EXPERIMENT 06

CLASS: BE CMPN A 2 ROLL NO. : 18

NAME: REBECCA DIAS PID: 182027

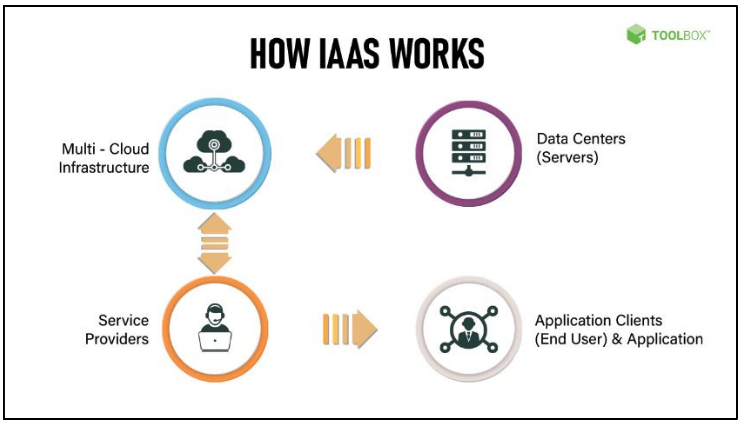
Aim: Study Infrastructure as a Service

Theory:

1. Prepare a detailed study of Infrastructure as a Service

Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage and networking resources on demand, on a pay-as-you-go basis. IaaS is one of the four types of cloud services, along with software as a service (SaaS), platform as a service (PaaS) and serverless.

Migrating your organisation's infrastructure to an IaaS solution helps you reduce maintenance of on-premises data centres, save money on hardware costs and gain real-time business insights. IaaS solutions give you the flexibility to scale your IT resources up and down with demand. They also help you quickly provision new applications and increase the reliability of your underlying infrastructure.


HOW IAAS WORKS
TOOLBOX
Multi - Cloud Infrastructure
Data Centers (Servers)
Service Providers
Application Clients (End User) & Application

IaaS lets you bypass the cost and complexity of buying and managing physical servers and datacentre infrastructure. Each resource is offered as a separate service component and you only pay for a particular resource for as long as you need it. A cloud computing service provider like Azure manages the infrastructure, while you purchase, install, configure and manage your own software—including operating systems, middleware and applications.

Key features:

- Instead of purchasing hardware outright, users pay for IaaS on demand.
- Infrastructure is scalable depending on processing and storage needs.
- Saves enterprises the costs of buying and maintaining their own hardware.
- Because data is on the cloud, there can be no single point of failure.
- Enables the virtualization of administrative tasks, freeing up time for other work.

2. Advantages and Limitation of IaaS

Advantages:

1. Cost Effective
IaaS is most economical option for businesses since it eliminates the cost of infrastructure. There is no need to purchase hardware as well as other networking equipments. And also, IaaS follows pay-as-you-go pricing scheme. Meaning, the users must spend only for what they use. The expenses are involved only at monthly level.

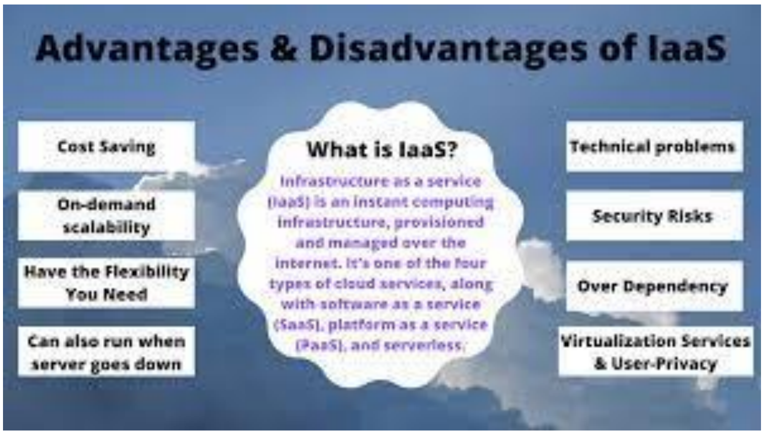
2. Scalability
When scaling an IaaS solution, it does not require investment in the hardware. The reason for this is the presence of cloud resources in unlimited quantity. As per the company's requirement, the IaaS allows it to be scaled up and down. As a result, businesses can save time as well as money. Once the usage of services are over, the users could scale down the solution.

3. Reliability
Reliability of data in IaaS is present to a very high extent. It is able to recover from worst case scenarios. This is because the resources of IaaS is present across various servers. Even if one server encounters problems, the remaining servers could deliver the resources without disruptions.

Even if there is an internet connection failure, hardware failure or a disaster, the infrastructure could still continue to function. Therefore, in any outages the IaaS could recover instantly.

4. Accessibility
Work today require greatest amount of flexibility. Especially, when it comes to accessibility. IaaS allows employees of an organization to easily access their files and other documents instantly. Virtual offices are made available to the employees anytime as long as they are having an internet connection.

5. Business Productivity
Whenever the workload of a business increases, maintenance becomes difficult without more staffs. But in IaaS, there is no burden of training new staffs. Instead it is taken care by a third party service provider. IaaS provider is responsible of maintaining and upgrading the infrastructure. Hence, the management could focus on other business operations.



Advantages & Disadvantages of IaaS

What is IaaS?

Infrastructure as a service (IaaS) is an instant computing infrastructure, provisioned and managed over the internet. It's one of the four types of cloud services, along with software as a service (SaaS), platform as a service (PaaS), and serverless.

Cost Saving
On-demand scalability
Have the Flexibility You Need
Can also run when server goes down
Technical problems
Security Risks
Over Dependency
Virtualization Services & User-Privacy

Disadvantages:

1. Security
Users in IaaS does not have the control of infrastructure. The security of the infrastructure is in the hands of the provider. Sometimes the level of security provided may not be adequate. As a result, it could expose your system to hacks and vulnerabilities. In this case, the businesses must be willing to accept the loss.

2. Control
The entire administration of the IaaS is taken care by the provider. While this could be a stress relief for the users, this can leave important part of controlling to the provider. Such as the users have no control over data and software. Under these conditions, the provider needs to make sure that the data as well as services are secure.

3. Customization
Customization is not an easy task in IaaS since it is based on virtualization services. This is because there is very less number of options for customization. As a result, the user privacy offered is not greater as it is with other solutions.

4. Upgradeability
Even though maintenance is provided by the IaaS providers, still they fail to provide upgrades for some businesses. Besides the hardware the IaaS provider is in charge of providing upgrades to the applications. Now the businesses without frequent upgrades to their software will face productivity issues since their employee efficiency is affected.

5. Technical Issues

Downtime is one of the most common technical issues faced when using IaaS solution. While the user data is spread across various data centers, still the issues that is faced from the providers end could restrict accessibility. Users will no longer will be able to access the applications and data which delays work that needs to be done.

3. Study security issues in IaaS

- Data Leaks

Data in the cloud is exposed to the same threats as traditional infrastructures. Due to the large amount of data, platforms of cloud providers become an attractive target for attackers. Data leaks can lead to a chain of unfortunate events for IT companies and infrastructure as a service (IaaS) providers.

- Compromising Accounts And Authentication Bypass

Data leaks often result from insufficient attention to authentication verification. More often than not, weak passwords in conjunction with poor management of encryption keys and certificates are to blame. In addition, IT organizations are faced with problems of managing rights and permissions when users are assigned with much greater powers than they actually need. The problem can also occur when a user takes another position or leaves the company: no one is in a rush to update permissions under the new user roles. As a result, the account has rights to more features than necessary.

- Interface And API Hacking

Today, it is impossible to imagine cloud services and applications without friendly user interfaces (UIs) and application program interfaces (APIs). The security and availability of cloud services depends on reliable mechanisms of data access control and encryption. Weak interfaces become bottlenecks in matters of availability, confidentiality, integrity and security of systems and data.

- Cyberattacks

Targeted cyberattacks are common in our times. An experienced attacker, who has secured his presence in a target infrastructure, is not so easy to detect. Remote network attacks may have significant impact on the availability of infrastructure in general.

Despite the fact that denial-of-service (DoS) attacks have a long history, the development of cloud computing has made them more common. DoS attacks can cause business critical services to slow down or even stop. DoS attacks consume a large amount of computing power that comes with a hefty bill. Despite the fact that the principles of DoS attacks are simple at first glance, you need to understand their characteristics at the application level: the focus on the vulnerability of web servers, databases and applications.

- Permanent Data Loss

Data loss due to malicious acts or accidents at the provider’s end is no less critical than a leak. Daily backups and their storage on external protected alternative platforms are particularly important for cloud environments.

In addition, if you are using encryption before moving data to the cloud, it is necessary to take care of secure storage for encryption keys. As soon as keys fall into the wrong hands, data itself becomes available to attackers, the loss of which can wreak havoc on any organization.

- Vulnerabilities

A common mistake when using cloud-based solutions in the IaaS model is paying too little attention to the security of applications, which are placed in the secure infrastructure of the cloud provider. And the vulnerability of applications becomes a bottleneck in enterprise infrastructure security.

