Hyper Elastic Cloud Server

User Guide

Issue	**08**
Date	**2021-01-06**



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Logging In to a Windows HECS 1
1.1 Login Overview 1
1.2 Login Using VNC 2
1.3 Logging In to a Windows HECS Using an RDP File 3
1.4 Login Using MSTSC 4
1.5 Logging In to a Windows HECS from a Linux Server 12
1.6 Logging In to a Windows HECS from a Mobile Terminal 14
1.7 Logging In to a Windows HECS from a Mac 21
2 Logging In to a Linux HECS 26
2.1 Login Overview 26
2.2 Login Using VNC 27
2.3 Logging In to a Linux HECS Using an SSH Password 29
2.4 Logging In to a Linux HECS from a Mobile Terminal 32
3 Managing HECSs 43
3.1 Viewing Details About an HECS 43
3.2 Changing an HECS Name 44
3.3 Reinstalling the OS 45
3.4 Changing an OS 46
3.5 Changing the Time Zone for an HECS 49
4 Modifying HECS Specifications 52
5 EVS Disks 56
5.1 Overview 56
5.2 Adding Disks to an HECS 56
5.3 Attaching a Disk to an HECS 60
5.4 Detaching a Disk from an HECS 62
5.5 Expanding Disk Capacity 64
5.6 Initializing a Windows Data Disk Using a Script 65
5.7 Initializing a Linux Data Disk Using a Script 72
6 Password 76
6.1 Resetting an HECS Password on the Management Console 76
6.2 Changing the Login Password on an HECS 78

 Copyright © Huawei Technologies Co., Ltd.

7 NICs 80
7.1 Overview 80
7.2 Adding a NIC 80
7.3 Deleting an Extension NIC 82
7.4 Changing a VPC 83
7.5 Modifying a Private IP Address 84
7.6 Managing Virtual Private IP Addresses 85
8 Security Groups 86
8.1 Overview 86
8.2 Default Security Group and Rules 87
8.3 Security Group Configuration Examples 88
8.4 Configuring Security Group Rules 91
8.5 Changing a Security Group 94
9 Host Security Service 95
10 Resources and Tags 97
10.1 Quota Adjustment 97
11 Monitoring 99
11.1 Monitoring HECSs 99
11.2 Basic HECS Metrics 99
11.3 OS Monitoring Metrics Supported by HECSs with the Agent Installed 103
11.4 OS Monitoring Metrics Supported by HECSs with the New Edition of Agent Installed 126
11.5 Setting Alarm Rules 130
11.6 Viewing HECS Metrics 131
12 Change History 133

 Copyright © Huawei Technologies Co., Ltd.

1 Logging In to a Windows HECS

1.1 Login Overview

Notes and Constraints

- Only a running HECS can be logged in.
- The username for logging in to a Windows HECS is **Administrator**.
- If you log in to an HECS for the first time or want to reset a password, locate the row that contains the target HECS and click **Reset Password** in the **Operation** column.

Login Modes

Select a login method and log in to the HECS.

Table 1-1 Windows HECS login modes

HECS OS	Local OS	Connection Method	Remarks
Windows	Windows	(Recommended) Use CloudShell on the management console to log in to the HECS. 1.3 Logging In to a Windows HECS Using an RDP File	The HECS has an EIP bound. (If you communicate with an HECS through the private network, for example, through VPN or Direct Connect, the HECS does not require an EIP.)
	Windows	Click **Start** on the local computer. In the **Search programs and files** text box, enter **mstsc** to open the **Remote Desktop Connection** dialog box. 1.5 Logging In to a Windows HECS from a Linux Server	
	Linux	Install a remote connection tool, for example, rdesktop. 1.5 Logging In to a Windows HECS from a Linux Server	
	Mac	Install a remote connection tool, for example, Microsoft Remote Desktop	

Copyright © Huawei Technologies Co., Ltd.

HECS OS	Local OS	Connection Method	Remarks
		for Mac. 1.6 Logging In to a Windows HECS from a Mobile Terminal	
	Mobile terminal	Install a remote connection tool, for example, Microsoft Remote Desktop. 1.6 Logging In to a Windows HECS from a Mobile Terminal	
	Windows	Use the remote login function available on the management console. For details, see 1.2 Login Using VNC.	No EIP is required.

Helpful Links

- Can I Retrieve My Remote Login Password?
- How Can I Enable Multi-User Login on a Windows HECS?
- Why Cannot I Log In to My Windows HECS?

1.2 Login Using VNC

Scenarios

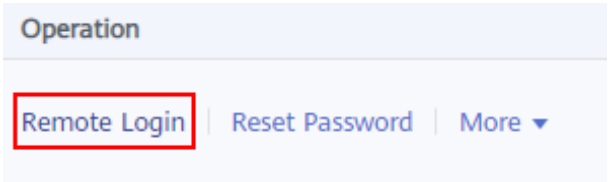
This section describes how to use VNC provided on the management console to log in to an HECS.

Procedure for Windows HECSs

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. Obtain the password for logging in to the HECS.

   Before logging in to an HECS using VNC, you must obtain the login password.
5. In the **Operation** column of the target HECS, click **Remote Login**.

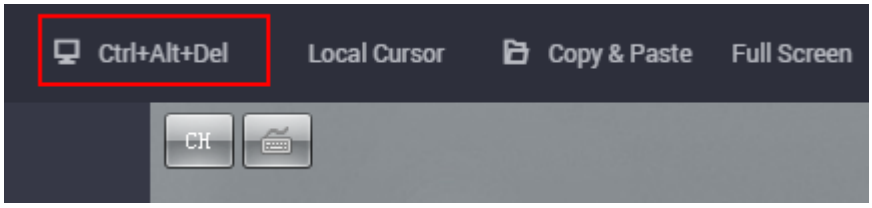
Figure 1-1 Remote Login



Copyright © Huawei Technologies Co., Ltd.

