Guided Lab: Setting Amazon Time Sync Service for Amazon EC2 Windows Instance

Description

Accurate timekeeping is crucial for the proper functioning of many applications and services running on cloud infrastructure. This includes logging events, coordinating distributed processes, and ensuring the security of communications through protocols that rely on synchronized time, such as TLS/SSL. In the AWS ecosystem, ensuring your EC2 instances have the correct time is vital for seamless operation and accurate billing. Guided Lab: Setting Amazon Time Sync Service for Amazon EC2 Instance (Linux)

This guided lab will walk you through configuring and managing time synchronization on a Linux instance running in Amazon EC2. You will learn how to use the Network Time Protocol (NTP) with Chrony, a versatile and powerful time synchronization tool that is the default for many modern Linux distributions. By following these steps, you will ensure your EC2 instance maintains accurate time, improving the reliability and accuracy of time-dependent processes and logs.

Prerequisites

This lab assumes you have basic knowledge of Windows Server operations and Amazon EC2 service.

If you find any gaps in your knowledge, consider taking the following lab:

- How to launch an Amazon EC2 Linux instance

Objectives

In this lab, you will:

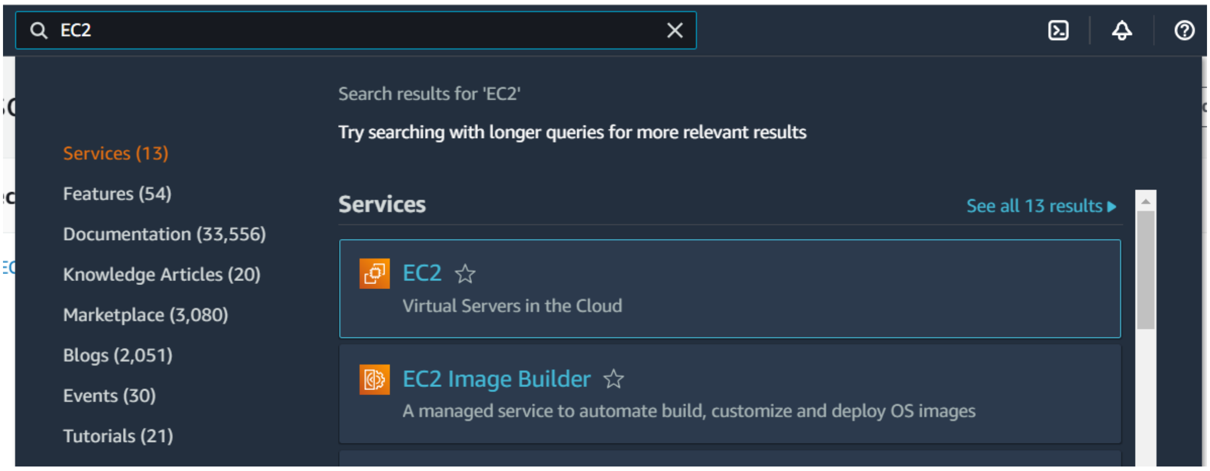
- Verify and configure time synchronization on a Windows EC2 instance.
- Understand the use of Windows Time service for maintaining accurate time.
- Ensure your instance’s time is correctly synchronized with time servers.

Subscribe to access AWS PlayCloud Labs

Lab Steps

Launch an EC2 Instance

1. **Navigate the EC2 Dashboard.**



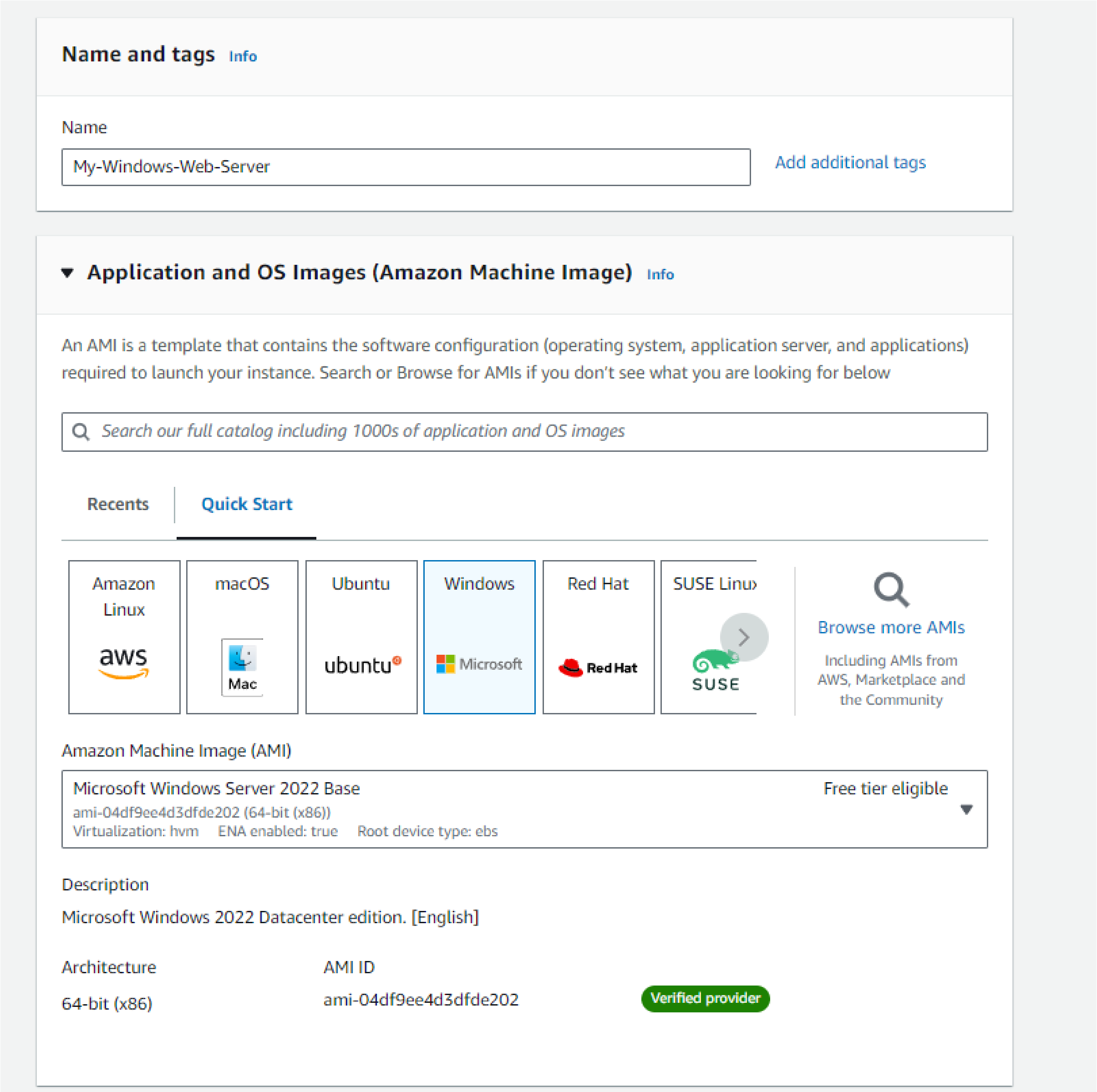
EC2

Search results for 'EC2'

Try searching with longer queries for more relevant results

2. L**aunch an EC2 Instances using the following configurations:**

- Name: **My-Windows-Web-Server**
- AMI: **Microsoft Windows 2022 Base**



Name: My-Windows-Web-Server

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

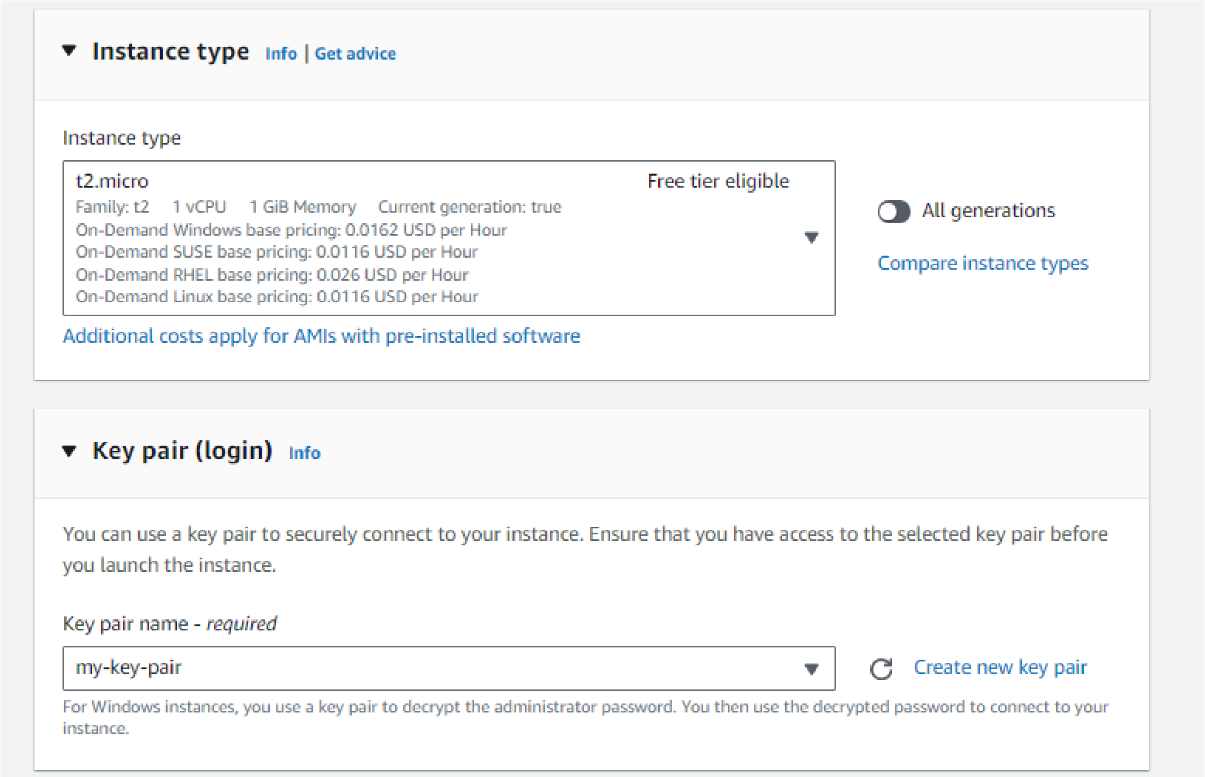
Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base — Free tier eligible
ami-04df9ee4d3dfde202 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Microsoft Windows 2022 Datacenter edition. [English]