- Lack Of Awareness

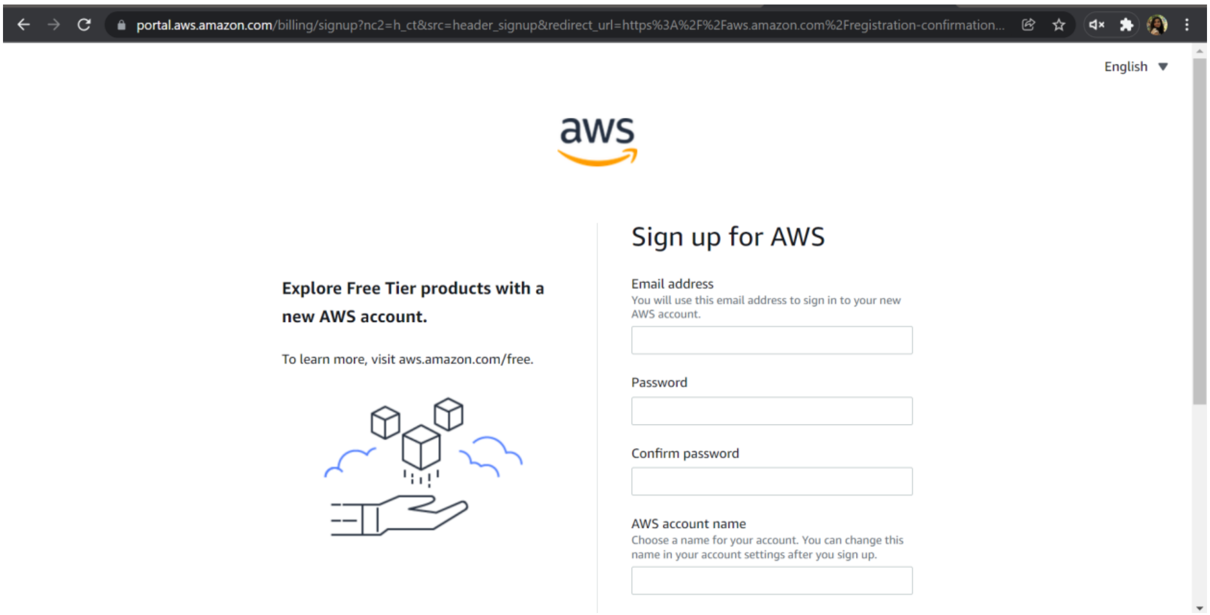
Organizations moving to the cloud without understanding the capabilities the cloud has to offer are faced with many problems. If a team of specialists is not very familiar with the features of cloud technologies and principles of deploying cloud-based applications, operational and architectural issues arise that can lead not only to downtime but also to much more serious problems.

- Abuse Of Cloud Services

The cloud can be used by legal and illegal businesses. The purpose of the latter is to use cloud resources for criminal activity: launching DoS attacks, sending spam, distributing malicious content, etc. It is extremely important for suppliers and service users to be able to detect such activities. To do this, detailed traffic inspections and cloud monitoring tools are recommended.

Activity:

1. Use AWS, to create a VM and configure it.
2. Access the created machine remotely



portal.aws.amazon.com/billing/signup?nc2=h_ct&src=header_signup&redirect_url=https%3A%2F%2Faws.amazon.com%2Fregistration-confirmation...

Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Sign up for AWS

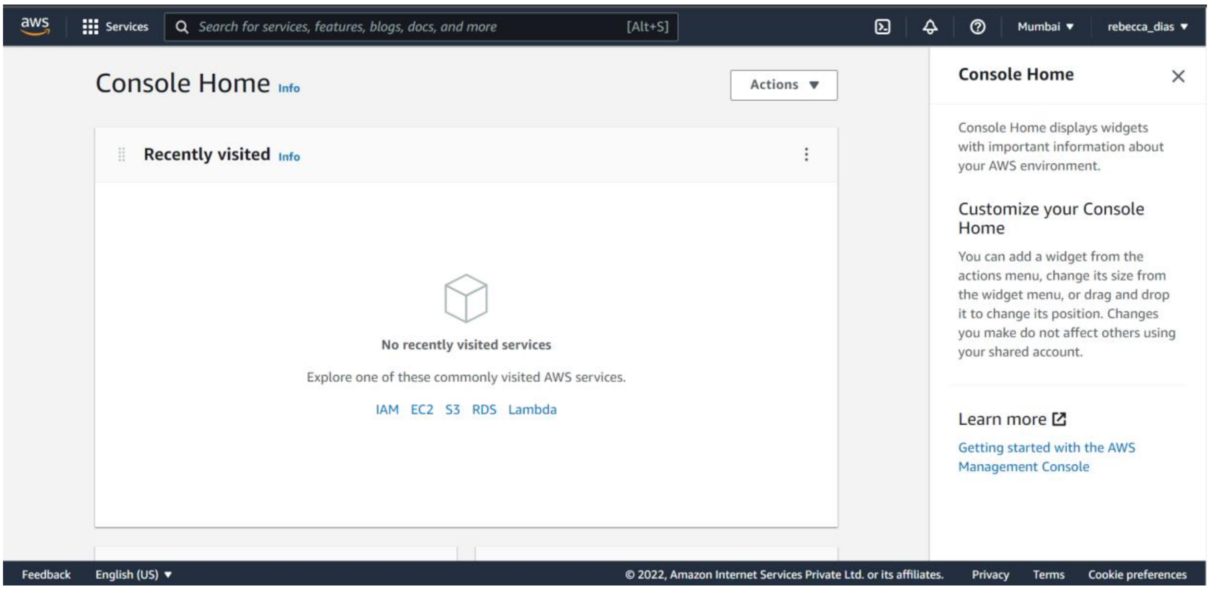
Email address
You will use this email address to sign in to your new AWS account.

Password

Confirm password

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

1.To demonstrate and implement IAAS service using AWS (Use t2.Micro (Free tier eligible) (instance only).



Console Home

Recently visited

No recently visited services

Explore one of these commonly visited AWS services.

Console Home

Console Home displays widgets with important information about your AWS environment.

Customize your Console Home

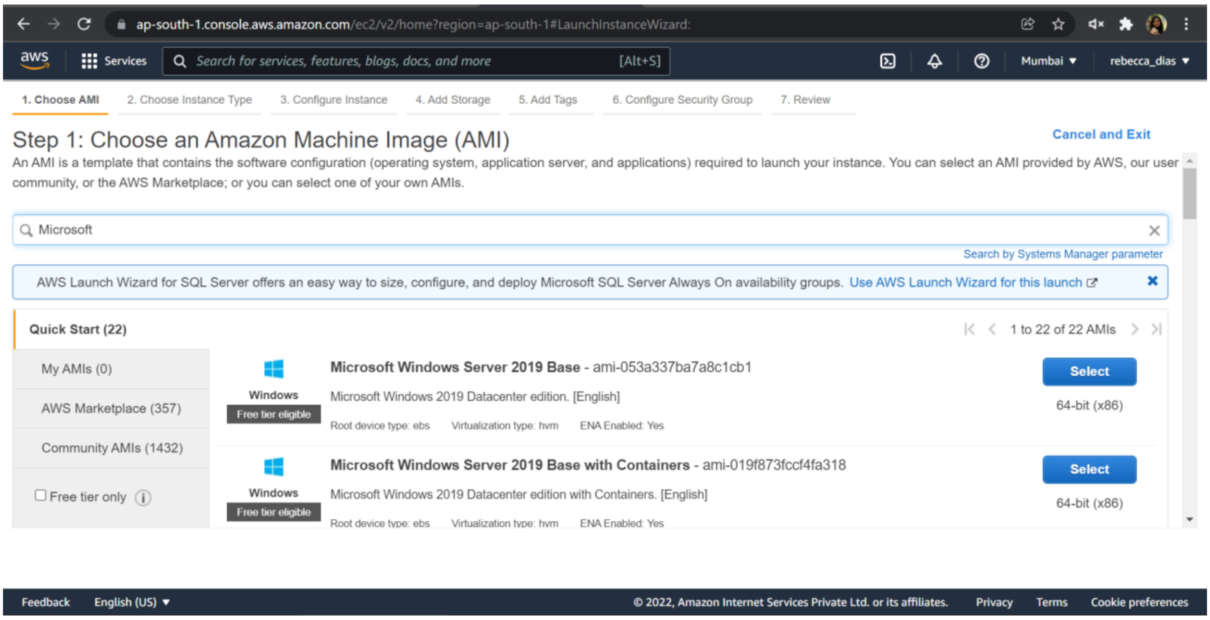
You can add a widget from the actions menu, change its size from the widget menu, or drag and drop it to change its position. Changes you make do not affect others using your shared account.

