

# **A guide to the use of the HCP platform on AWS**

## **1. What is AWS?**

AWS, Amazon Web Services, is Amazon's cloud computing IaaS and PaaS platform services. AWS provides users with a complete set of cloud computing services, including elastic computing, storage, databases, and applications, which can help enterprises reduce IT input costs and maintenance costs.

AWS provides a complete set of infrastructure and application services to run virtually everything in the cloud: from enterprise applications and big data projects to social games and mobile applications.

Website: [https://aws.amazon.com/what-is-aws/?nc1=h\\_ls](https://aws.amazon.com/what-is-aws/?nc1=h_ls)

## **2. What is Amazon EC2**

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable compute capacity in the Amazon Cloud Technologies (AWS) cloud. Using Amazon EC2 avoids upfront hardware investments, so you can quickly develop and deploy your applications. You can use Amazon EC2 to start as many virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 lets you scale up or down to handle changes in demand or spikes in usage, reducing the need to forecast traffic.

Website:

[https://docs.aws.amazon.com/zh\\_cn/AWSEC2/latest/WindowsGuide/concepts.html](https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/WindowsGuide/concepts.html)

## **3. How to use Amazon EC2**

**(1) If you do not have an account, create an AWS account:**

[https://portal.aws.amazon.com/billing/signup?nc2=h\\_ct&src=gettingstarted\\_signup&redirect\\_url=https%3A%2F%2Faws.amazon.com%2Fregistration-confirmation&language=zh\\_cn#/start](https://portal.aws.amazon.com/billing/signup?nc2=h_ct&src=gettingstarted_signup&redirect_url=https%3A%2F%2Faws.amazon.com%2Fregistration-confirmation&language=zh_cn#/start)

**(2) If you already have an account, log in to AWS, enter Amazon Web Services Management Console, and select "Launch a virtual machine".**

# Amazon Web Services Management Console

## (3) Use the "Quick Start" wizard to create an EC2 instance

### Step 1: Choose an Amazon Machine Image (AMI)

Suggestion: Select a windows version that meets your habits

### Step 2: Choose an Instance Type

Recommended:

Low level	High level
Amazon AWS EC2 Instance: c5.xlarge CPU: Intel® Xeon® Cascade Lake @ 3.60 GHz vCPU Count: 4 RAM: 8 GB Storage: EBS NIC: 10 Gbps	Amazon AWS EC2 Instance: m5.xlarge CPU: Intel® Xeon® Platinum 8175M @ 3.10 GHz vCPU Count: 4 RAM: 16 GB Storage: EBS NIC: 10 Gbps

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

<input type="checkbox"/>	t3a	t3a.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	c4	c4.large	2	3.75	EBS only	Yes	Moderate	Yes
<input type="checkbox"/>	c4	c4.xlarge	4	7.5	EBS only	Yes	High	Yes
<input type="checkbox"/>	c4	c4.2xlarge	8	15	EBS only	Yes	High	Yes
<input type="checkbox"/>	c4	c4.4xlarge	16	30	EBS only	Yes	High	Yes
<input type="checkbox"/>	c4	c4.8xlarge	32	60	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	c5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
<input checked="" type="checkbox"/>	c5	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5	c5.4xlarge	16	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5	c5.9xlarge	36	72	EBS only	Yes	10 Gigabit	Yes
<input type="checkbox"/>	c5	c5.12xlarge	48	96	EBS only	Yes	12 Gigabit	Yes
<input type="checkbox"/>	c5	c5.18xlarge	72	144	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	c5	c5.24xlarge	96	192	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	c5	c5.metal	96	192	EBS only	Yes	25 Gigabit	Yes
<input type="checkbox"/>	c5a	c5a.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5a	c5a.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5a	c5a.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

### Step 3: Configure Instance Details

#### Instructions:

**Network:** Launch your instance into an Amazon Virtual Private Cloud (VPC). You can create a VPC and select your own IP address range, create subnets, configure route tables, and configure network gateways. Learn more about Amazon VPC.

(Boot your instance into Amazon Virtual Private Cloud (VPC). You can create a VPC and select your own IP address range, create subnets, configure routing tables, and configure network gateways.)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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

Purchasing option  Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)

Auto-assign Public IP  Use subnet setting (Enable)

Placement group  Add instance to placement group

Capacity Reservation  [Create new Capacity Reservation](#)

Domain join directory  [Create new directory](#)

IAM role  [Create new IAM role](#)

Shutdown behavior

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   
Additional charges will apply for dedicated tenancy.