Architecture	AMI ID
64-bit (x86)	ami-04df9ee4d3dfde202

- Instance type: **t2.micro**
- Key pair: (**Please create a new one.**)
  - Key pair name: **my-key-pair**
  - Key pair type: **RSA**
  - Private key file format: **.pem**



Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

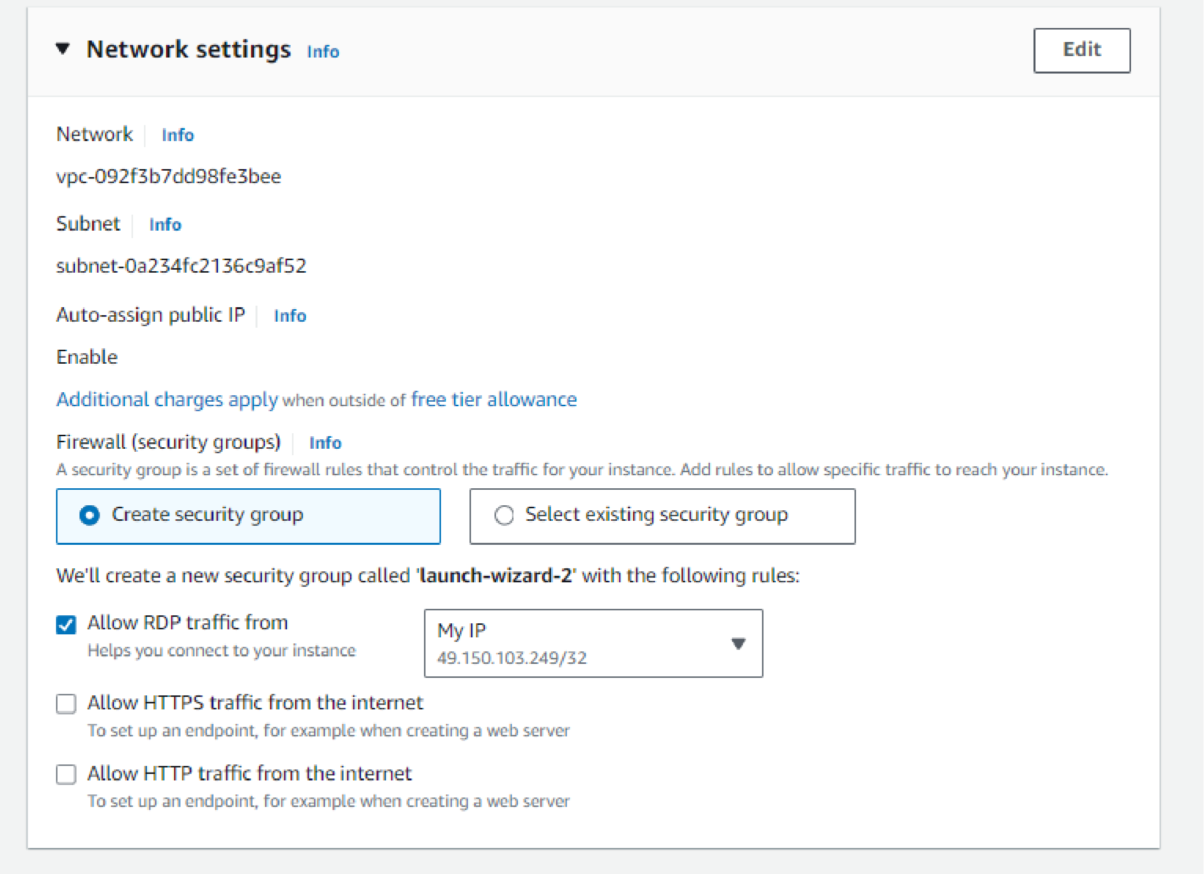
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

my-key-pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

- Network settings:
    - Auto-assign public IP: Select **Enable**
    - Firewall (security groups): tick on the **Create security group**
    - Ensure that **Allow SSH traffic from** is **checked** and is **My IP**



Network Info

vpc-092f3b7dd98fe3bee

Subnet Info

subnet-0a234fc2136c9af52

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-2**' with the following rules:

☑ Allow RDP traffic from — My IP 49.150.103.249/32
Helps you connect to your instance

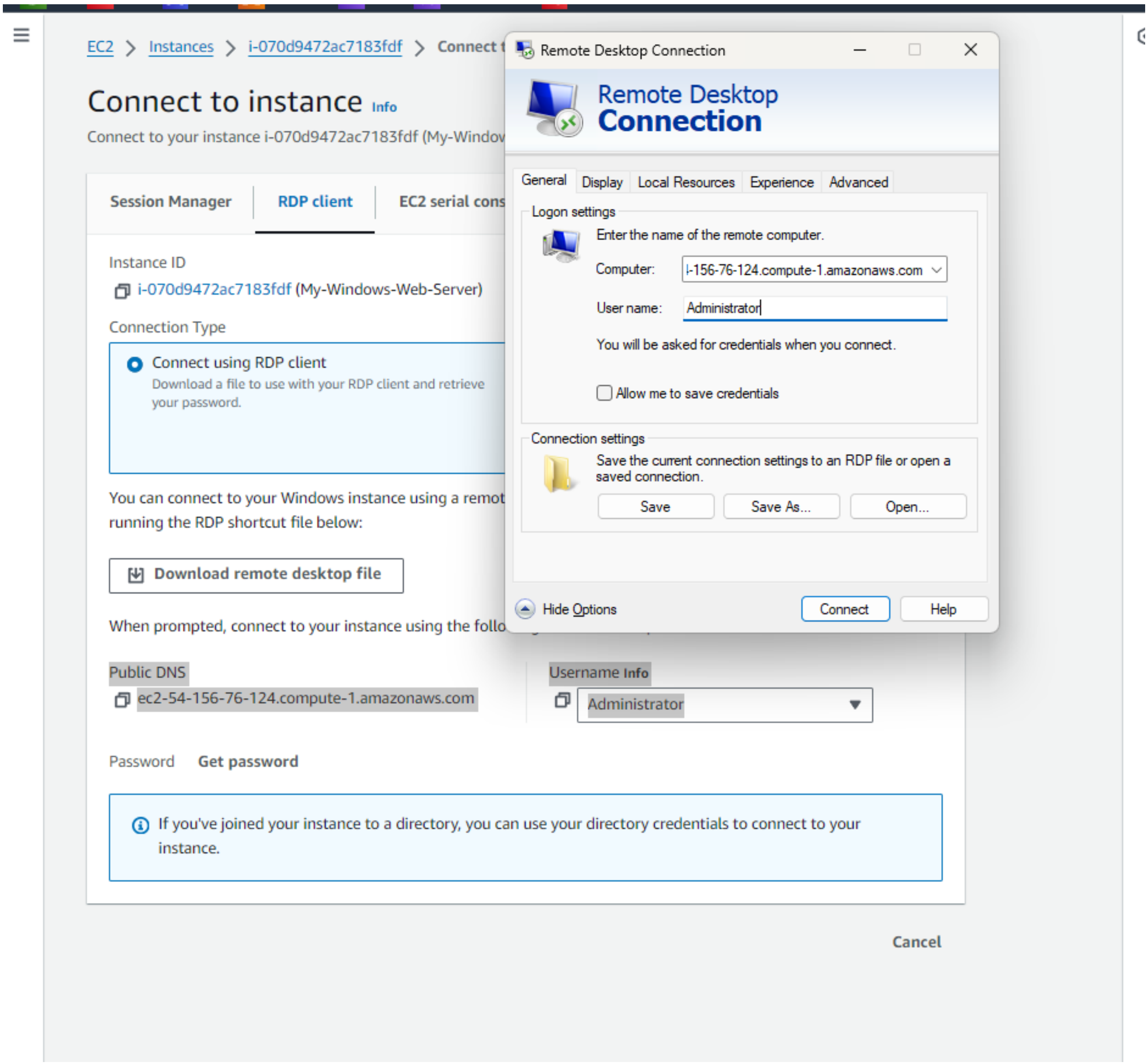
□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

- Click on **Launch instance**

Verify Current Time and Time Zone

1. Connect to your newly created EC2 instance using Remote Desktop Protocol (RDP). Copy The Public DNS and Username to your RDP:



EC2 > Instances > i-070d9472ac7183fdf > Connect t

Connect to instance Info

Connect to your instance i-070d9472ac7183fdf (My-Windov

Session Manager | RDP client | EC2 serial cons

Instance ID

i-070d9472ac7183fdf (My-Windows-Web-Server)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

You can connect to your Windows instance using a remot running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the follo

Public DNS: ec2-54-156-76-124.compute-1.amazonaws.com

Username Info: Administrator

Password: Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

Remote Desktop Connection

Remote Desktop **Connection**

General | Display | Local Resources | Experience | Advanced

Logon settings

Enter the name of the remote computer.