6. (Optional) When the system displays "Press CTRL+ALT+DELETE to log on", click **Ctrl+Alt+Del** in the upper part of the remote login page to log in to the HECS.

   Figure 1-2 Ctrl+Alt+Del

7. Enter the HECS password as prompted.

1.3 Logging In to a Windows HECS Using an RDP File

Scenarios

Remote Desktop Protocol (RDP) is a multi-channel remote login protocol provided by Microsoft. This section describes how to use an RDP file to remotely log in to a Windows HECS.

NOTE

Each RDP file downloaded from the management console can be used to log in to only one HECS, and the file is named in the format of "HECS name-EIP".

Prerequisites

- The target HECS is running.
- The HECS has an EIP bound.
- Access to port 3389 is allowed in the inbound direction of the security group to which the HECS belongs.
- The network connection between the login tool and the target HECS is normal. For example, the default port 3389 is not blocked by a firewall.
- RDP has been enabled on the target HECS. By default, RDP has been enabled on the HECSs created using a public image. For instructions on how to enable RDP, see Enabling RDP.

Logging In to a Windows HECS Using an RDP File

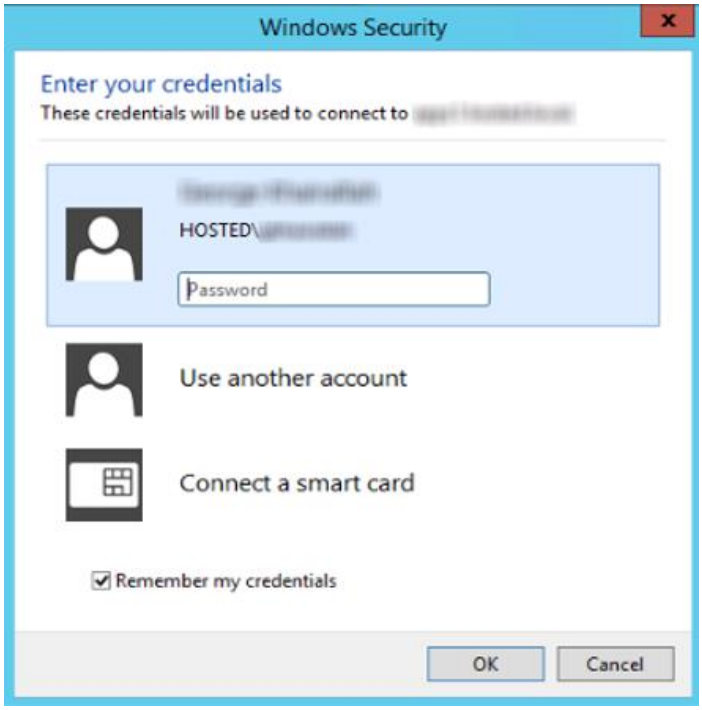
If your local server runs the Windows, you can use an RDP file to log in to a Windows HECS.

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. In the **Logging In to a Windows HECS** dialog box, select **RDP-based Login** and click **Download RDP File** to download the RDP file to the local server.
4. Double-click the downloaded RDP file and enter the password to remotely access the Windows HECS.

Copyright © Huawei Technologies Co., Ltd.

- If your HECS uses password for login, log in to the HECS using the password configured when you created this HECS.
- If your password has been forgotten, see 6.1 Resetting an HECS Password on the Management Console.

Figure 1-3 Logging in to a Windows HECS using an RDP file



1.4 Login Using MSTSC

Scenarios

This section describes how to use the remote login tool MSTSC to log in to a Windows HECS from a local computer.

Prerequisites

- The HECS is running.
- The HECS has an EIP bound.

  When logging in to an HECS through an intranet using MSTSC, for example, through VPN or Direct Connect, you do not need to bind an EIP to the HECS.
- Access to port 3389 is allowed in the inbound direction of the security group to which the HECS belongs.
- The network connection between the login tool and the target HECS is normal. For example, the default port 3389 is not blocked by a firewall.

 Copyright © Huawei Technologies Co., Ltd.