Credit specification  Unlimited  
Additional charges may apply

Advanced Details

Cancel Previous **Review and Launch** Next: Add Storage

If no VPC is available, create a “VPC with a Single Public Subnet”.

## Step 1: Select a VPC Configuration

### VPC with a Single Public Subnet

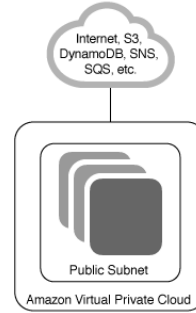
### VPC with Public and Private Subnets

Your instances run in a private, isolated section of the Amazon Web Services cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

#### Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select



## Step 2: VPC with a Single Public Subnet

IPv4 CIDR block: 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block:  No IPv6 CIDR block  
 Amazon provided IPv6 CIDR block

VPC name: vpc-new

Public subnet's IPv4 CIDR: 10.0.0.0/24 (251 IP addresses available)

Availability Zone: No Preference

Subnet name: Public subnet

You can add more subnets after Amazon Web Services creates the VPC.

#### Service endpoints

Add Endpoint

Enable DNS hostnames:  Yes  No

Hardware tenancy: Default

Cancel and Exit Back Create VPC

## Step 4: Add Storage

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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 (MiB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0e5cc602ca2356395b	1024	Magnetic (standard)	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

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

## Step 5: Add Tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### 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
------------------------------	--------------------------------	-----------	---------	--------------------

This resource currently has no tags.

Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

## Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic of 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 to allow unrestricted access to HTTP and HTTPS ports.

## Suggestion:

1. Configure the port opening rules required by users
2. Configure an external port rule based on the external port provided by the HCP platform, for example, the external port of HTTP port 80

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:

Description:

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

Add Rule

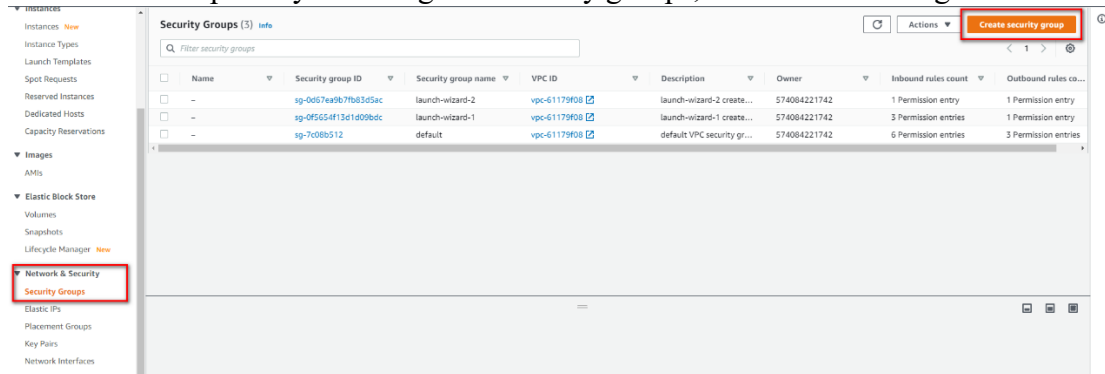
**Warning**  
Rules with source of 0.0.0.0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

## What is a security group:

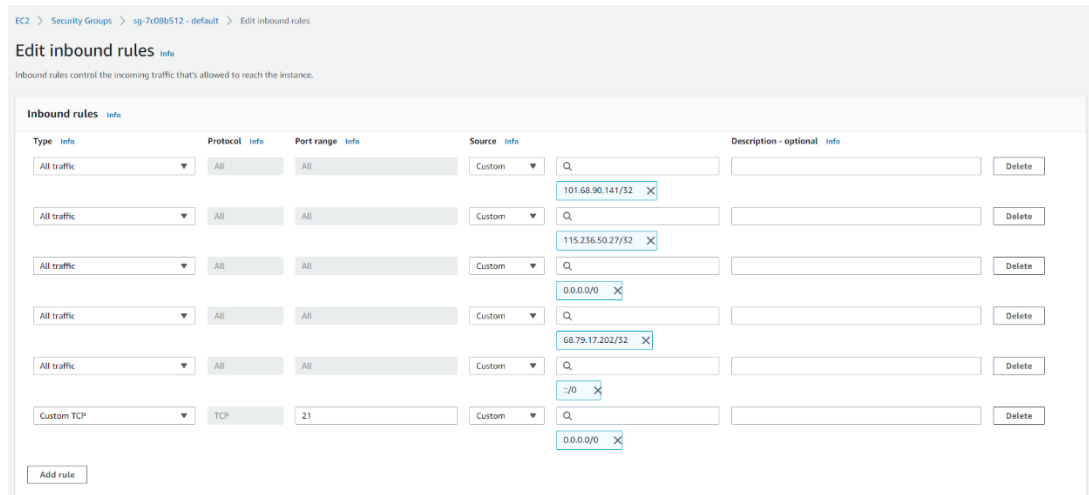
A security group acts as a virtual firewall that controls the traffic of one or more instances. When you start an instance, you can specify one or more security groups. You can modify security group rules at any time. The new rule is automatically applied to all instances associated with the security group. When deciding whether to allow traffic to reach an instance, we evaluate the rules from all the security groups associated with that instance.