Computer: i-156-76-124.compute-1.amazonaws.com

User name: Administrator

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

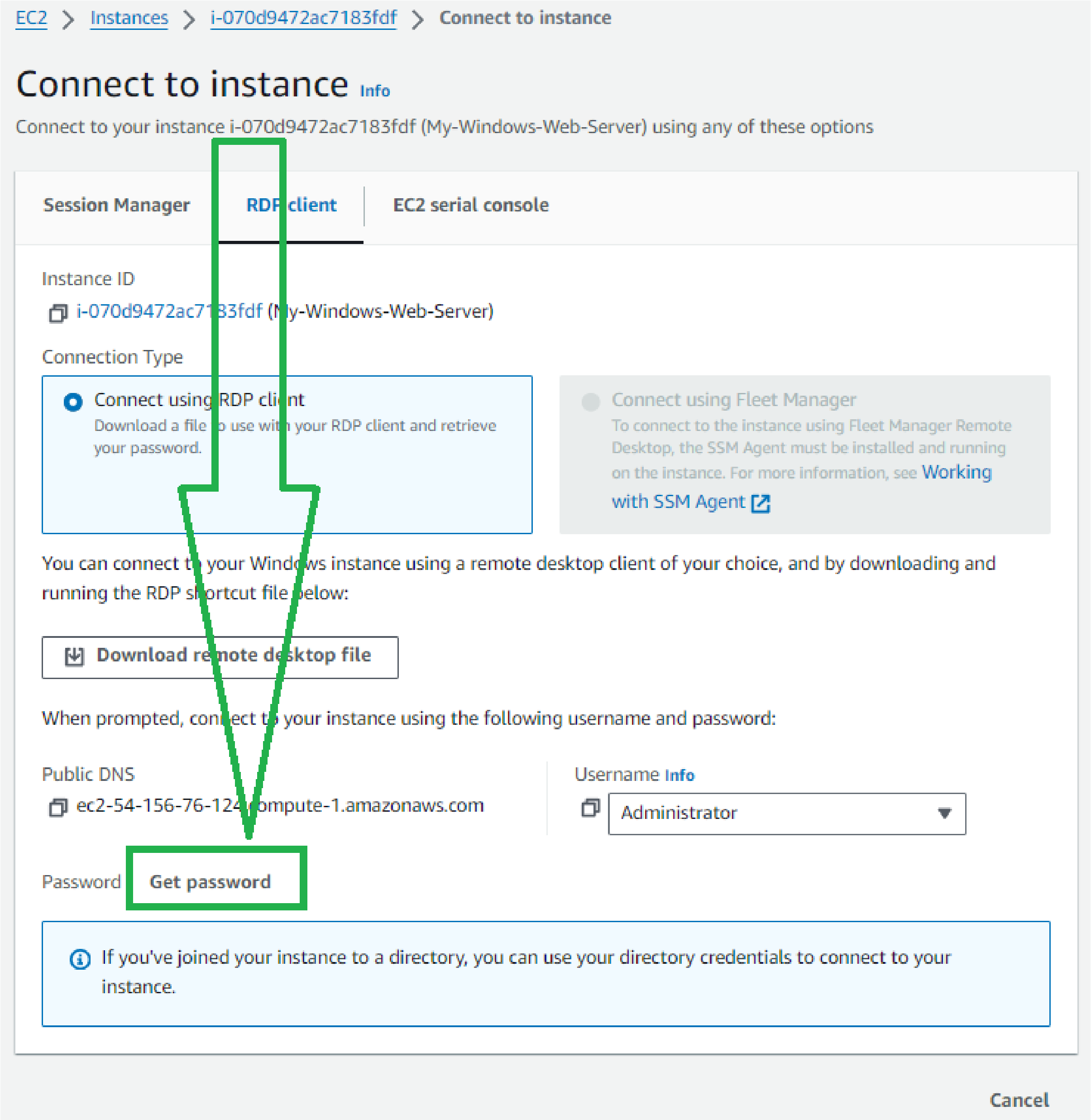
Save the current connection settings to an RDP file or open a saved connection.

Save | Save As... | Open...

Hide Options | Connect | Help

It will prompt you to the password after Clicking **Connect**:

- You can decrypt your password by Clicking the **Get Password** in the Connect to Instance Dashboard under RDP Client of EC2 console.



EC2 > Instances > i-070d9472ac7183fdf > Connect to instance

Connect to instance Info

Connect to your instance i-070d9472ac7183fdf (My-Windows-Web-Server) using any of these options

Session Manager | RDP client | EC2 serial console

Instance ID

i-070d9472ac7183fdf (My-Windows-Web-Server)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the following username and password:

Public DNS
ec2-54-156-76-124.compute-1.amazonaws.com

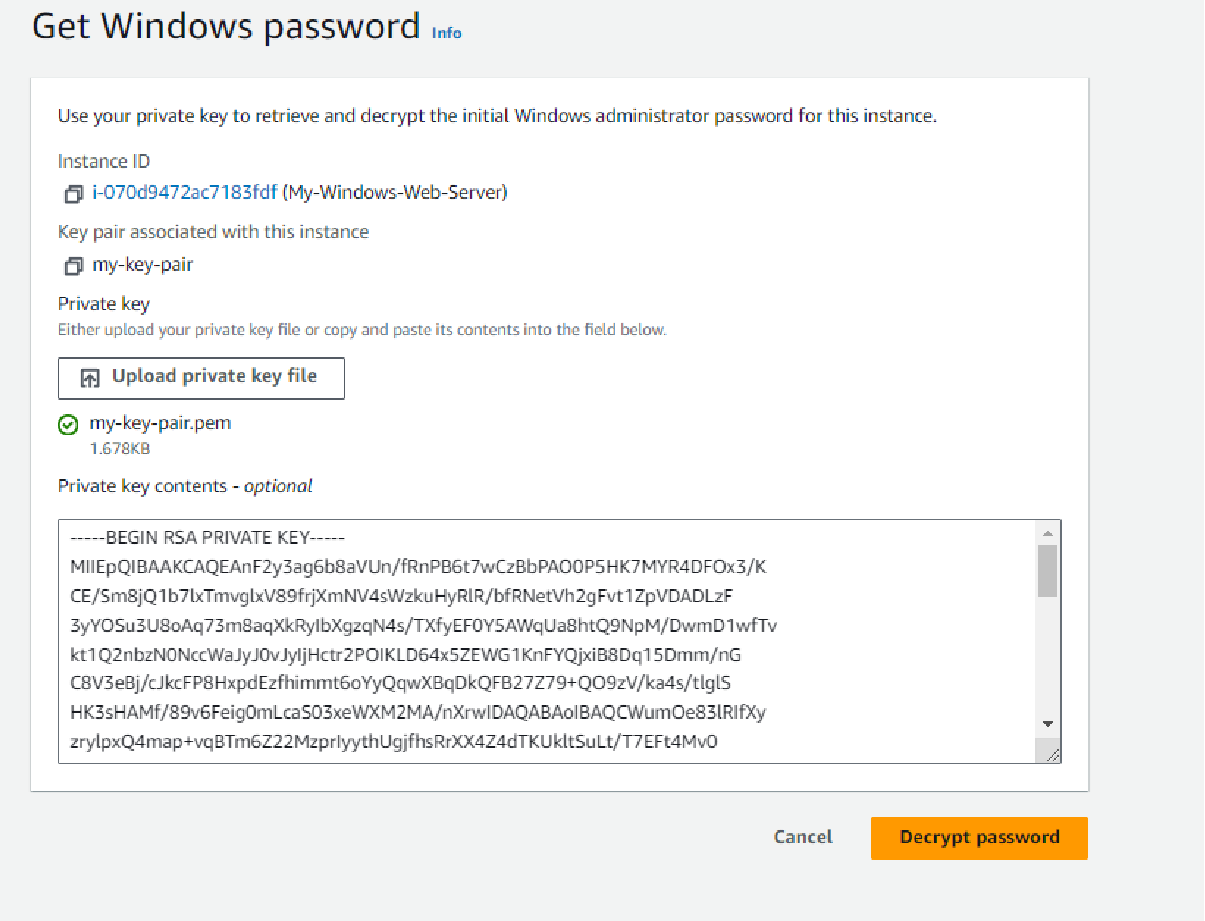
Username Info
Administrator

Password Get password

ⓘ If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

- Next, Upload the **.pem** file of your keypair, and lastly, Clicking **Decrypt password**



Get Windows password

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID

i-070d9472ac7183fdf (My-Windows-Web-Server)

Key pair associated with this instance

my-key-pair

Private key

Either upload your private key file or copy and paste its contents into the field below.