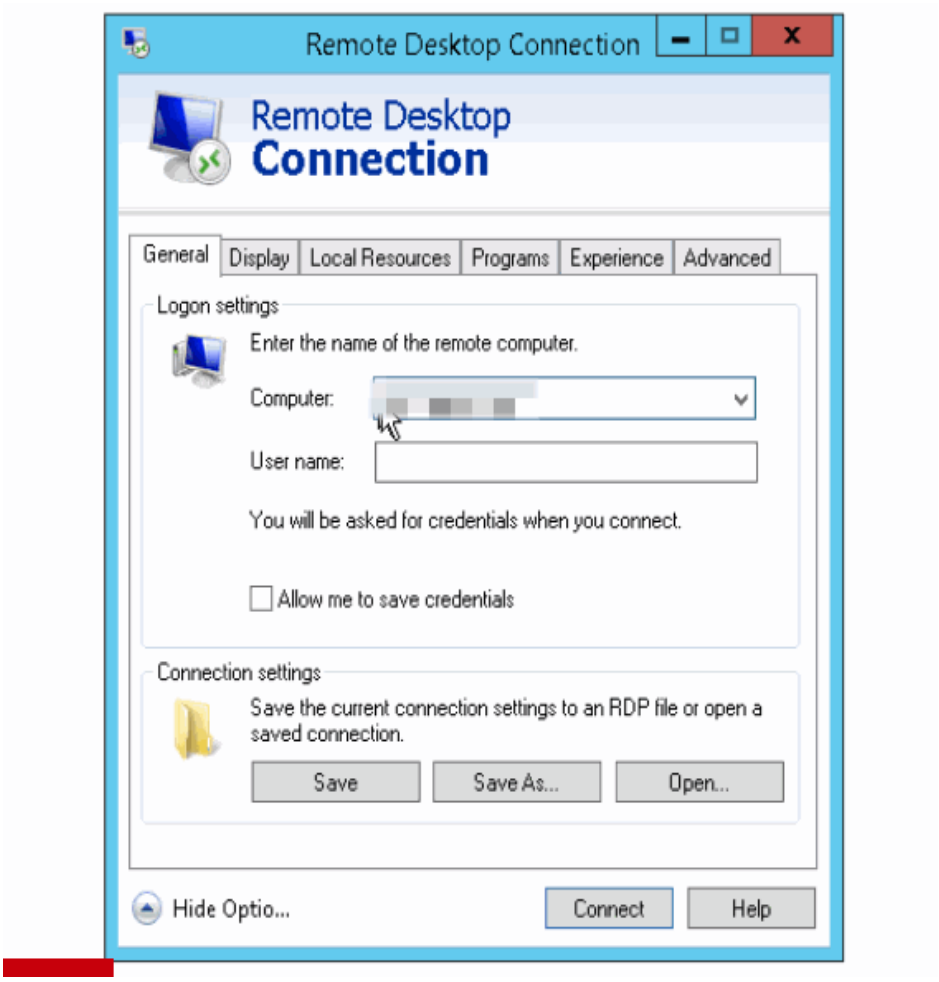
- Remote Desktop Protocol (RDP) has been enabled on the target HECS. By default, RDP has been enabled on the HECSs created using a public image. For instructions on how to enable RDP, see Enabling RDP.

Logging In to a Windows HECS Using VNC

If your local server runs Windows, you can use the remote desktop connection tool MSTSC delivered with the Windows OS to log in to a Windows HECS.

The following section describes how to use MSTSC to log in to the Windows Server 2012 HECS.

Figure 1-4 Logging in to an HECS using MSTSC

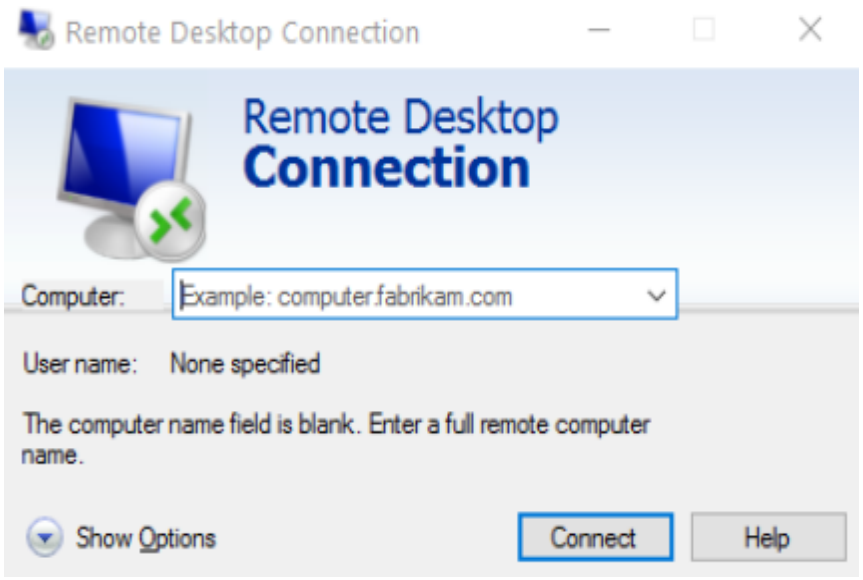


The procedure is as follows:

1. Click the start menu on the local server.
2. In the **Search programs and files** text box, enter **mstsc**.
3. In the **Remote Desktop Connection** dialog box, click **Show Options**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-5 Show Options