Learn more

Getting started with the AWS Management Console

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Choose Msft windows server base 2019



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Microsoft

Search by Systems Manager parameter

AWS Launch Wizard for SQL Server offers an easy way to size, configure, and deploy Microsoft SQL Server Always On availability groups. Use AWS Launch Wizard for this launch

Microsoft Windows Server 2019 Base - ami-053a337ba7a8c1cb1

Microsoft Windows 2019 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

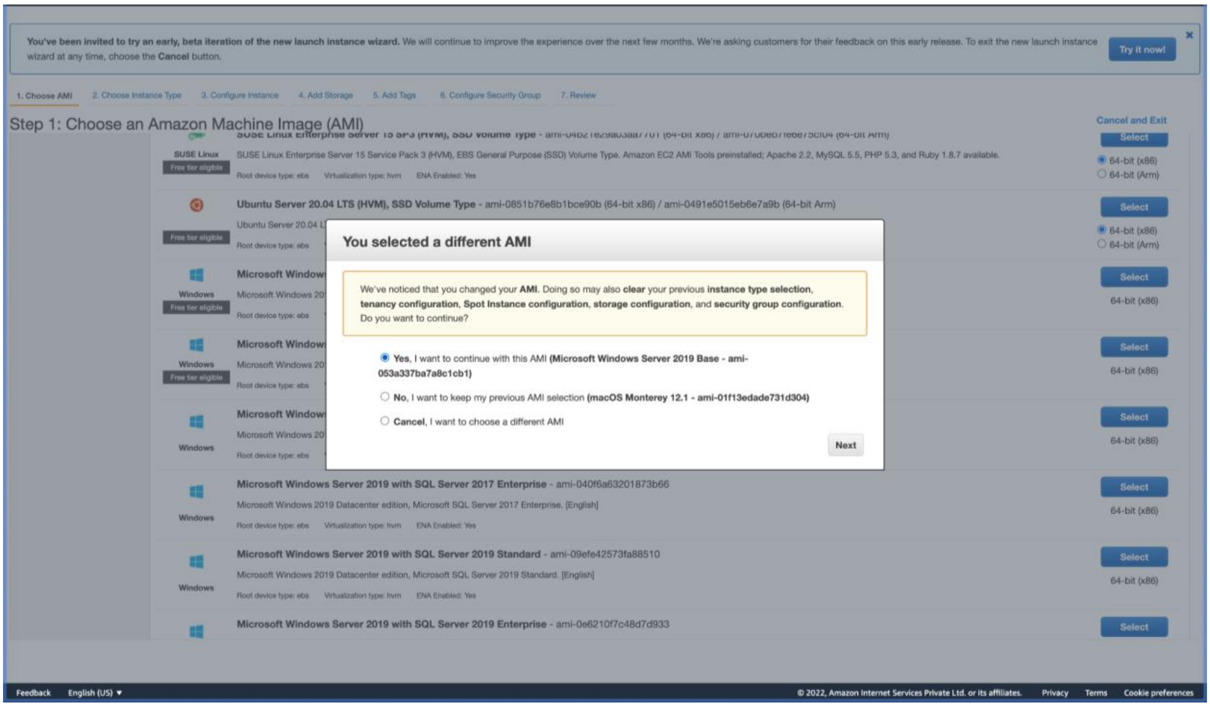
Microsoft Windows Server 2019 Base with Containers - ami-019f873fccf4fa318

Microsoft Windows 2019 Datacenter edition with Containers. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

© 2022, Amazon Internet Services Private Ltd. or its affiliates.



You've been invited to try an early, beta iteration of the new launch instance wizard. We will continue to improve the experience over the next few months. We're asking customers for their feedback on this early release. To exit the new launch instance wizard at any time, choose the **Cancel** button.

Step 1: Choose an Amazon Machine Image (AMI)

SUSE Linux Enterprise Server 15 SP3 (HVM), SSD Volume Type - ami-04b21e29a03aa7701 (64-bit x86) / ami-070be07fe6e75c104 (64-bit Arm)

SUSE Linux Enterprise Server 15 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0851b76e8b1bce90b (64-bit x86) / ami-0491e5015eb6e7a9b (64-bit Arm)

● 64-bit (x86)
○ 64-bit (Arm)

You selected a different AMI

We've noticed that you changed your **AMI**. Doing so may also **clear** your previous **instance type selection**, **tenancy configuration**, **Spot Instance configuration**, **storage configuration**, and **security group configuration**. Do you want to continue?

● **Yes**, I want to continue with this AMI **(Microsoft Windows Server 2019 Base - ami-053a337ba7a8c1cb1)**

○ **No**, I want to keep my previous AMI selection **(macOS Monterey 12.1 - ami-01f13edade731d304)**

○ **Cancel**, I want to choose a different AMI

Microsoft Windows Server 2019 with SQL Server 2017 Enterprise - ami-040f6a63201873b66

Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2017 Enterprise. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

Microsoft Windows Server 2019 with SQL Server 2019 Standard - ami-09efe42573fa88510

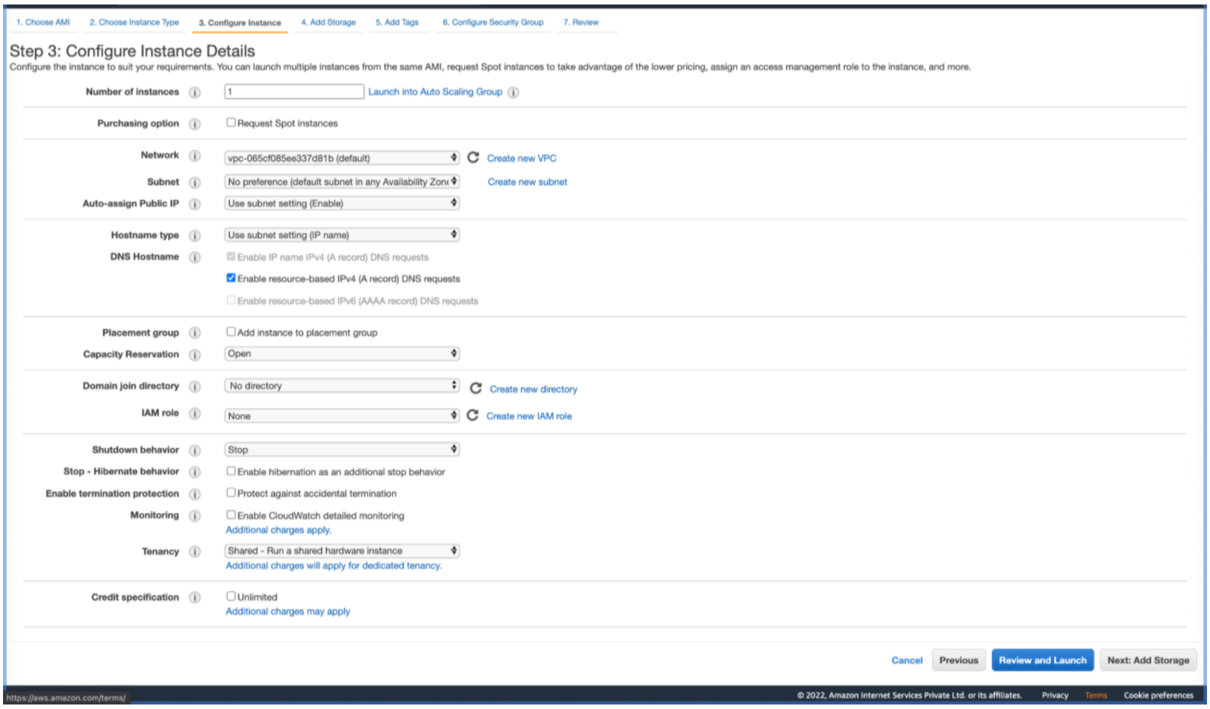
Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2019 Standard. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

Microsoft Windows Server 2019 with SQL Server 2019 Enterprise - ami-0e6210f7c48d7d933