When you start an instance in a VPC, you must specify a security group to be created for that VPC. After you start an instance, you can change its security group. A security group is associated with a network interface. Changing the security group of an instance also changes the security group associated with the primary network interface (eth0). For more information, see "Changing an Instance's Security Group" in the Amazon VPC User Guide. You can also change the security group associated with any other network interface.

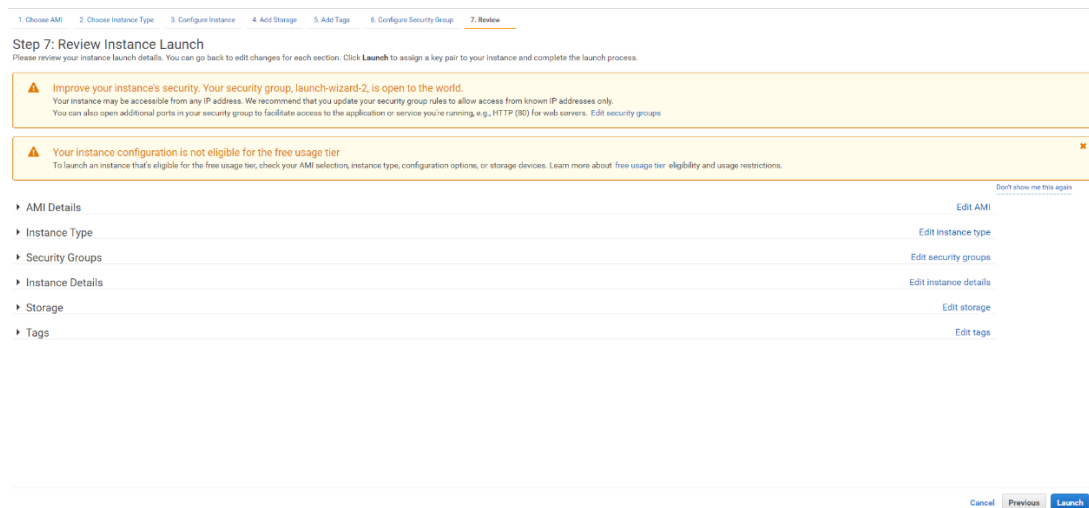
AWS has the capability to manage all security groups, as shown in the figure below.



To edit a security group, you can modify rules.