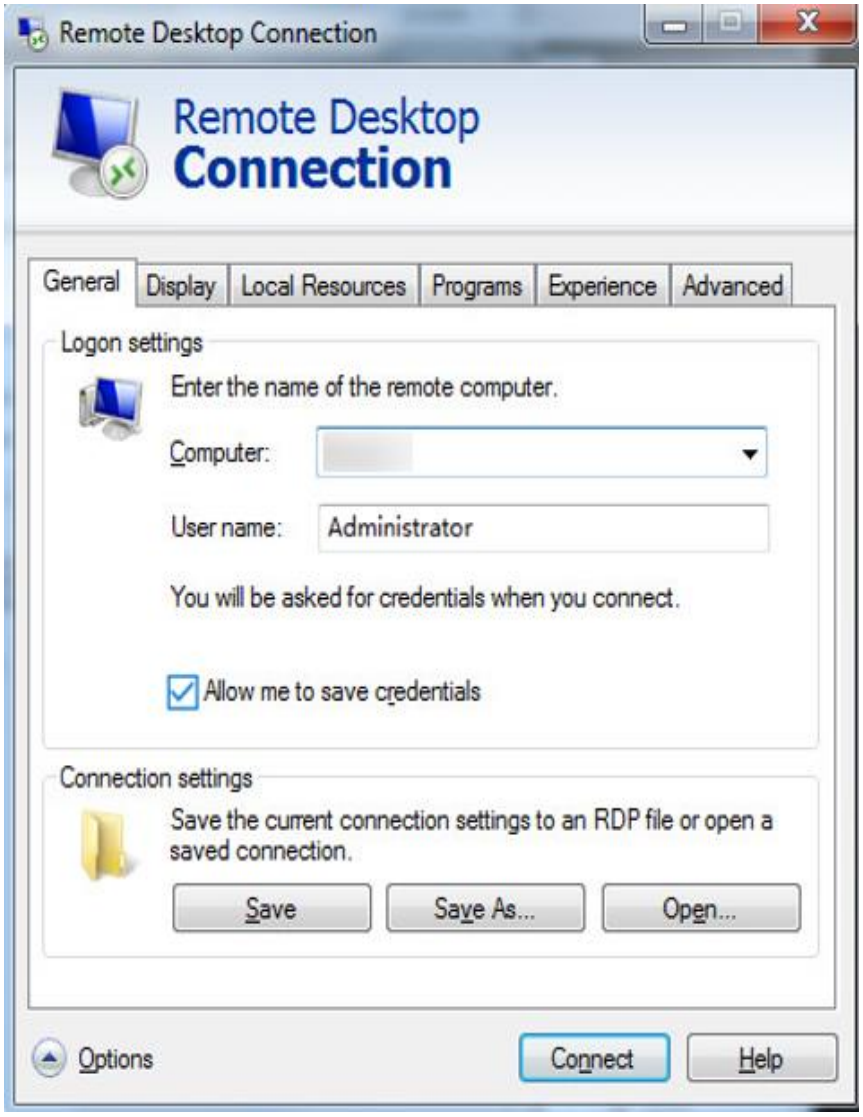
4. Enter the EIP and username (**Administrator** by default) of the target HECS.

NOTE

If you do not want to enter the username and password in follow-up logins, select **Allow me to save credentials**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-6 Remote Desktop Connection



5. (Optional) To use local server resources in a remote session, configure parameters on the **Local Resources** tab.

   To copy data from the local server to your HECS, select **Clipboard**.

 Copyright © Huawei Technologies Co., Ltd.

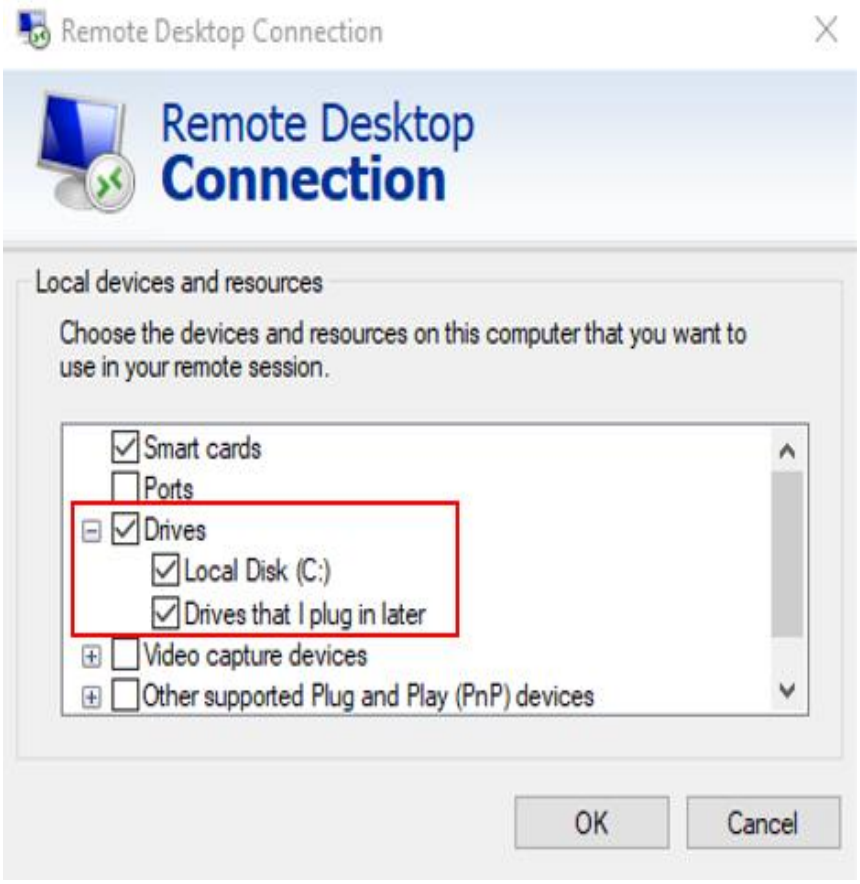
Figure 1-7 Clipboard



To copy files from the local server to your HECS, click **More** and select **Drives** and the desired disks.

 Copyright © Huawei Technologies Co., Ltd.