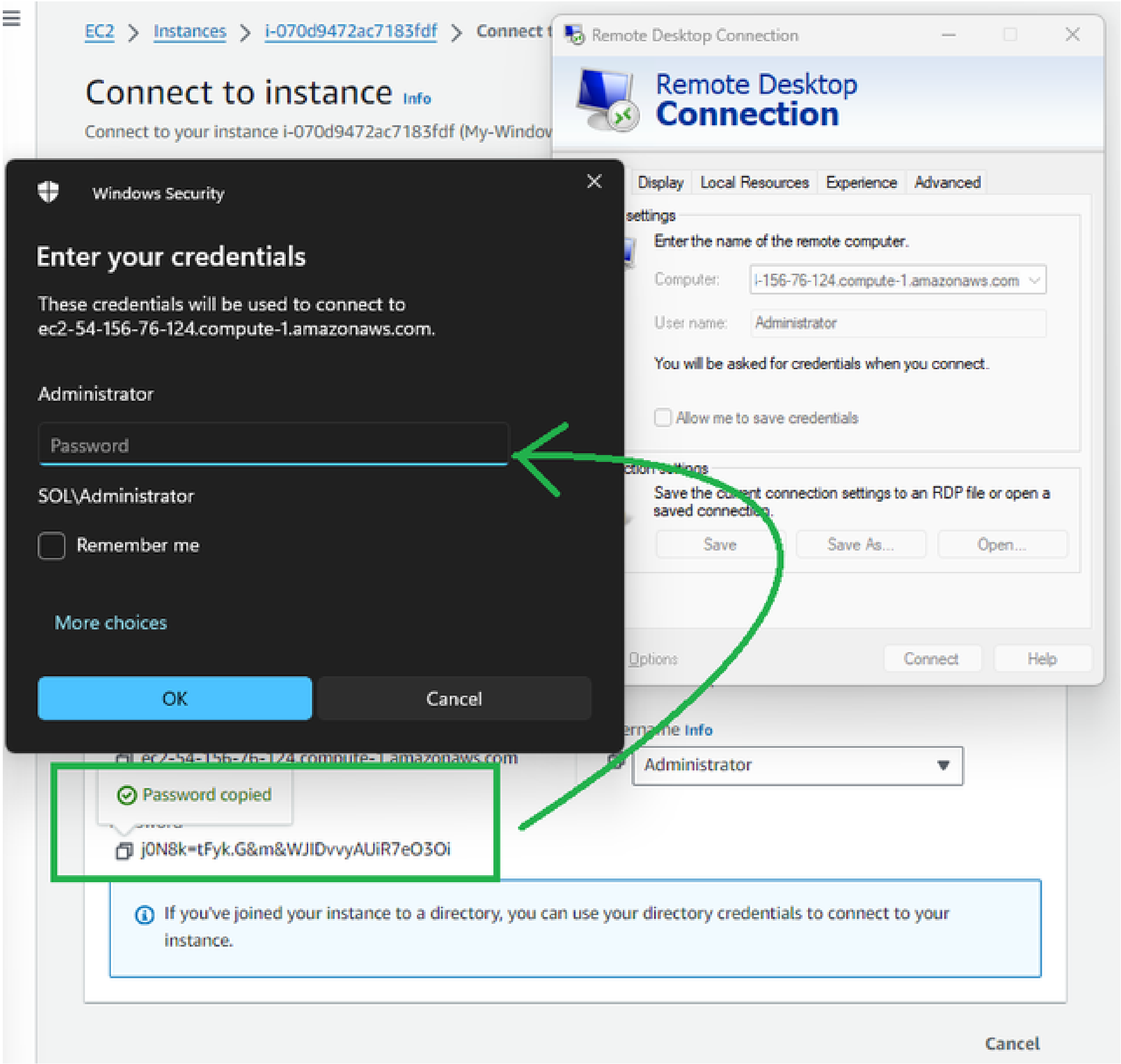
✓ my-key-pair.pem

1.678KB

Private key contents - *optional*

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAnF2y3ag6b8aVUn/fRnPB6t7wCzBbPAO0P5HK7MYR4DFOx3/K
CE/Sm8jQ1b7lxTmvglxV89frjXmNV4sWzkuHyRlR/bfRNetVh2gFvt1ZpVDADLzF
3yYOSu3U8oAq73m8aqXkRyIbXgzqN4s/TXfyEF0Y5AWqUa8htQ9NpM/DwmD1wfTv
kt1Q2nbzN0NccWaJyJ0vJyIjHctr2POIKLD64x5ZEWG1KnFYQjxiB8Dq15Dmm/nG
C8V3eBj/cJkcFP8HxpdEzfhimmt6oYyQqwXBqDkQFB27Z79+QO9zV/ka4s/tlglS
HK3sHAMf/89v6Feig0mLcaS03xeWXM2MA/nXrwIDAQABAoIBAQCWumOe83lRIfXy
zrylpxQ4map+vqBTm6Z22MzprIyythUgjfhsRrXX4Z4dTKUkltSuLt/T7EFt4Mv0
```

- Copy and paste the password.



EC2 > Instances > i-070d9472ac7183fdf > Connect t

Connect to instance Info

Connect to your instance i-070d9472ac7183fdf (My-Windov

Windows Security

Enter your credentials

These credentials will be used to connect to ec2-54-156-76-124.compute-1.amazonaws.com.

Administrator

Password

SOL\Administrator

□ Remember me

More choices

Remote Desktop Connection

Remote Desktop Connection

settings

Enter the name of the remote computer.

Computer: i-156-76-124.compute-1.amazonaws.com

User name: Administrator

You will be asked for credentials when you connect.

□ Allow me to save credentials

ction settings

Save the current connection settings to an RDP file or open a saved connection.

ec2-54-156-76-124.compute-1.amazonaws.com

