL=37
Reply from 209.85.203.100: bytes=32 time=1ms TTL=37

Ping statistics for 209.85.203.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>
```