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

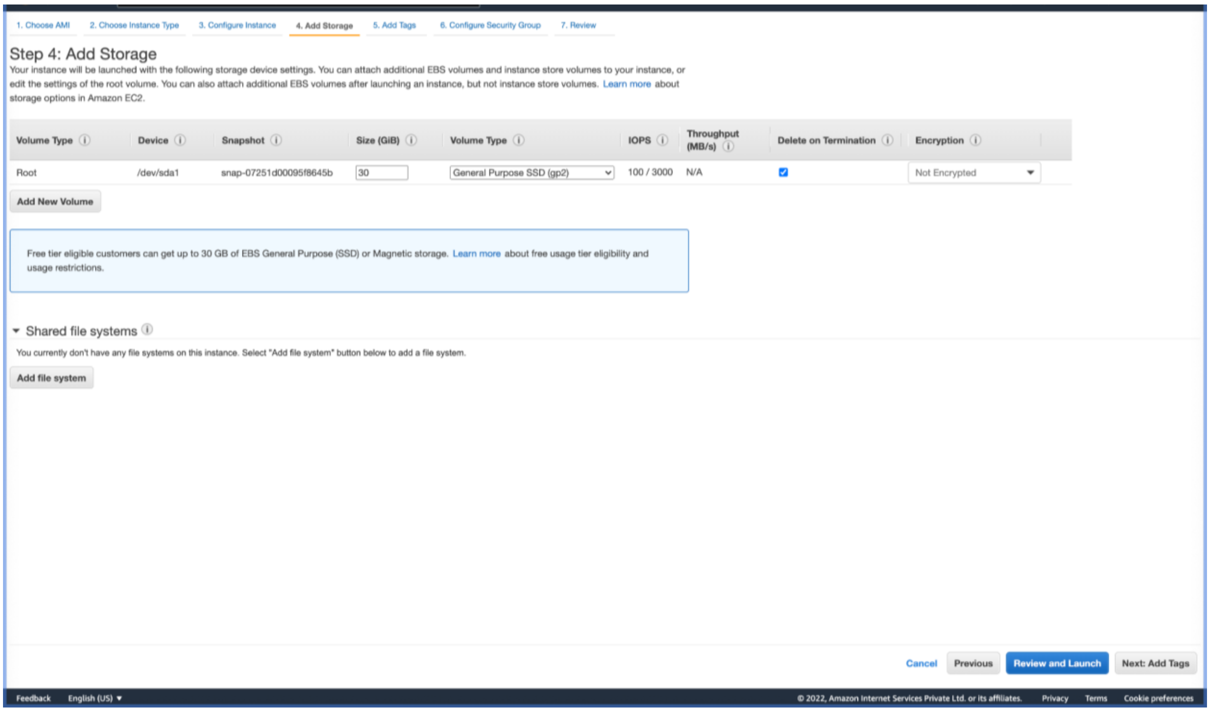


Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-065cf085ee337d81b (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zon Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
Hostname type	Use subnet setting (IP name)
DNS Hostname	☑ Enable IP name IPv4 (A record) DNS requests ☑ Enable resource-based IPv4 (A record) DNS requests □ Enable resource-based IPv6 (AAAA record) DNS requests
Placement group	□ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory Create new directory
IAM role	None Create new IAM role
Shutdown behavior	Stop
Stop - Hibernate behavior	□ Enable hibernation as an additional stop behavior
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
Credit specification	□ Unlimited Additional charges may apply

Cancel
Previous
Review and Launch
Next: Add Storage
https://aws.amazon.com/terms/
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences



Step 4: Add Storage

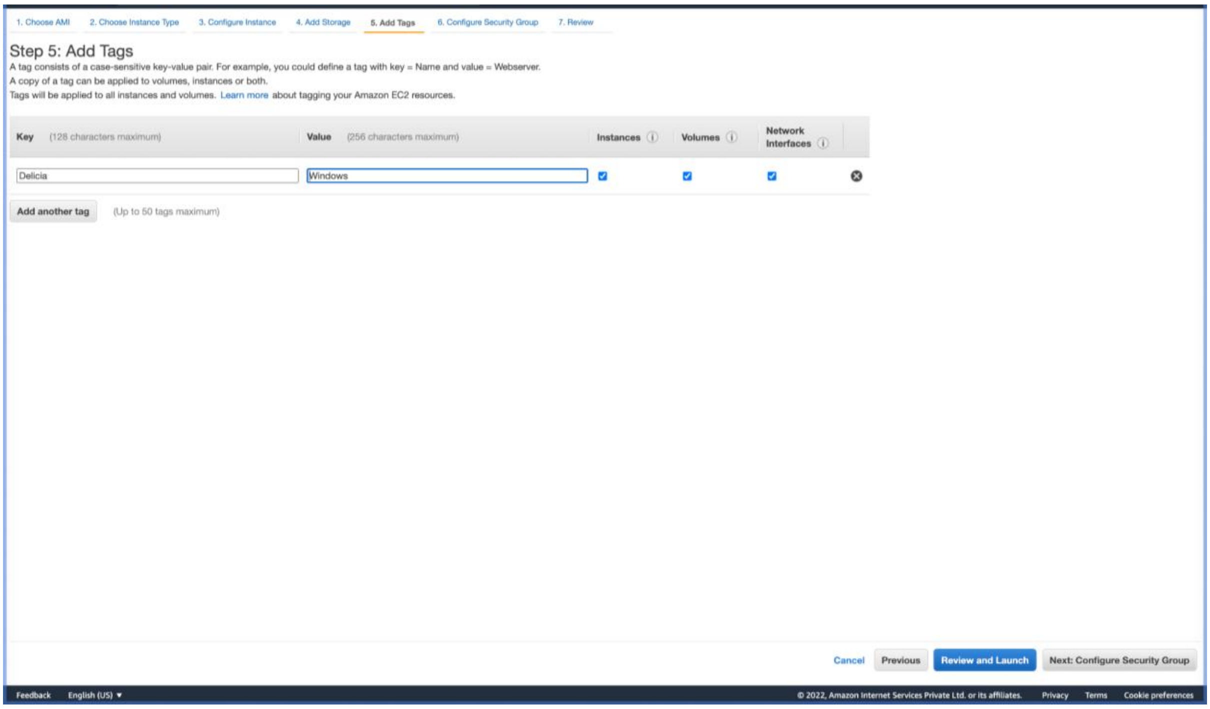
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-07251d00095f8645b	30	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

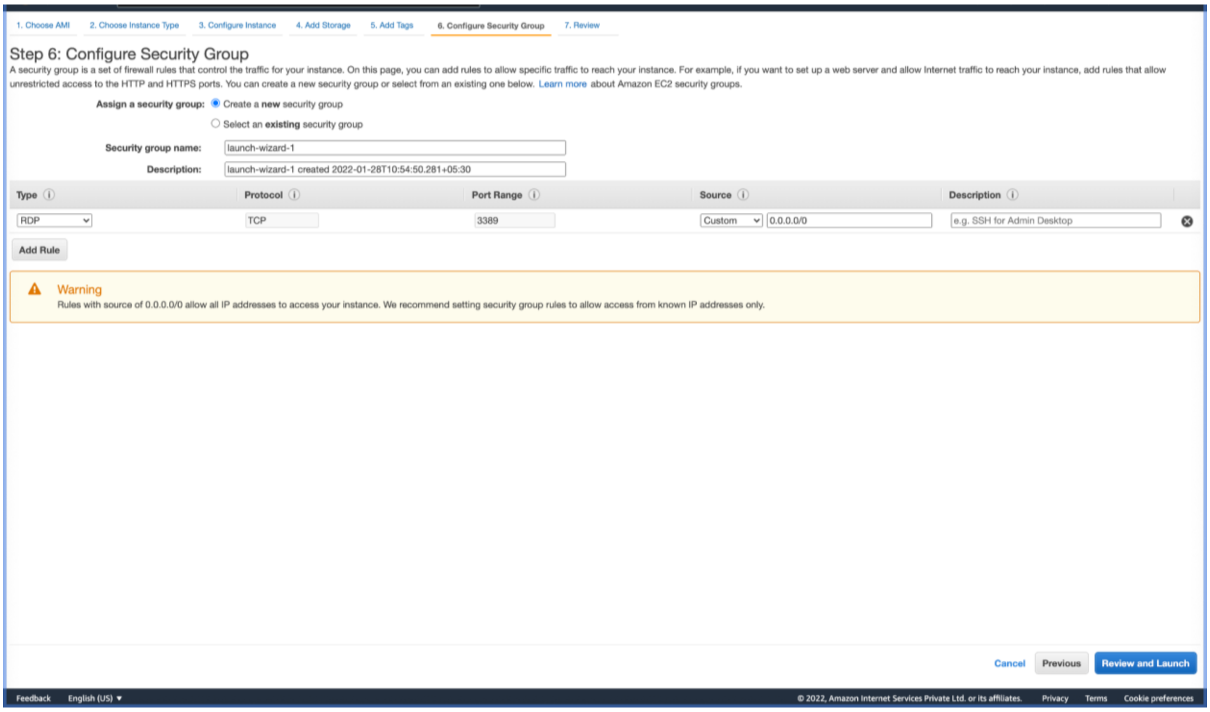
You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Delicia	Windows	☑	☑	☑