Password copied

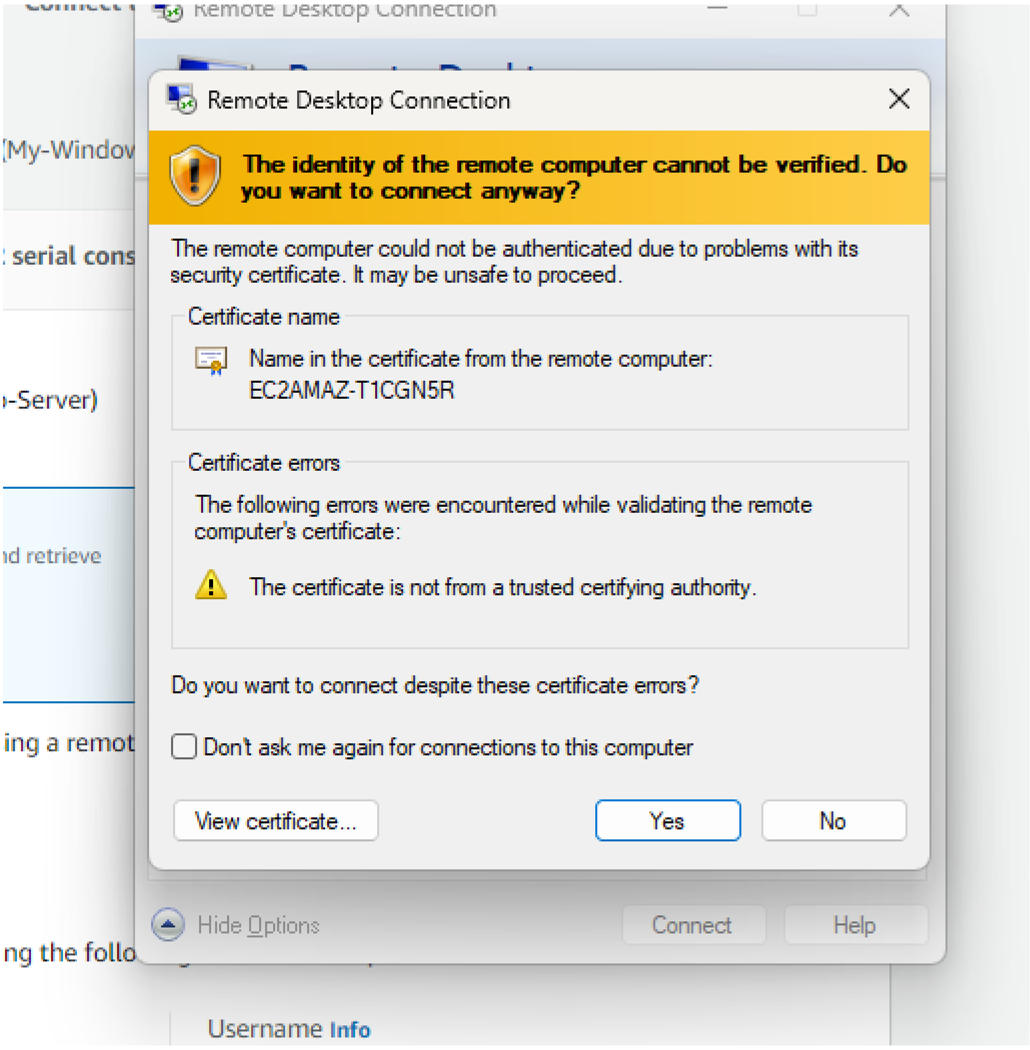
ername Info

Administrator

jON8k=tFyk.G&m&WJIDvvyAUiR7eO3Oi

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

- Click yes, when prompted:



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
EC2AMAZ-T1CGN5R

Certificate errors

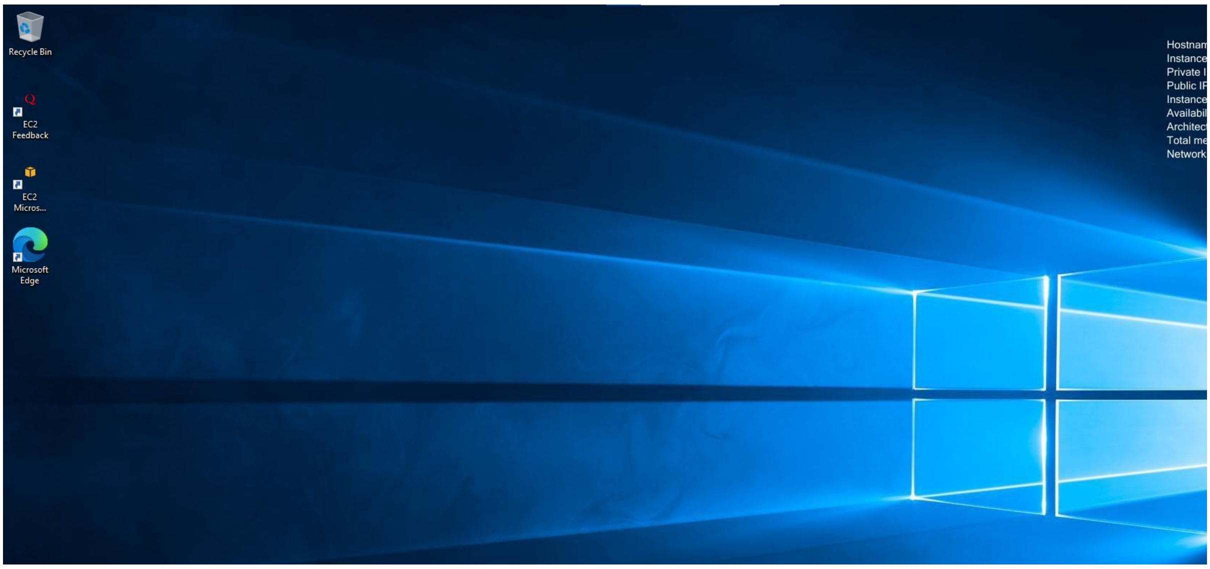
The following errors were encountered while validating the remote computer's certificate:

⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

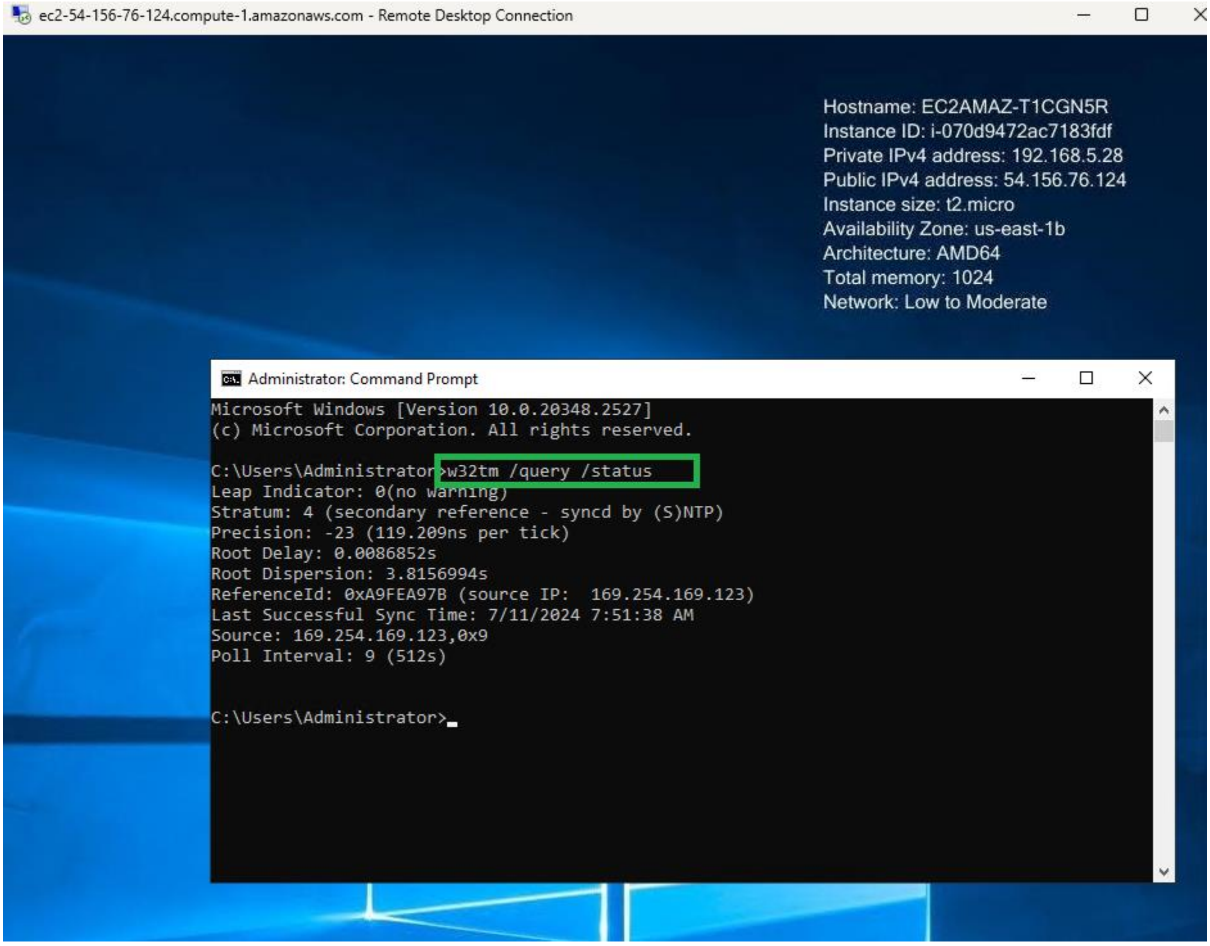
- And you should be connected to your Windows Instance



2. Check the current system time and time zone:

- Open the Command Prompt and type:

w32tm /query /status



ec2-54-156-76-124.compute-1.amazonaws.com - Remote Desktop Connection
Administrator: Command Prompt

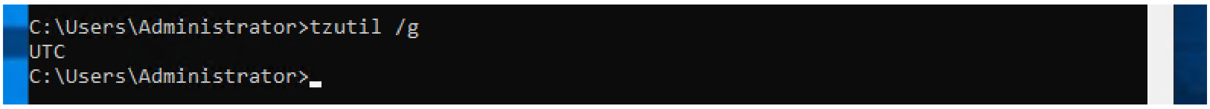
Hostname: EC2AMAZ-T1CGN5R
Instance ID: i-070d9472ac7183fdf
Private IPv4 address: 192.168.5.28
Public IPv4 address: 54.156.76.124
Instance size: t2.micro
Availability Zone: us-east-1b
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate

```
Microsoft Windows [Version 10.0.20348.2527]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0086852s
Root Dispersion: 3.8156994s
ReferenceId: 0xA9FEA97B (source IP:  169.254.169.123)
Last Successful Sync Time: 7/11/2024 7:51:38 AM
Source: 169.254.169.123,0x9
Poll Interval: 9 (512s)