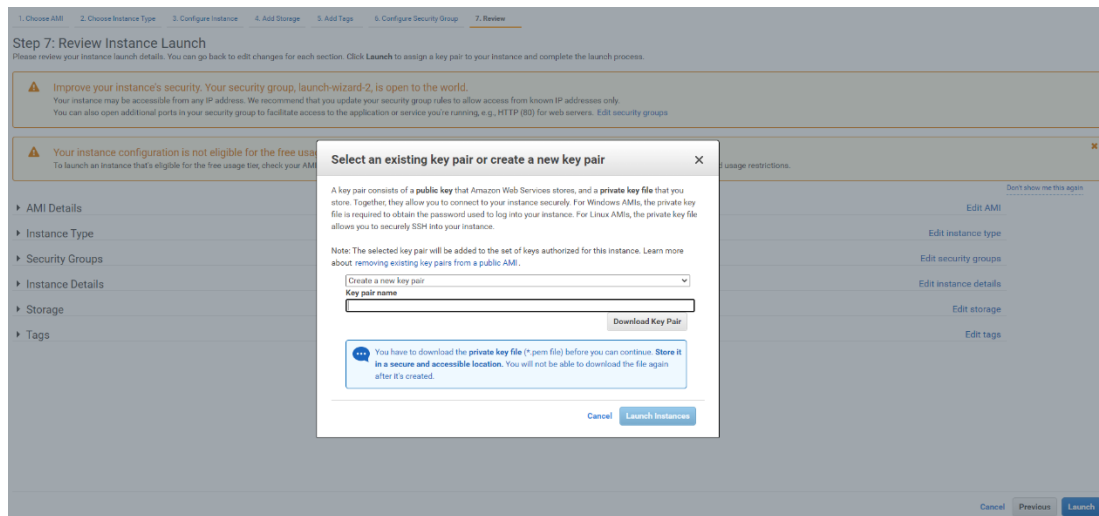
## Step 7: Review Instance Launch



- The Key pairs page lists all of your key pairs in the currently selected AWS Region.
- You can change which columns are visible in the table. Choose the settings icon in the top-right corner of the page, and select the columns to display.
- You can manage a key pair's tags and delete a key pair. Select a key pair by selecting its check box, and then choose an action from the Actions menu.
- You can have Amazon EC2 create a new key pair for you. You can also use a third-party tool to create a new key pair and import the key pair to Amazon EC2. To have Amazon EC2 create a key pair, choose Create key pair. To import a key pair that was created using a third-party tool, choose Import key pair from the Actions menu.

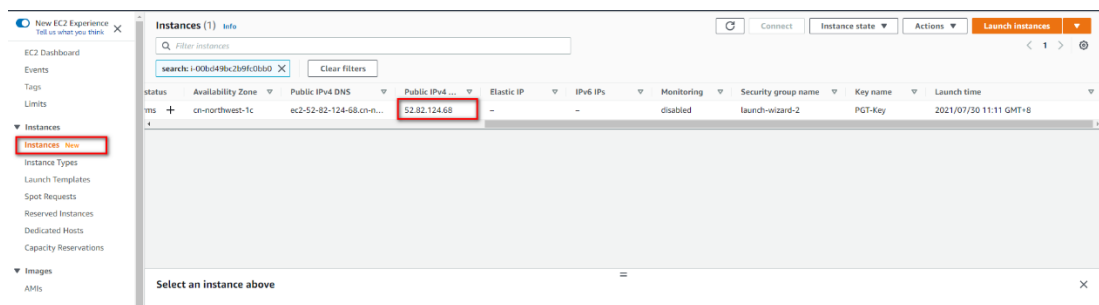
Note:

If you create a new key pair, download the corresponding key pair file to the local PC. This file is required when you obtain the administrator password of the windows operating system.

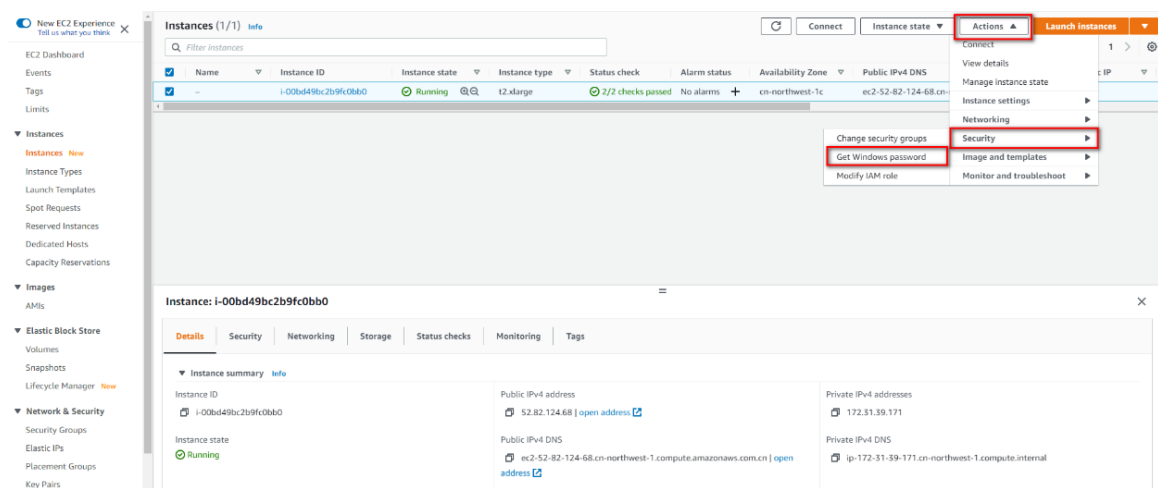


#### (4) How to connect the EC2 instance after it is successfully created

a. Provide the external IP address and DNS address. The default IP address and DNS address assigned will change each time you start up. It is recommended to purchase a fixed IP address or DNS service from AWS.