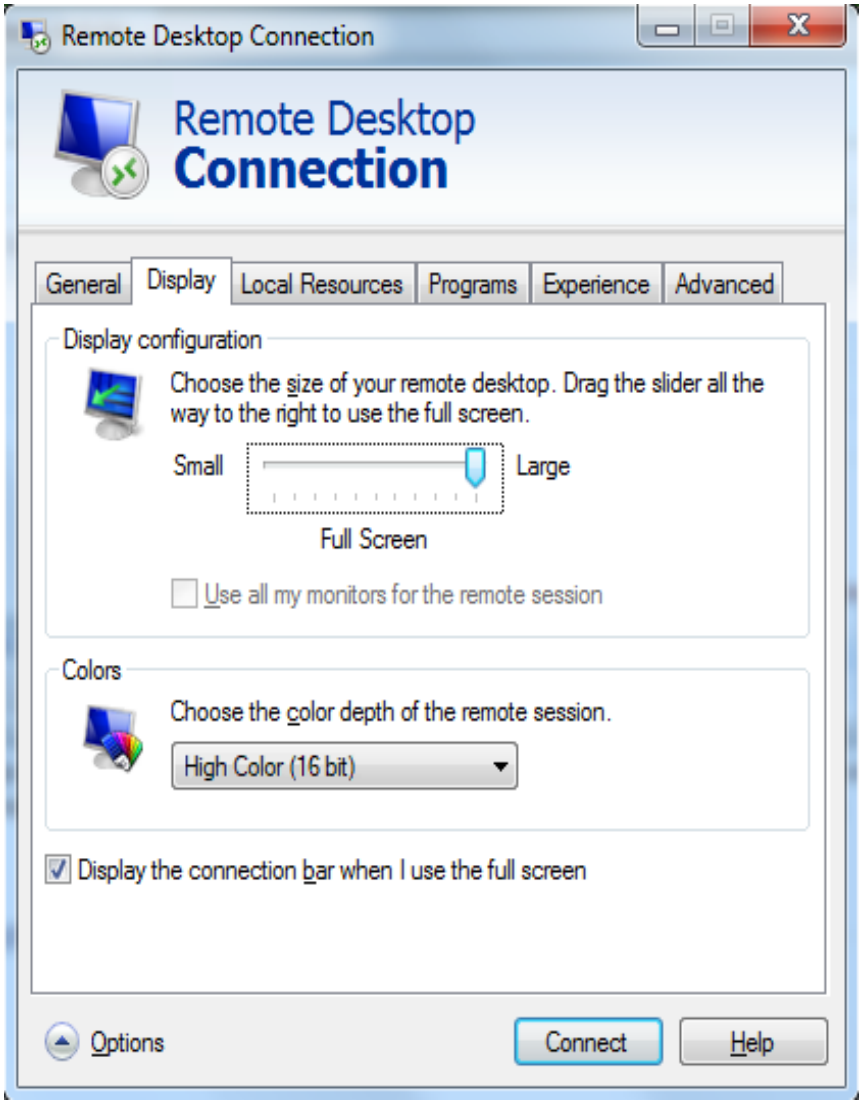
Figure 1-8 Drives



6. (Optional) Click the **Display** tab and then adjust the size of the remote desktop.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-9 Adjusting the size of the desktop

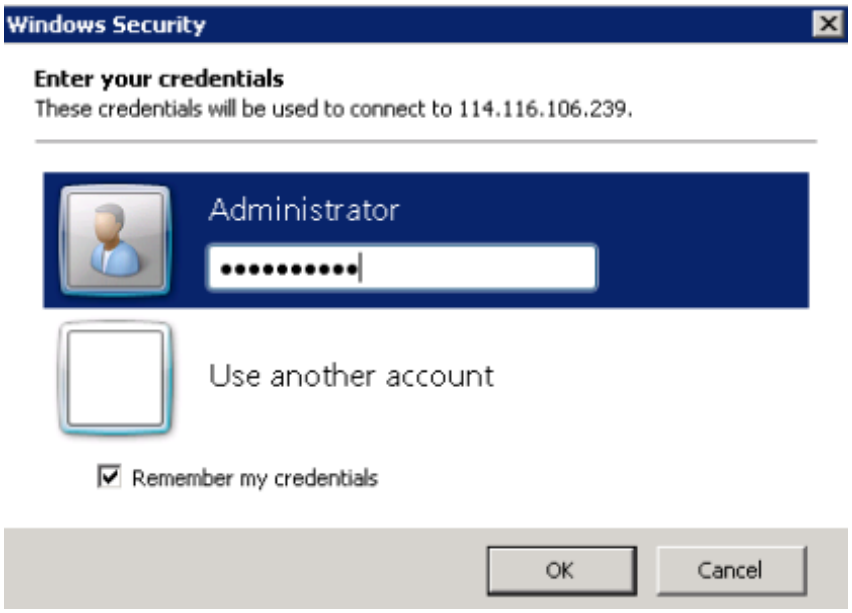


7. Click **OK** and enter the login password as prompted to log in to the HECS.

   To ensure system security, change the login password after you log in to the HECS for the first time.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-10 Entering the login password



8. (Optional) After logging in to the HECS using RDP, handle the issue that local files larger than 2 GB cannot be copied to a remote Windows HECS.

   For details, see troubleshooting cases.

Enabling RDP

When you log in to an HECS for the first time, log in to it using VNC, enable RDP, and access the HECS using MSTSC.

NOTE

By default, RDP has been enabled on the HECSs created using a public image.