C:\Users\Administrator>_
```

Take note of these details for comparison later

3. Check the time zone settings:

tzutil /g



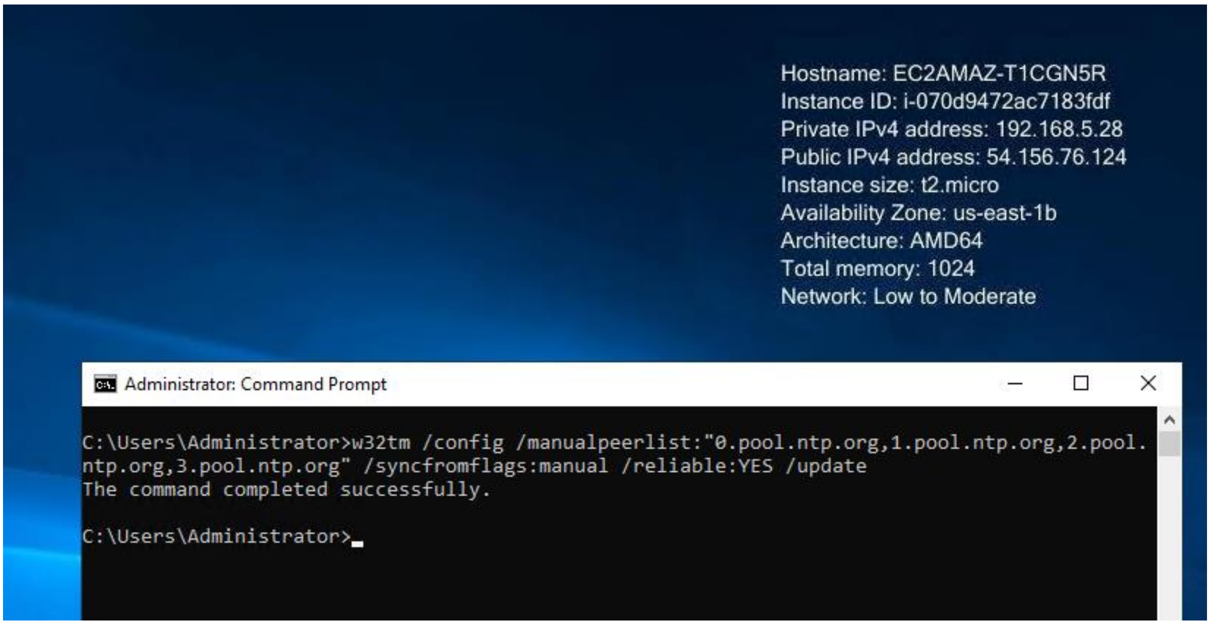
```
C:\Users\Administrator>tzutil /g
UTC
C:\Users\Administrator>_
```

NOTE: you can use the command cls to clear the contents of the terminal screen. It is the same as the clear command in Linux

Configure Windows Time Service

1. Configure the Windows Time service to use a specific NTP server:

w32tm /config /manualpeerlist:"0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org,3.pool.ntp.org" /syncfromflags:manual /reliable:YES /update



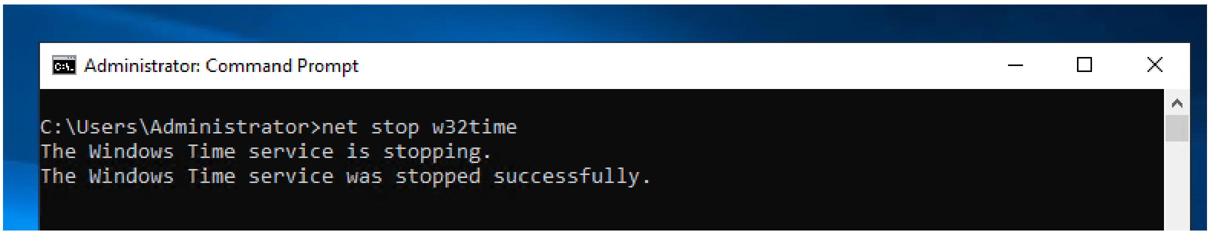
Hostname: EC2AMAZ-T1CGN5R
Instance ID: i-070d9472ac7183fdf
Private IPv4 address: 192.168.5.28
Public IPv4 address: 54.156.76.124
Instance size: t2.micro
Availability Zone: us-east-1b
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate

```
C:\Users\Administrator>w32tm /config /manualpeerlist:"0.pool.ntp.org,1.pool.ntp.org,2.pool.
ntp.org,3.pool.ntp.org" /syncfromflags:manual /reliable:YES /update
The command completed successfully.

C:\Users\Administrator>_
```

This command configures the Windows Time service to synchronize the system clock with the specified NTP servers. By listing multiple NTP servers, the command ensures redundancy and improves reliability. The configuration ensures that the system clock stays accurate by regularly synchronizing with these external time sources.

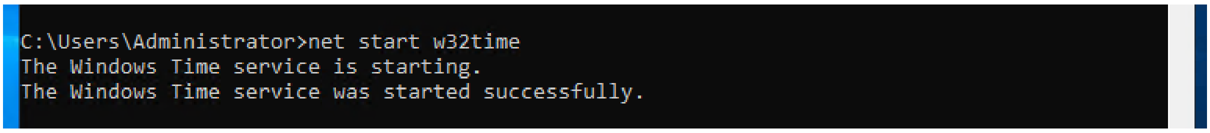
2. Start and stop the Windows Time service:

net stop w32time



```
C:\Users\Administrator>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.
```

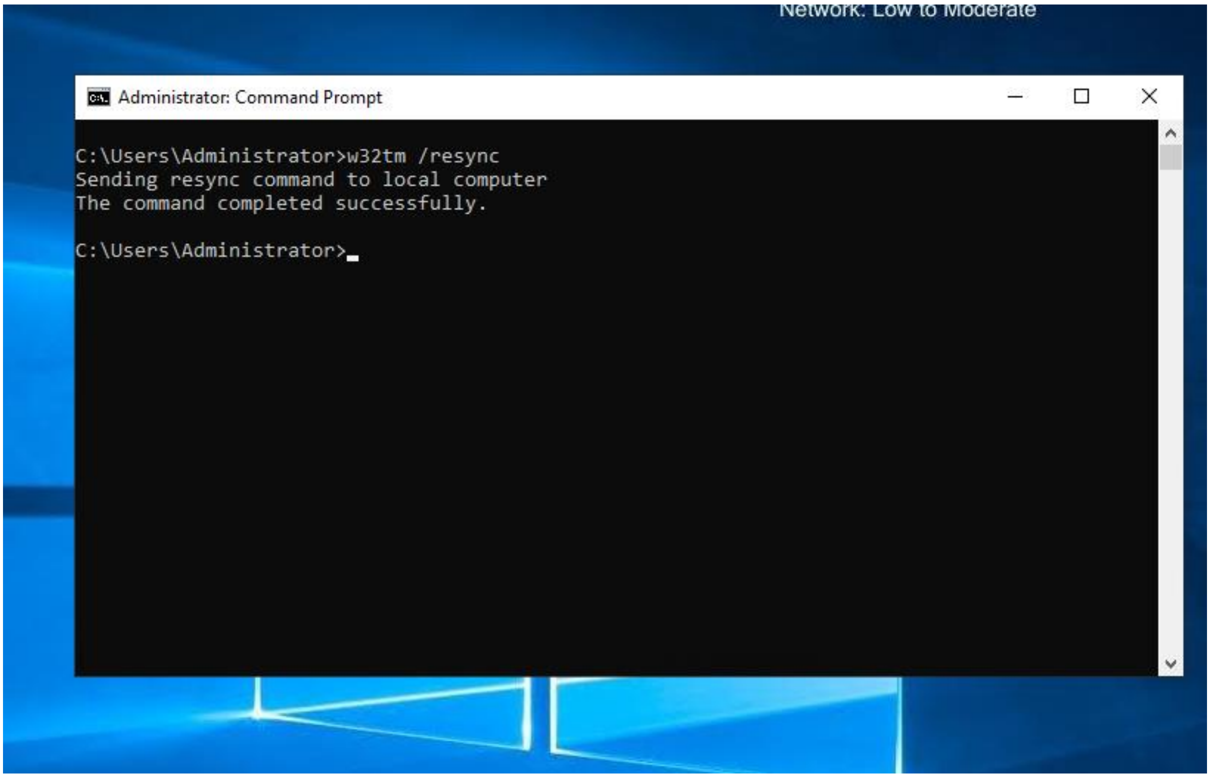
net start w32time