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

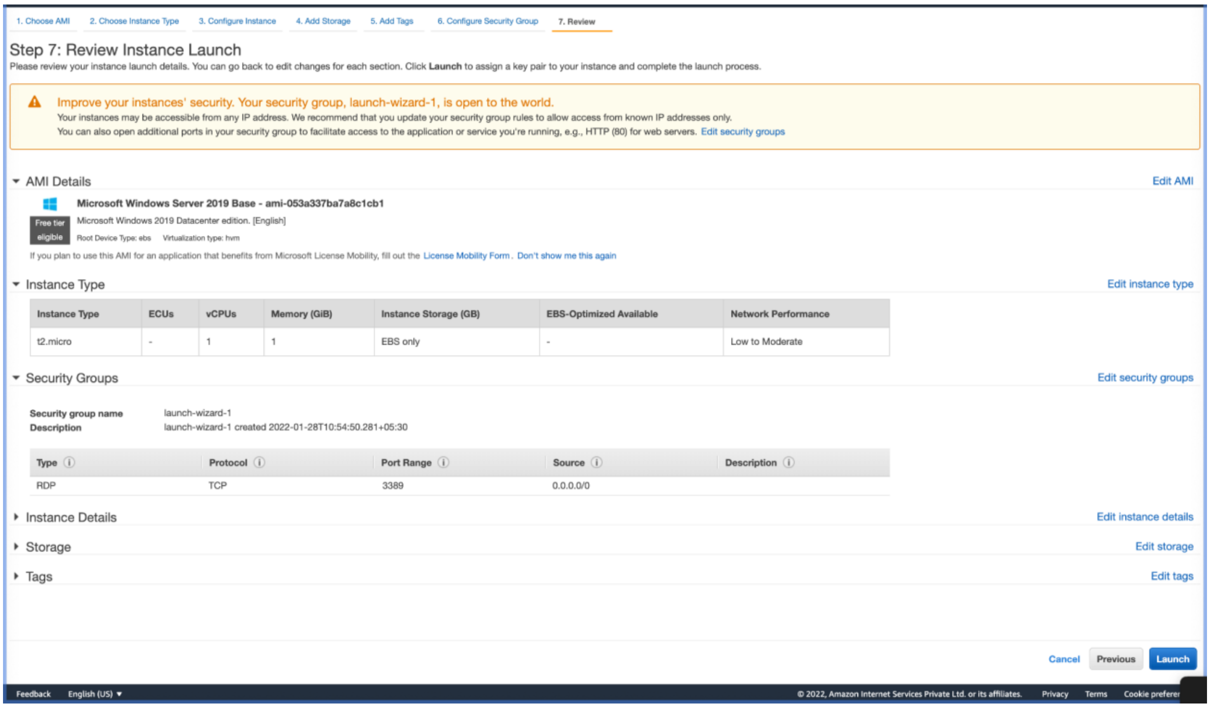
Security group name: launch-wizard-1

Description: launch-wizard-1 created 2022-01-28T10:54:50.281+05:30

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

⚠ Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

3. Download the rem file here, use it at the end



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, launch-wizard-1, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details — Edit AMI

Microsoft Windows Server 2019 Base - ami-053a337ba7a8c1cb1
Free tier eligible
Microsoft Windows 2019 Datacenter edition. [English]
Root Device Type: ebs   Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups — Edit security groups

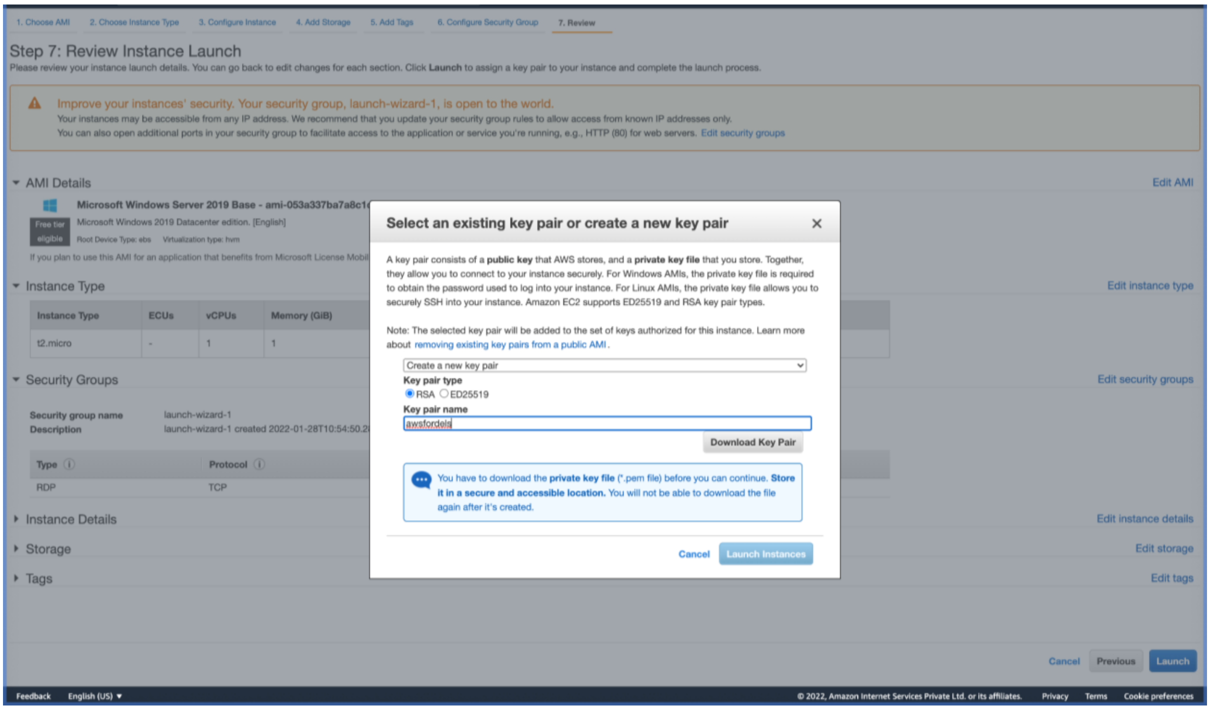
Security group name launch-wizard-1
Description launch-wizard-1 created 2022-01-28T10:54:50.281+05:30

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	0.0.0.0/0	

Instance Details — Edit instance details

Storage — Edit storage

Tags — Edit tags



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, launch-wizard-1, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

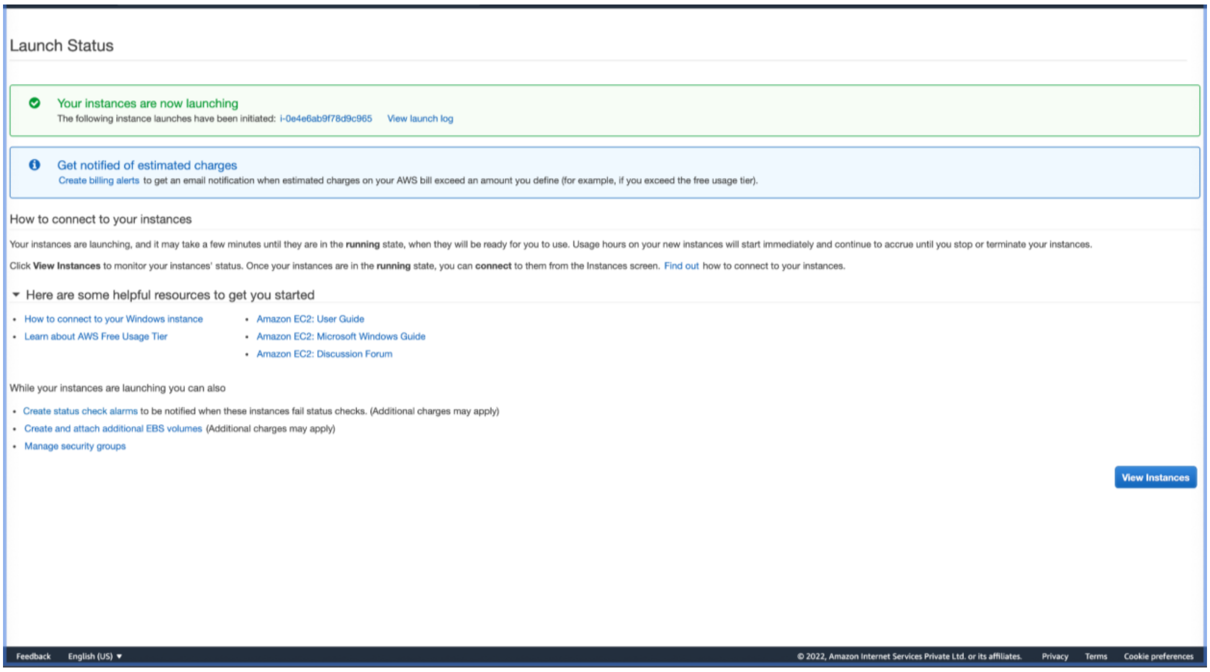
Create a new key pair

Key pair type
● RSA ○ ED25519

Key pair name
awsfordels

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.



Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0e4e6ab9f78d9c965 View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

▾ Here are some helpful resources to get you started

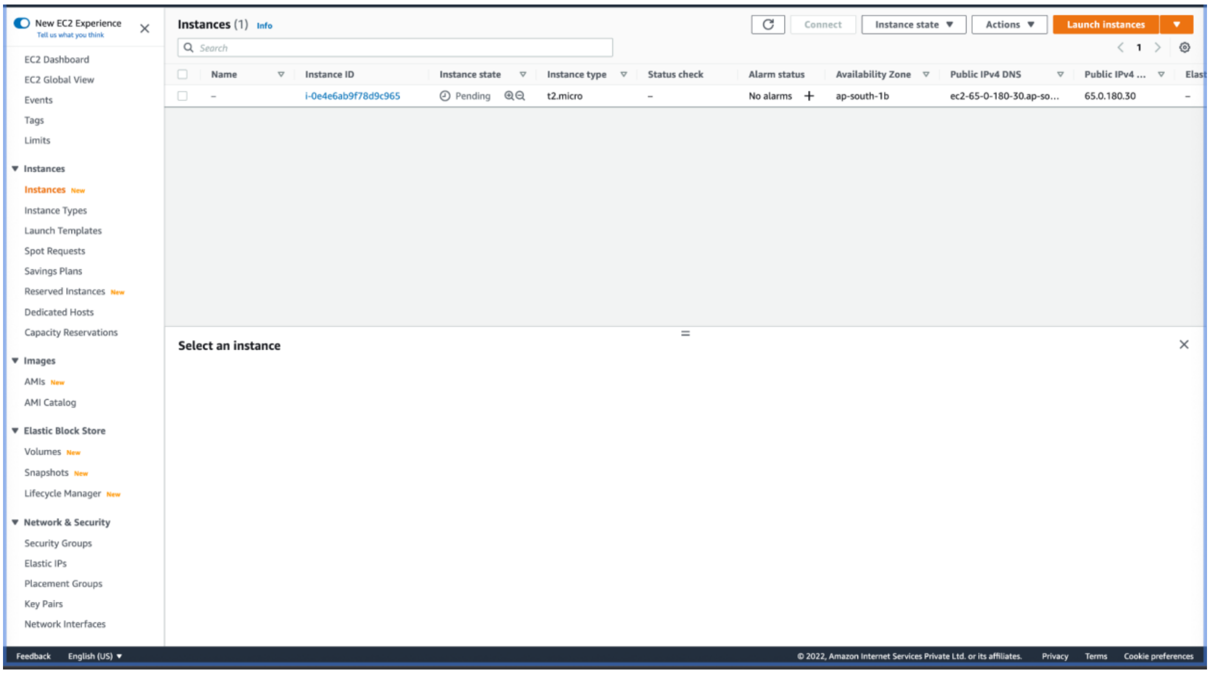
- How to connect to your Windows instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Microsoft Windows Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances
Feedback English (US) ▾
© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

4. Wait for 2 mins, let it change from pending to running, then Click your instance here and click connect



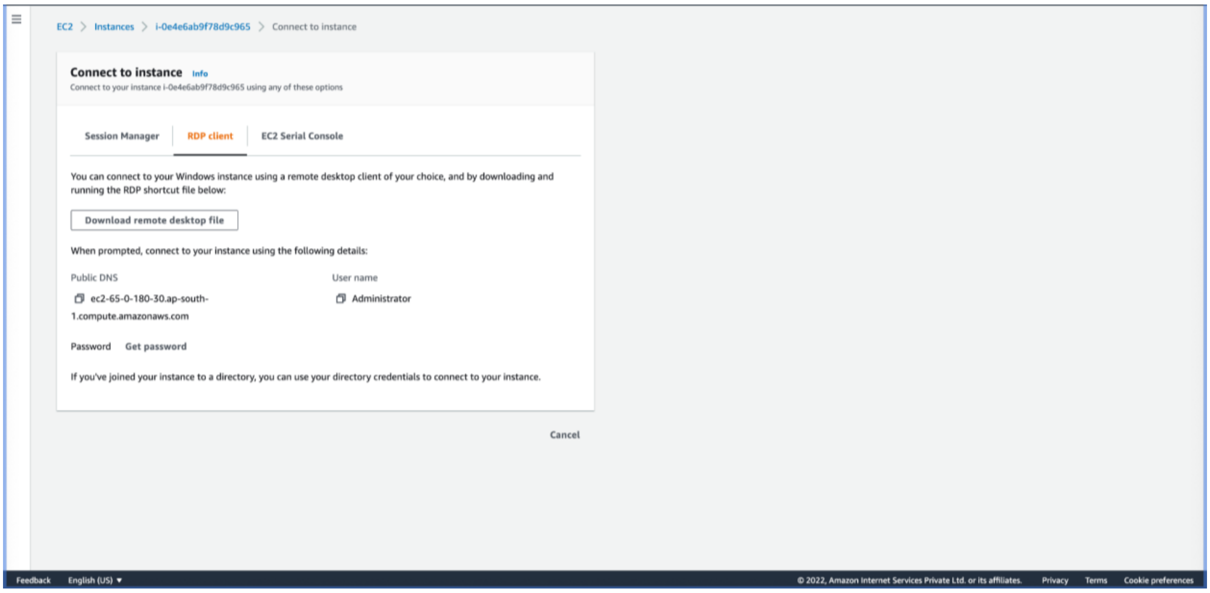
Instances (1) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elast
□	–	i-0e4e6ab9f78d9c965	Pending	t2.micro	–	No alarms +	ap-south-1b	ec2-65-0-180-30.ap-so...	65.0.180.30	–

Select an instance

Feedback English (US) ▾
© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

5. Download the rdp file here


EC2 > Instances > i-0e4e6ab9f78d9c965 > Connect to instance
Info
Session Manager
RDP client
EC2 Serial Console
Download remote desktop file
Cancel
Feedback
English (US) ▾
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Connect to instance

Connect to your instance i-0e4e6ab9f78d9c965 using any of these options

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:

When prompted, connect to your instance using the following details:

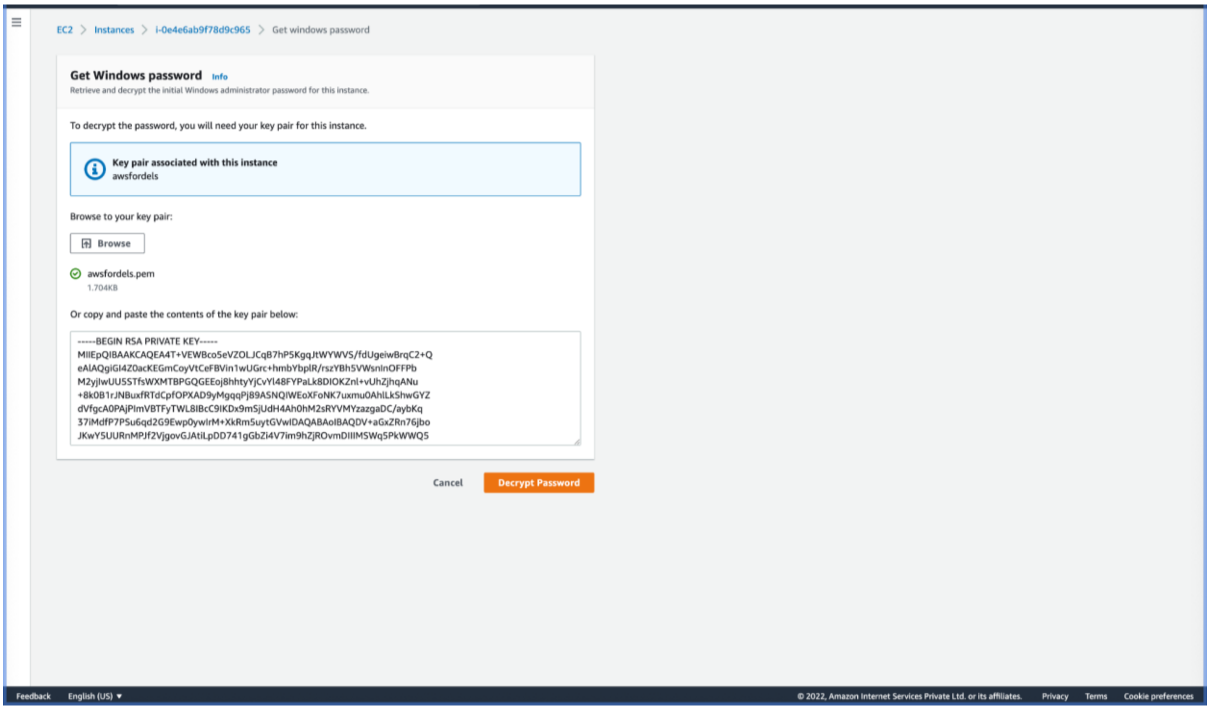
Public DNS: ec2-65-0-180-30.ap-south-1.compute.amazonaws.com

User name: Administrator

Password: Get password

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

6. Upload the rem file here and decrypt


EC2 > Instances > i-0e4e6ab9f78d9c965 > Get windows password
Info
Browse
Cancel
Decrypt Password
Feedback
English (US) ▾
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Get Windows password

Retrieve and decrypt the initial Windows administrator password for this instance.

To decrypt the password, you will need your key pair for this instance.