1. Log in to the HECS using VNC.

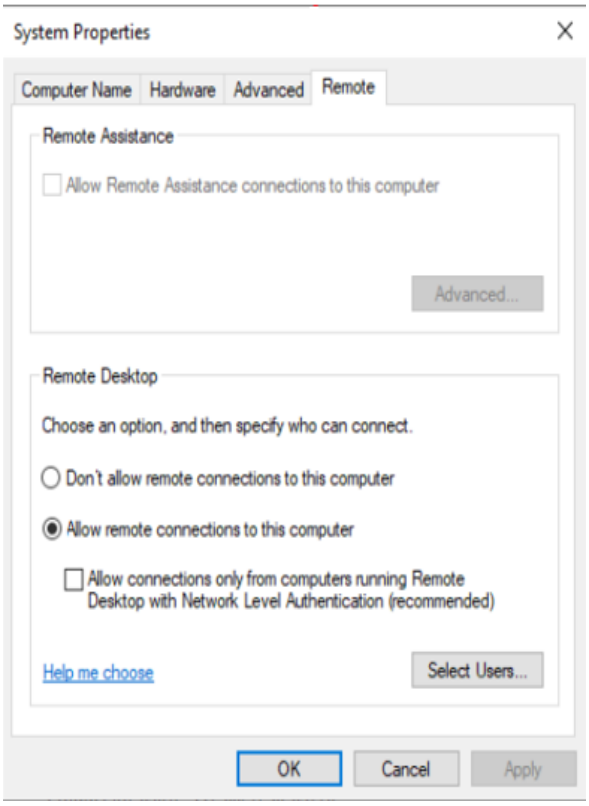
   For details, see 1.2 Login Using VNC.

2. Click **Start** in the task bar and choose **Control Panel** > **System and Security** > **System** > **Remote settings**.

   The **System Properties** dialog box is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-11 System Properties



3. Click the **Remote** tab and select **Allow connections from computers running any version of Remote Desktop (less secure)**.
4. Click **OK**.

1.5 Logging In to a Windows HECS from a Linux Server

Scenarios

This section describes how to log in to a Windows HECS from a Linux server.

Prerequisites

- The HECS is running.
- The HECS has an EIP bound.

  When logging in to an HECS through an intranet using MSTSC, for example, through VPN or Direct Connect, you do not need to bind an EIP to the HECS.
- Access to port 3389 is allowed in the inbound direction of the security group that the HECS is associated with.
- The network connection between the login tool and the target HECS is normal. For example, the default port 3389 is not blocked by the firewall.

 Copyright © Huawei Technologies Co., Ltd.

- RDP has been enabled on the target HECS. By default, RDP has been enabled on the HECSs created using a public image. For instructions about how to enable RDP, see Enabling RDP.

Logging In to a Windows HECS from Local Linux Server

If your local server runs Linux, use a remote access tool, such as rdesktop, to log in to a Windows HECS.

1. Download and install rdesktop on the local server. Download rdesktop.

   yum -y install rdesktop

2. Run the following command to log in to the HECS:

   rdesktop -u *Username* **-p** *Password* **-g** *Resolution EIP*

   For example, run **rdesktop -u administrator -p password -g 1024*720 192.168.x.x**.

Table 1-2 Parameters in the remote login command

Parameter	Description
-u	Username, which defaults to **Administrator** for Windows HECSs
-p	Password for logging in to the Windows HECS
-f	Full screen by default, which can be switched using **Ctrl+Alt+Enter**
-g	Resolution, which uses an asterisk (*) to separate numbers. This parameter is optional. If it is not specified, the remote desktop is displayed in full screen by default, for example, **1024*720**.
EIP	EIP of the Windows HECS to be remotely logged in Replace it with the EIP bound to your Windows HECS.

Enabling RDP

When you log in to an HECS for the first time, log in to it using VNC, enable RDP, and access the HECS using MSTSC.

NOTE

By default, RDP has been enabled on the HECSs created using a public image.

1. Log in to the HECS using VNC.

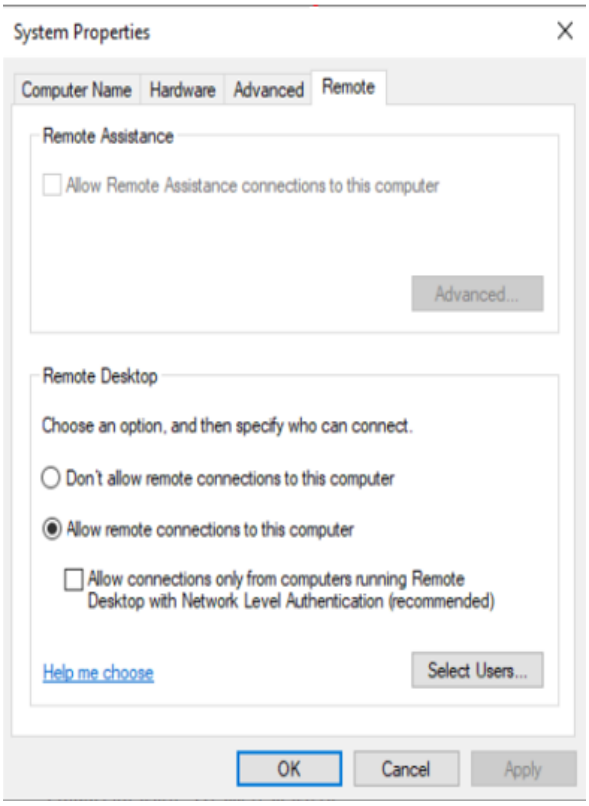
   For details, see 1.2 Login Using VNC.

2. Click **Start** in the task bar and choose **Control Panel** > **System and Security** > **System** > **Remote settings**.

   The **System Properties** dialog box is displayed.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-12 System Properties



3. Click the **Remote** tab and select **Allow connections from computers running any version of Remote Desktop (less secure)**.
4. Click **OK**.

1.6 Logging In to a Windows HECS from a Mobile Terminal

Scenarios

This section describes how to log in to an HECS running Windows Server 2012 R2 DataCenter 64bit from the Microsoft Remote Desktop client.