```
C:\Users\Administrator>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.
```

3. Force synchronization with the NTP servers:

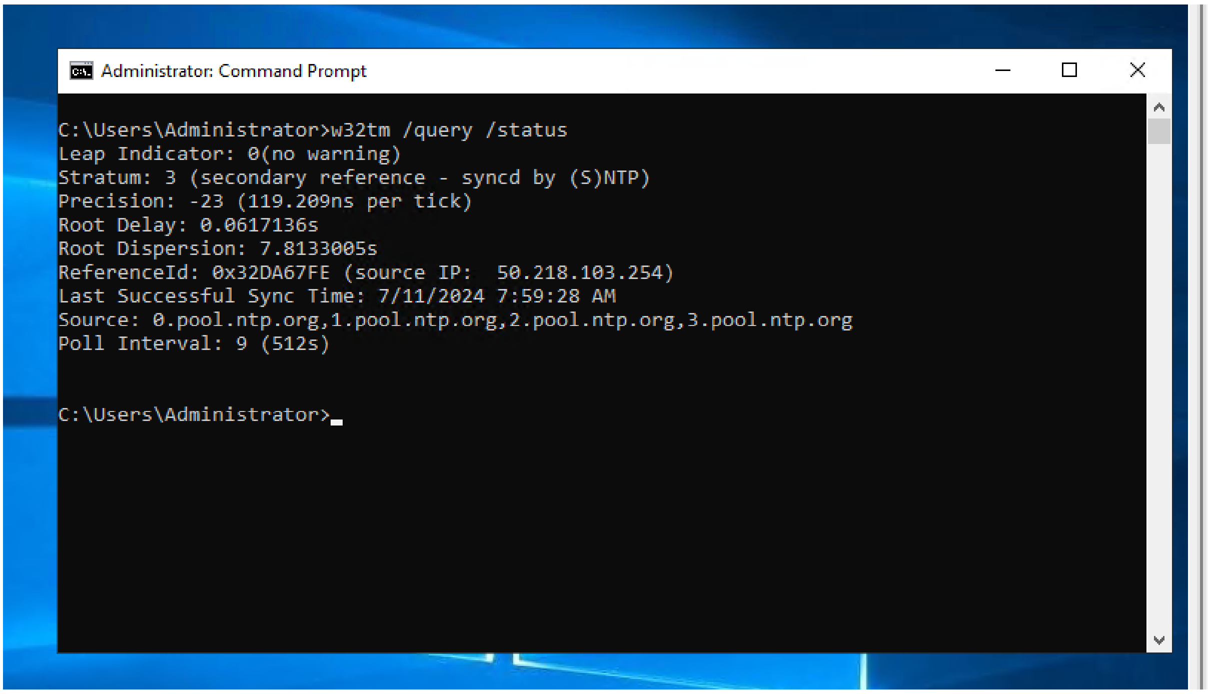
w32tm /resync



```
C:\Users\Administrator>w32tm /resync
Sending resync command to local computer
The command completed successfully.

C:\Users\Administrator>_
```

4.Check the status of the Windows Time service to ensure it is synchronized:

w32tm /query /status

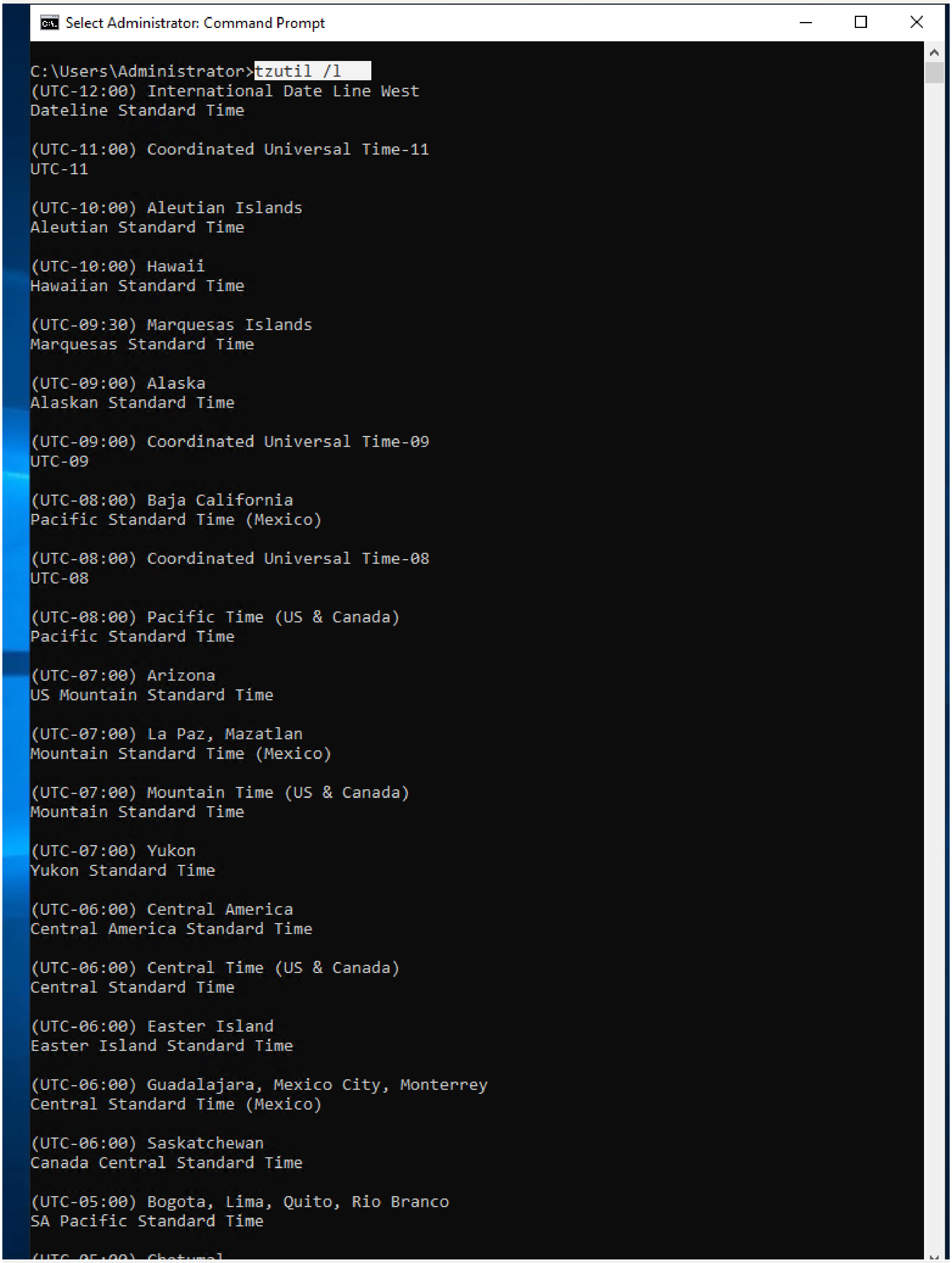


```
C:\Users\Administrator>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0617136s
Root Dispersion: 7.8133005s
ReferenceId: 0x32DA67FE (source IP:  50.218.103.254)
Last Successful Sync Time: 7/11/2024 7:59:28 AM
Source: 0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org,3.pool.ntp.org
Poll Interval: 9 (512s)


C:\Users\Administrator>_
```

Set the Correct Time Zone

1. List available time zones:

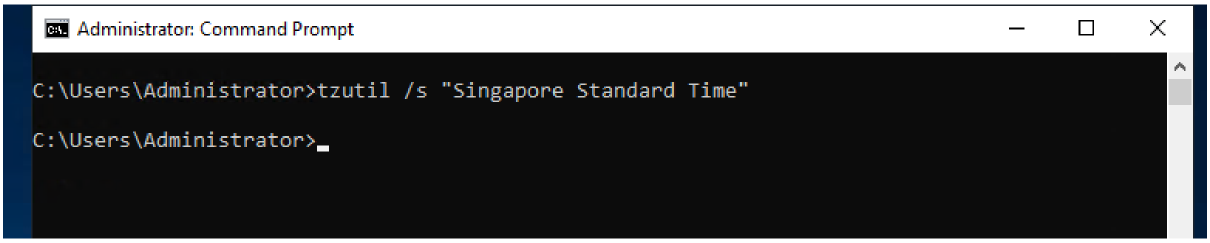
tzutil /l



```
C:\Users\Administrator>tzutil /l
(UTC-12:00) International Date Line West
Dateline Standard Time

(UTC-11:00) Coordinated Universal Time-11
UTC-11

(UTC-10:00) Aleutian Islands
Aleutian Standard Time

(UTC-10:00) Hawaii
Hawaiian Standard Time

(UTC-09:30) Marquesas Islands
Marquesas Standard Time

(UTC-09:00) Alaska
Alaskan Standard Time

(UTC-09:00) Coordinated Universal Time-09
UTC-09

(UTC-08:00) Baja California
Pacific Standard Time (Mexico)

(UTC-08:00) Coordinated Universal Time-08
UTC-08

(UTC-08:00) Pacific Time (US & Canada)
Pacific Standard Time

(UTC-07:00) Arizona
US Mountain Standard Time

(UTC-07:00) La Paz, Mazatlan
Mountain Standard Time (Mexico)

(UTC-07:00) Mountain Time (US & Canada)
Mountain Standard Time

(UTC-07:00) Yukon
Yukon Standard Time

(UTC-06:00) Central America
Central America Standard Time

(UTC-06:00) Central Time (US & Canada)
Central Standard Time

(UTC-06:00) Easter Island
Easter Island Standard Time

(UTC-06:00) Guadalajara, Mexico City, Monterrey
Central Standard Time (Mexico)