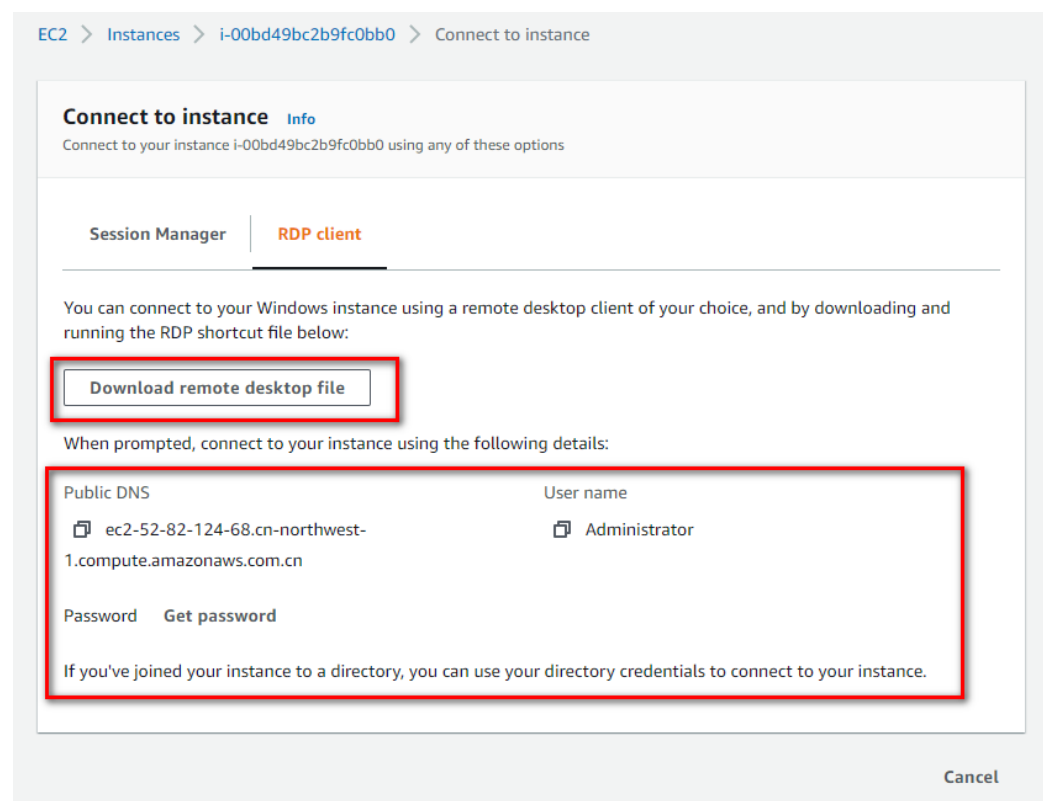
b. Obtain the password of the windows operating system.







c. Download the tool RDP for remotely connecting EC2 instances. After downloading and installing the tool, you can use the following information to connect EC2 instances. Or use windows Remote desktop to login.



Note:

a. When you apply for VM configuration, see Chapter 2 in the Software Requirements document of the HCP platform software.

<https://www.hikvision.com/en/support/download/software/hikcentral-professional-v2-4-1/>

b. Amazon has banned ports 80 and 443, so after HCP is installed, 80 and 443 need to be changed to other ports such as 81 and 444 in the external network configuration of SYS.

## 4. Acquisition, installation and use of HCP

(1) HCP Download

<https://www.hikvision.com/en/support/download/software/hikcentral-professional-v2-4-1/>

(2) Installation the HCP

"Quick Start Guide" for HCP document, download link:

[https://pinfo.hikvision.com/hkwsen/unzip/20230314155521\\_74796\\_doc/](https://pinfo.hikvision.com/hkwsen/unzip/20230314155521_74796_doc/)

(3) Use of HCP

Obtain HCP User Manual of Control Client, User Manual of Web Client, etc., download link:

[https://pinfo.hikvision.com/hkwsen/unzip/20230712151753\\_98833\\_doc/](https://pinfo.hikvision.com/hkwsen/unzip/20230712151753_98833_doc/)

(4) More HCP information please refer to the website:

<https://www.hikvision.com/en/support/download/software/>