Prerequisites

- The target HECS is running.
- You have obtained the username and password for logging in to the Windows HECS. If the password has been forgotten, reset the password on the management console.
- The HECS has an EIP bound.
- Access to port 3389 is allowed in the inbound direction of the security group to which the HECS belongs.
- Microsoft Remote Desktop has been installed on the mobile terminal.

 Copyright © Huawei Technologies Co., Ltd.

You can also use other applications that can function as Remote Desktop.

Procedure

1. Start the Microsoft Remote Desktop client.
2. In the upper right corner of the **Remote Desktop** page, tap  and select **Desktop**.

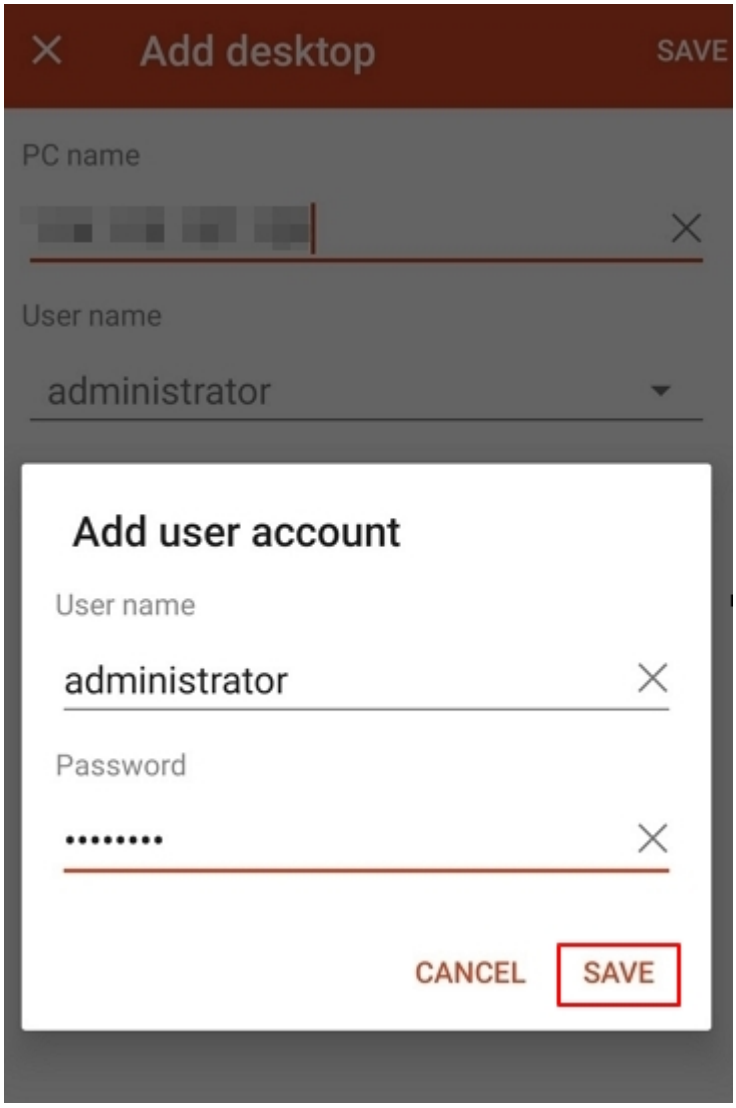
Figure 1-13 Remote Desktop



3. On the **Add desktop** page, set login information and tap **SAVE**.
   - **PC name**: Enter the EIP bound to the target Windows HECS.
   - Perform the following operations to set **User name**:
     i. Tap **User name** and select **Add user account** from the drop-down list.
     The **Add user account** dialog box is displayed.
     ii. Enter username **administrator** and password for logging in to the Windows HECS and tap **SAVE**.

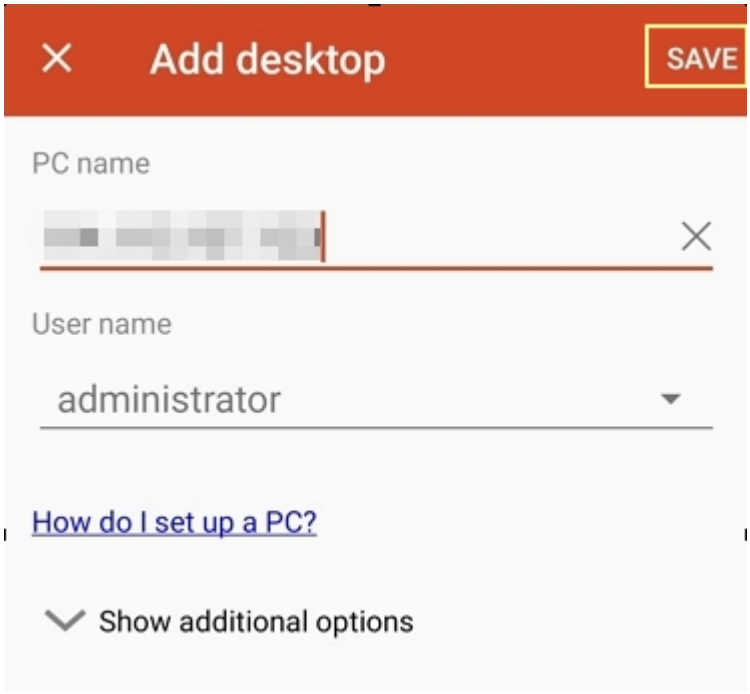
 Copyright © Huawei Technologies Co., Ltd.

Figure 1-14 Setting the login information



Copyright © Huawei Technologies Co., Ltd.