(UTC-06:00) Saskatchewan
Canada Central Standard Time

(UTC-05:00) Bogota, Lima, Quito, Rio Branco
SA Pacific Standard Time

(UTC-05:00) Chetumal
```

2. Set your desired time zone (e.g., “Singapore Standard Time”):

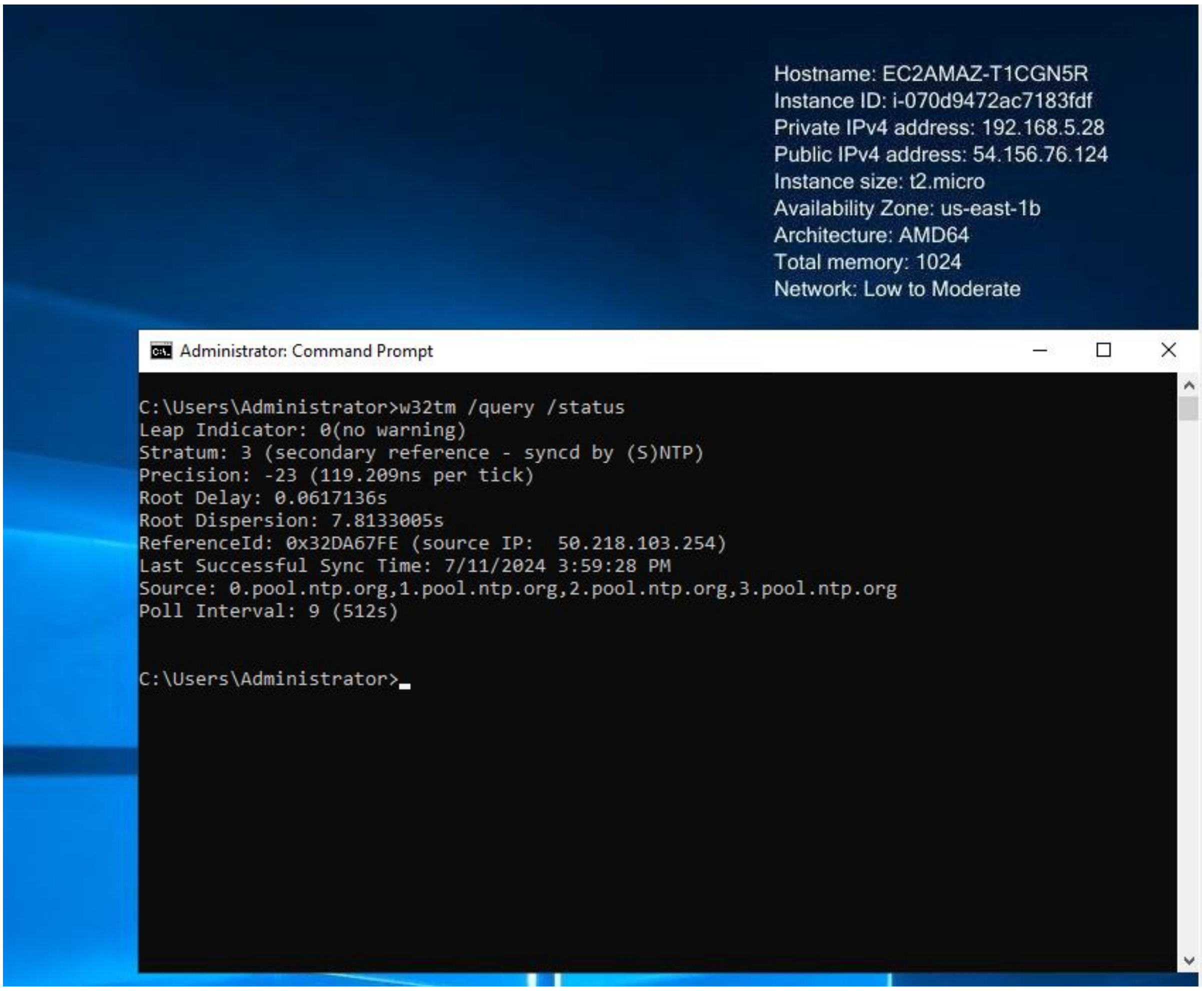
tzutil /s "Singapore Standard Time"



```
C:\Users\Administrator>tzutil /s "Singapore Standard Time"

C:\Users\Administrator>_
```

3. Verify the changes:

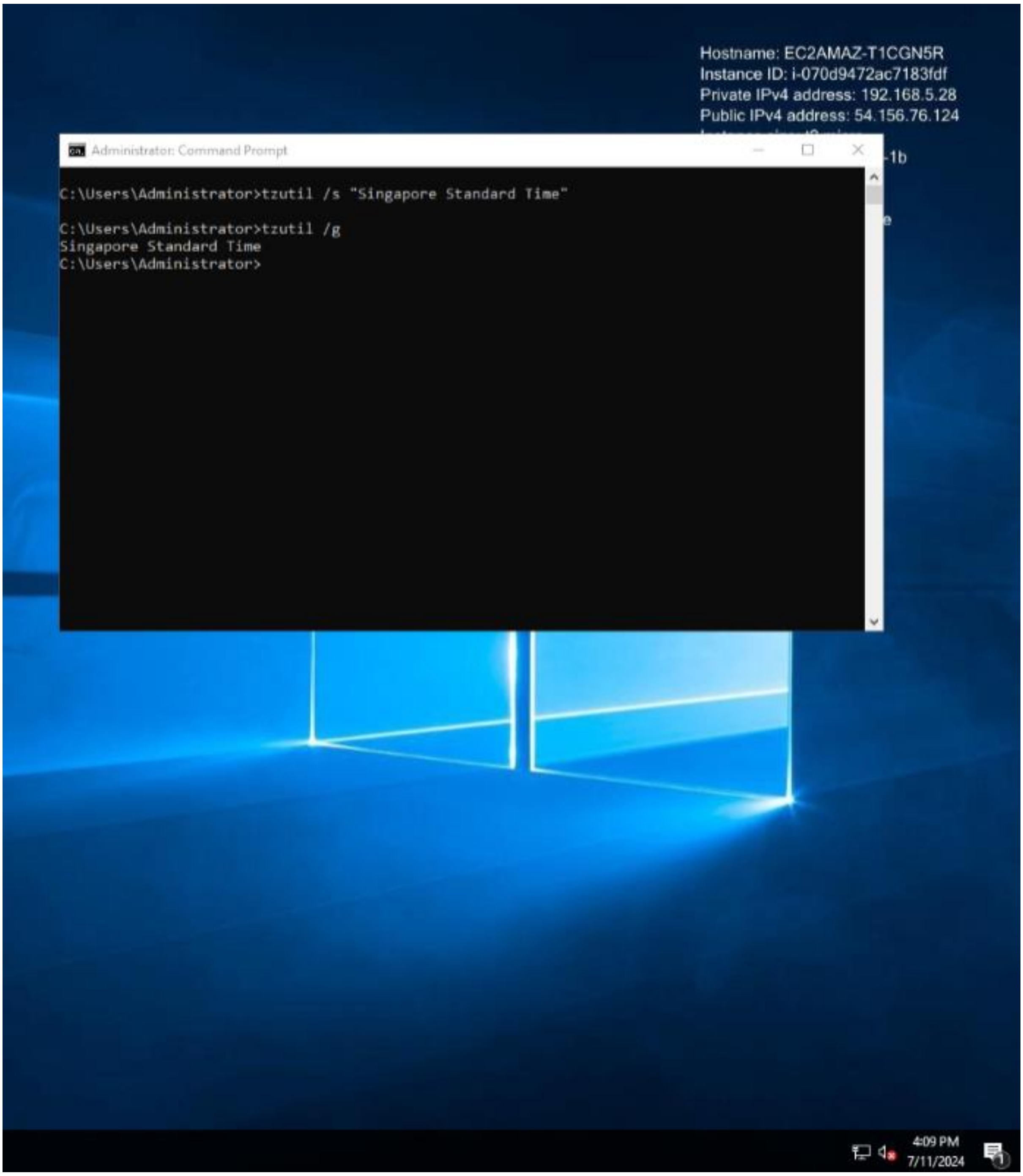
w32tm /query /status



Hostname: EC2AMAZ-T1CGN5R
Instance ID: i-070d9472ac7183fdf
Private IPv4 address: 192.168.5.28
Public IPv4 address: 54.156.76.124
Instance size: t2.micro
Availability Zone: us-east-1b
Architecture: AMD64
Total memory: 1024
Network: Low to Moderate

```
C:\Users\Administrator>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0617136s
Root Dispersion: 7.8133005s
ReferenceId: 0x32DA67FE (source IP:  50.218.103.254)
Last Successful Sync Time: 7/11/2024 3:59:28 PM
Source: 0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org,3.pool.ntp.org
Poll Interval: 9 (512s)


C:\Users\Administrator>_
```

tzutil /g



Hostname: EC2AMAZ-T1CGN5R
Instance ID: i-070d9472ac7183fdf
Private IPv4 address: 192.168.5.28
Public IPv4 address: 54.156.76.124

```
C:\Users\Administrator>tzutil /s "Singapore Standard Time"

C:\Users\Administrator>tzutil /g
Singapore Standard Time
C:\Users\Administrator>
```

That’s it! you have successfully learned how to configure time synchronization on your Windows EC2 instance using the Windows Time service. Accurate timekeeping is essential for maintaining system logs, data consistency, and secure communications. You have also configured the correct time zone for your instance, ensuring that all time-based operations reflect the proper local time.

Time synchronization plays a critical role in troubleshooting, coordination of distributed systems, and the security of transactions and communications. By regularly verifying and managing time settings, you can maintain the optimal operation of your applications and services.

These practices help ensure your cloud infrastructure’s reliability and performance, making sure your systems operate with precise time synchronization. Apply these techniques in future deployments and maintenance tasks to uphold system integrity and efficiency. Happy learning!