Key pair associated with this instance
awsfordels

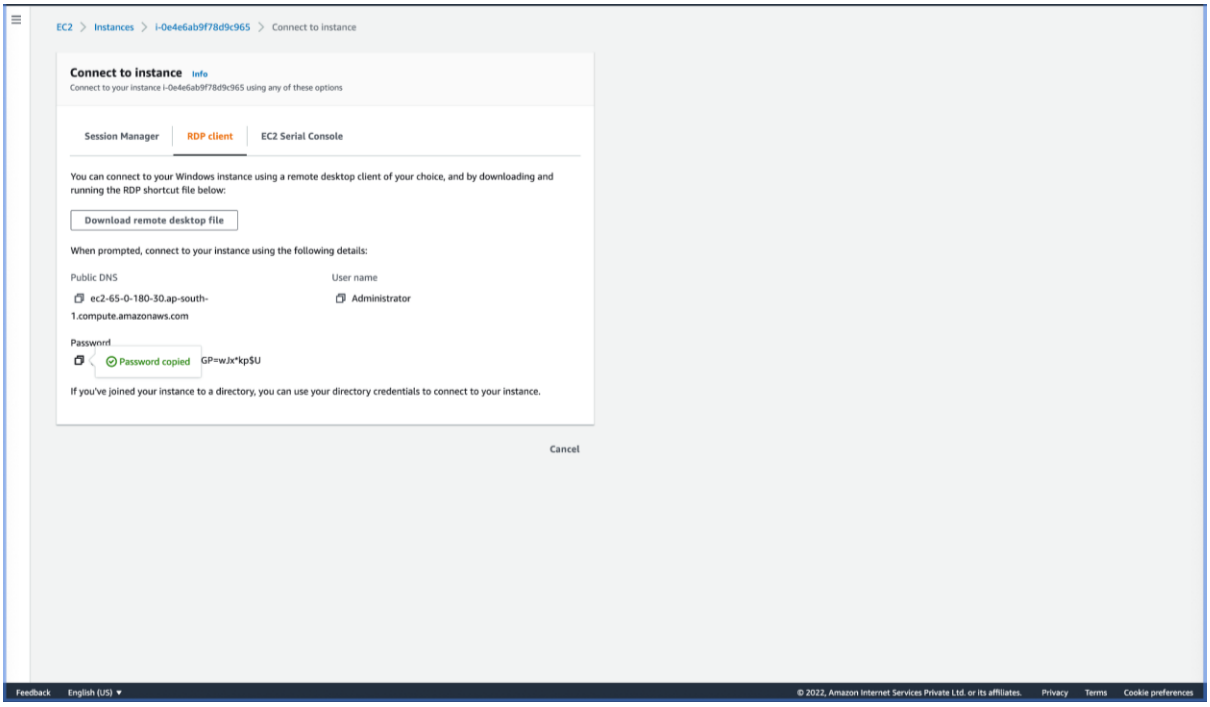
Browse to your key pair:

awsfordels.pem
1.704KB

Or copy and paste the contents of the key pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA4T+VEWBco5eVZOLJCqB7hP5KgqJtWYWVS/fdUgeiwBrqC2+Q
eAlAQgiGI4Z0acKEGmCoyVtCeFBVin1wUGrc+hmbYbplR/rszYBh5VWsnInOFFPb
M2yjIwUU5STfsWXMTBPGQGEEoj8hhtyYjCvYl48FYPaLk8DIOKZnl+vUhZjhqANu
+8k0B1rJNBuxfRTdCpfOPXAD9yMgqqPj89ASNQIWEoXFoNK7uxmu0AhlLkShwGYZ
dVfgcA0PAjPlmVBTFyTWL8IBcC9IKDx9mSjUdH4Ah0hM2sRYVMYzazgaDC/aybKq
37iMdfP7PSu6qd2G9Ewp0ywIrM+XkRm5uytGVwIDAQABAoIBAQDV+aGxZRn76jbo
JKwY5UURnMPJf2VjgovGJAtiLpDD741gGbZi4V7im9hZjROvmDIIIMSWq5PkWWQ5
```

7. Copy this password and click on the RDP file on your local machine. Use the password there.


EC2 > Instances > i-0e4e6ab9f78d9c965 > Connect to instance
Info
Session Manager
RDP client
EC2 Serial Console
Download remote desktop file
Cancel
Feedback
English (US) ▾
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Connect to instance

Connect to your instance i-0e4e6ab9f78d9c965 using any of these options

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:

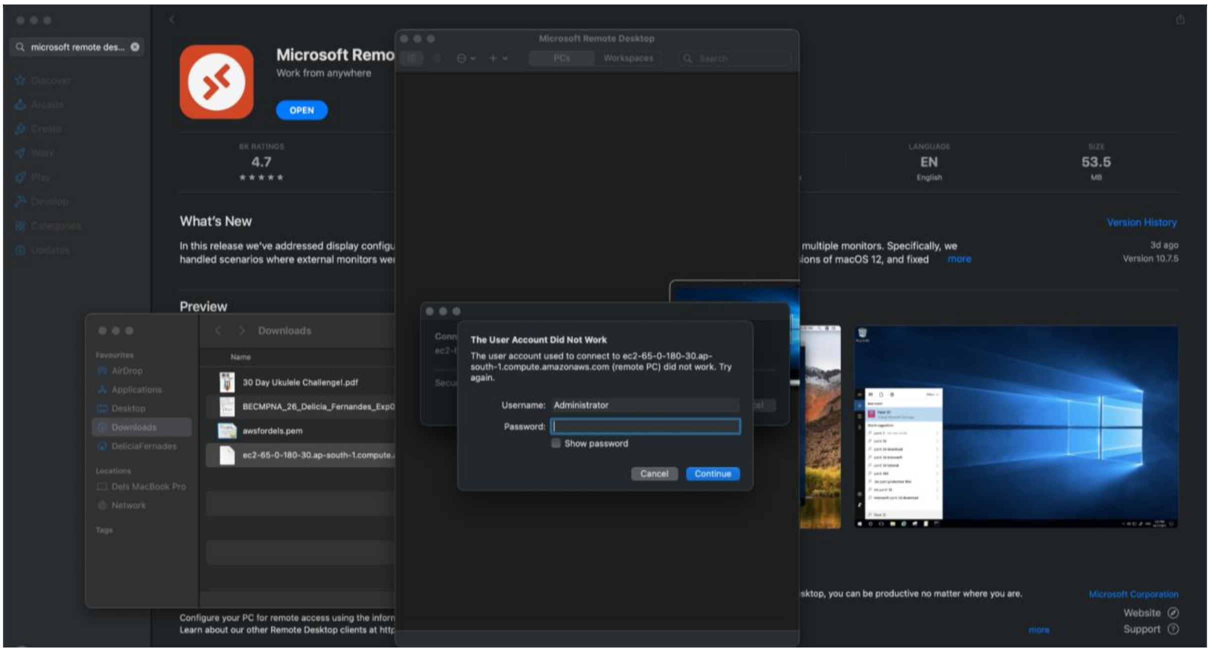
When prompted, connect to your instance using the following details:

Public DNS: ec2-65-0-180-30.ap-south-1.compute.amazonaws.com

User name: Administrator

Password: Password copied GP=wJx*kp$U

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



The User Account Did Not Work

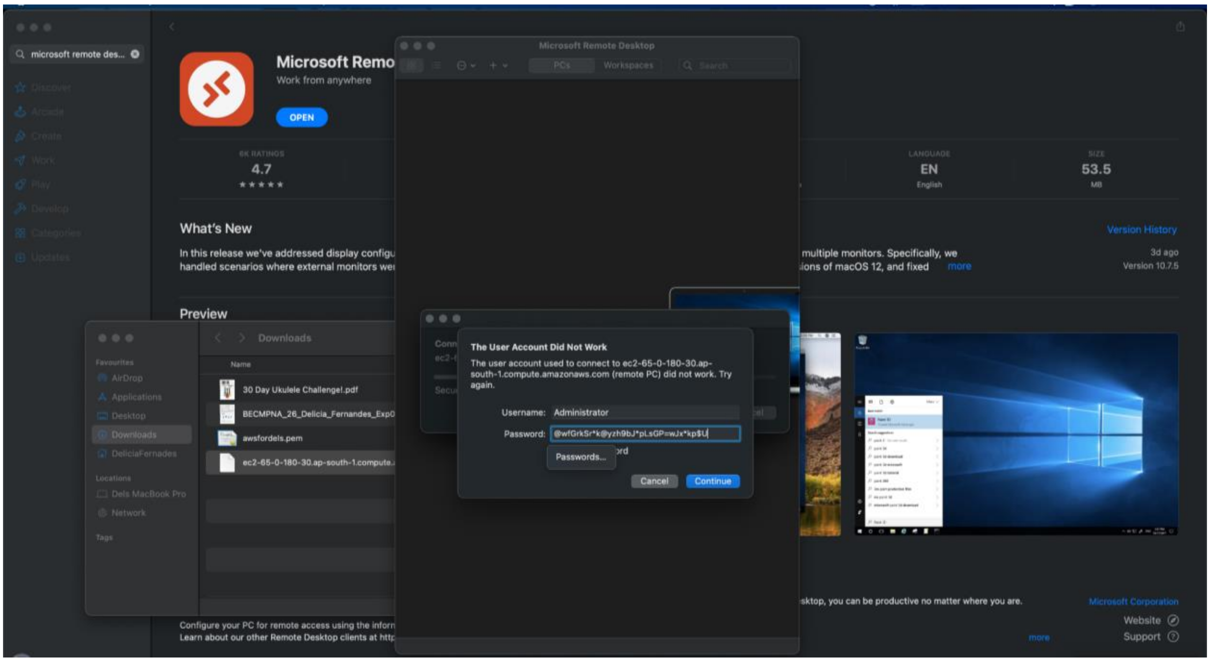
The user account used to connect to ec2-65-0-180-30.ap-south-1.compute.amazonaws.com (remote PC) did not work. Try again.

Username: Administrator

Password:

□ Show password

Cancel | Continue



The User Account Did Not Work

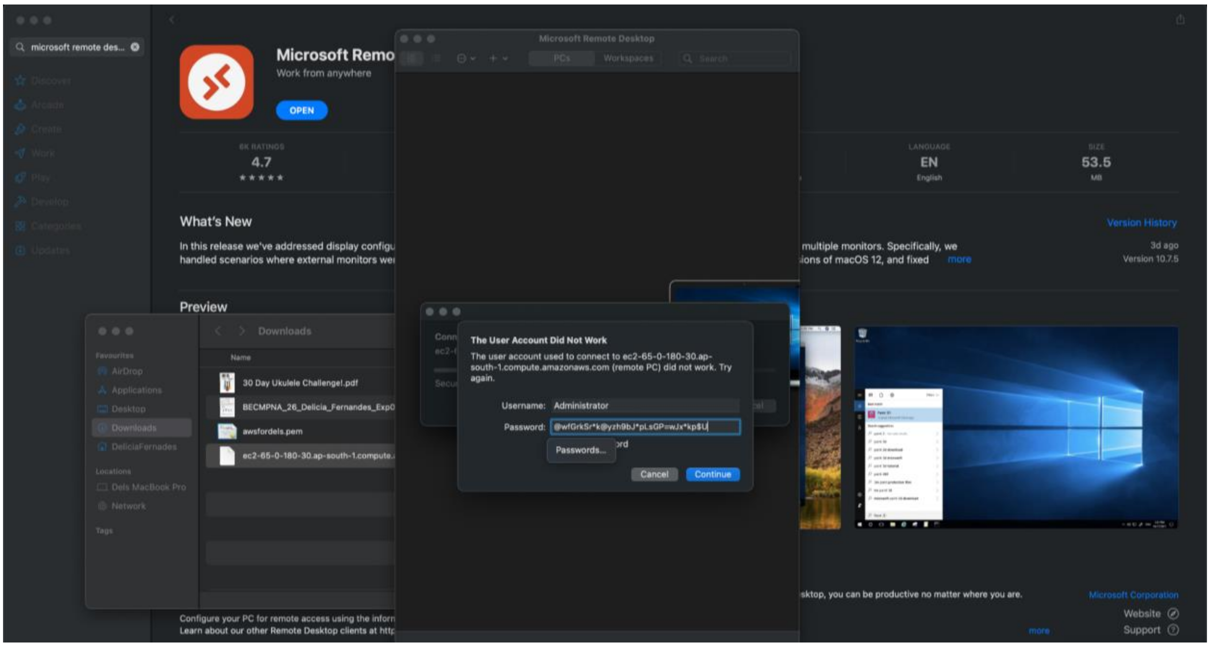
The user account used to connect to ec2-65-0-180-30.ap-south-1.compute.amazonaws.com (remote PC) did not work. Try again.

Username: Administrator

Password: @wfGrkSr*k@yzh9bJ*pLsGP=wJx*kp$U

Passwords...

Cancel Continue


The User Account Did Not Work

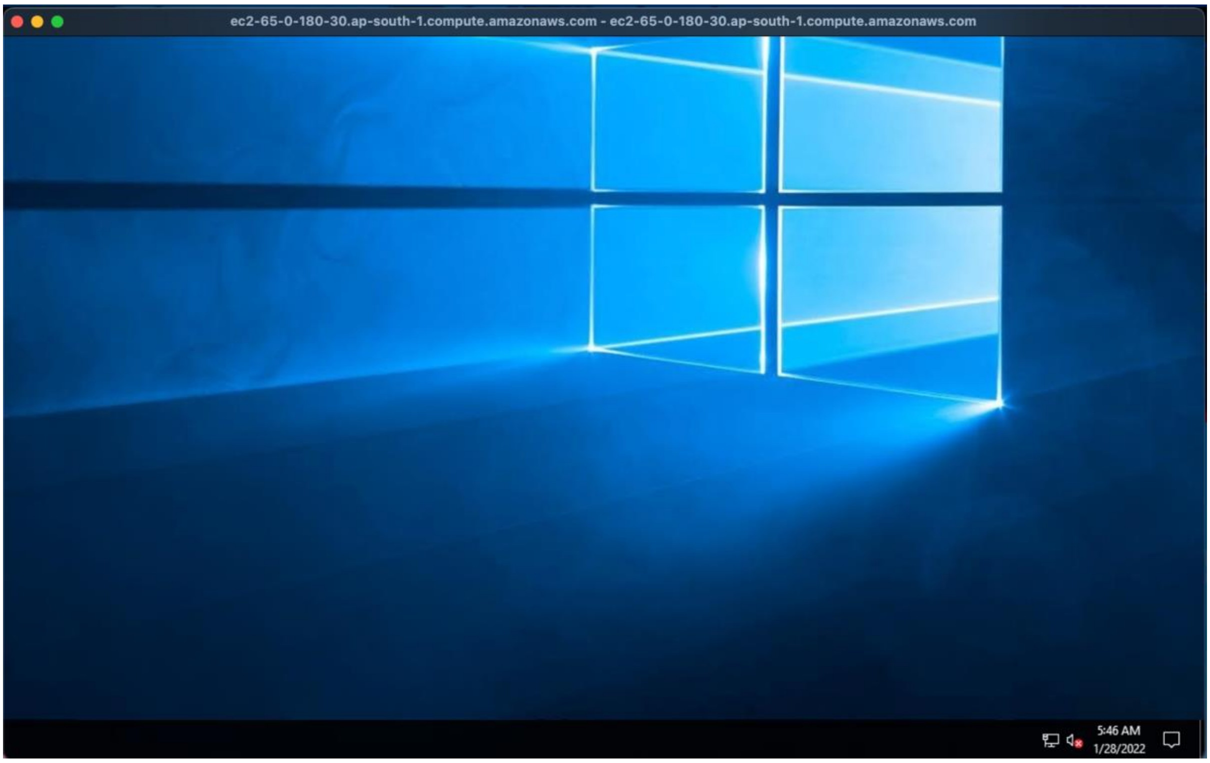
The user account used to connect to ec2-65-0-180-30.ap-south-1.compute.amazonaws.com (remote PC) did not work. Try again.

Username: Administrator

Password: @wfGrkSr*k@yzh9bJ*pLsGP=wJx*kp$U

Passwords...

Cancel Continue



ec2-65-0-180-30.ap-south-1.compute.amazonaws.com - ec2-65-0-180-30.ap-south-1.compute.amazonaws.com
5:46 AM
1/28/2022

Conclusion:

What are the benefits of using IaaS?

Cost savings:
An obvious benefit of moving to the IaaS model is lower infrastructure costs. No longer do organizations have the responsibility of ensuring uptime, maintaining hardware and networking equipment, or replacing old equipment. IaaS also saves enterprises from having to buy more capacity to deal with sudden business spikes. Organizations with a smaller IT infrastructure generally require a smaller IT staff as well.

The pay-as-you-go model also provides significant cost savings. Because IaaS use is metered, organizations pay for only the capacity needed at any given time. This method also allows them to avoid large fixed monthly or annual fees for benefits they may not use. The IaaS model demands no upfront charges, bandwidth utilization fees or minimum term commitments.

Scalability and flexibility:
One of the greatest benefits of IaaS is the ability to scale up and down quickly in response to an enterprise’s requirements. IaaS providers generally have the latest, most powerful storage, servers and networking technology to accommodate the needs of their customers. This on-demand scalability provides added flexibility and greater agility to respond to changing opportunities and requirements. This is especially helpful in building and dismantling test and development environments, which greatly benefit from this increased speed and agility.

Faster time to market:
Competition is strong in every sector, and time to market is one of the best ways to beat the competition. Because IaaS provides elasticity and scalability, organizations can ramp up and get the job done (and the product or service to market) more rapidly.

Support for DR, BC and high availability:
While every enterprise has some type of disaster recovery plan, the technology behind those plans is often expensive and unwieldy. Organizations with several disparate locations often have different disaster recovery and business continuity plans and technologies, making management virtually impossible.

IaaS provides a consolidated disaster recovery infrastructure, reducing costs and increasing manageability. Frost & Sullivan research has determined that CIOs consider business continuity and preparing for disaster recovery the top drivers for adopting IaaS.

If disaster strikes, employees can access the same infrastructure they have always accessed via an Internet connection, from wherever they happen to be. This includes everything the organization needs to function as usual — email, web servers and critical applications. The result: quick recovery with no loss of data.

Focus on business growth:
Time, money and energy spent making technology decisions and hiring staff to manage and maintain the technology infrastructure is time not spent on growing the business. By moving infrastructure to a service-based model, organizations can focus their time and resources where they belong, on developing innovations in applications and solutions.

Benefits of IaaS Technology

- 1. Increased Performance, Decreased CapEx
- 2. Increased Security
- 3. Increased Scalability and Flexibility
- 4. Increased Support for Disaster Recovery and Business Continuity

References:

Infrastructure-as-a-Service: Benefits of IaaS Cloud Computing
infrastructure-service-5-important-benefits
IBM/Iass
Advantages and disadvantages of IaaS (Infrastructure as a Service) – Business Tech Planet