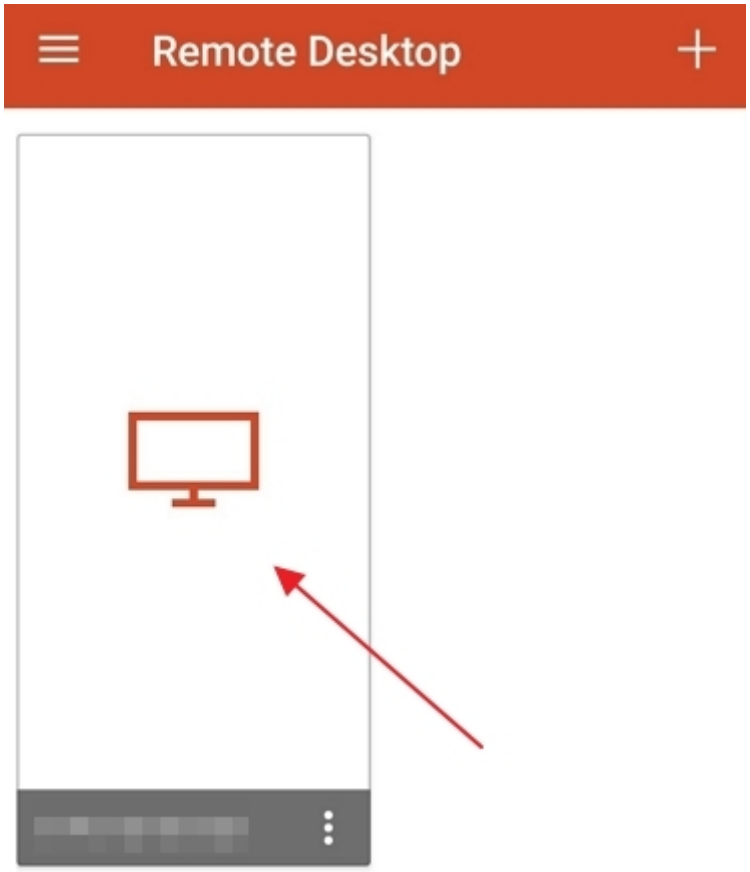
Figure 1-15 Saving the settings



4. On the **Remote Desktop** page, tap the icon of the target Windows HECS.

Copyright © Huawei Technologies Co., Ltd.

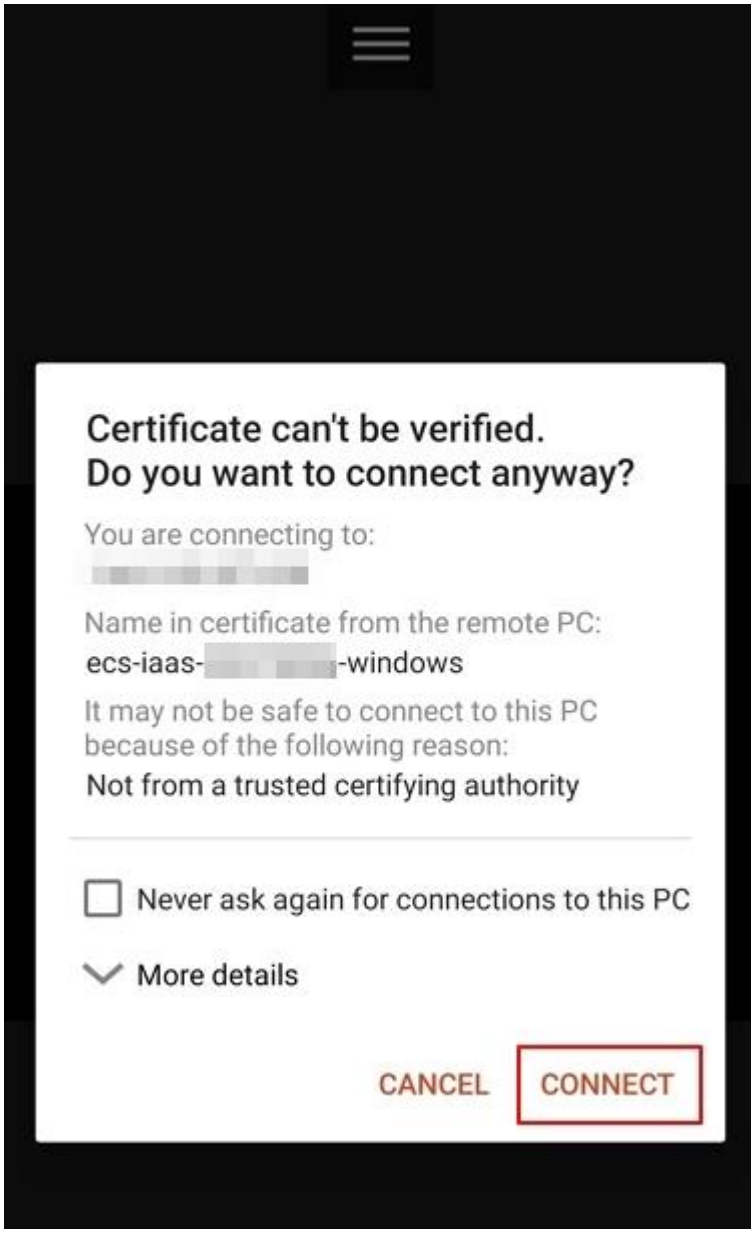
Figure 1-16 Logging in to the Windows HECS



5. Confirm the information and tap **CONNECT**.

 Copyright © Huawei Technologies Co., Ltd.

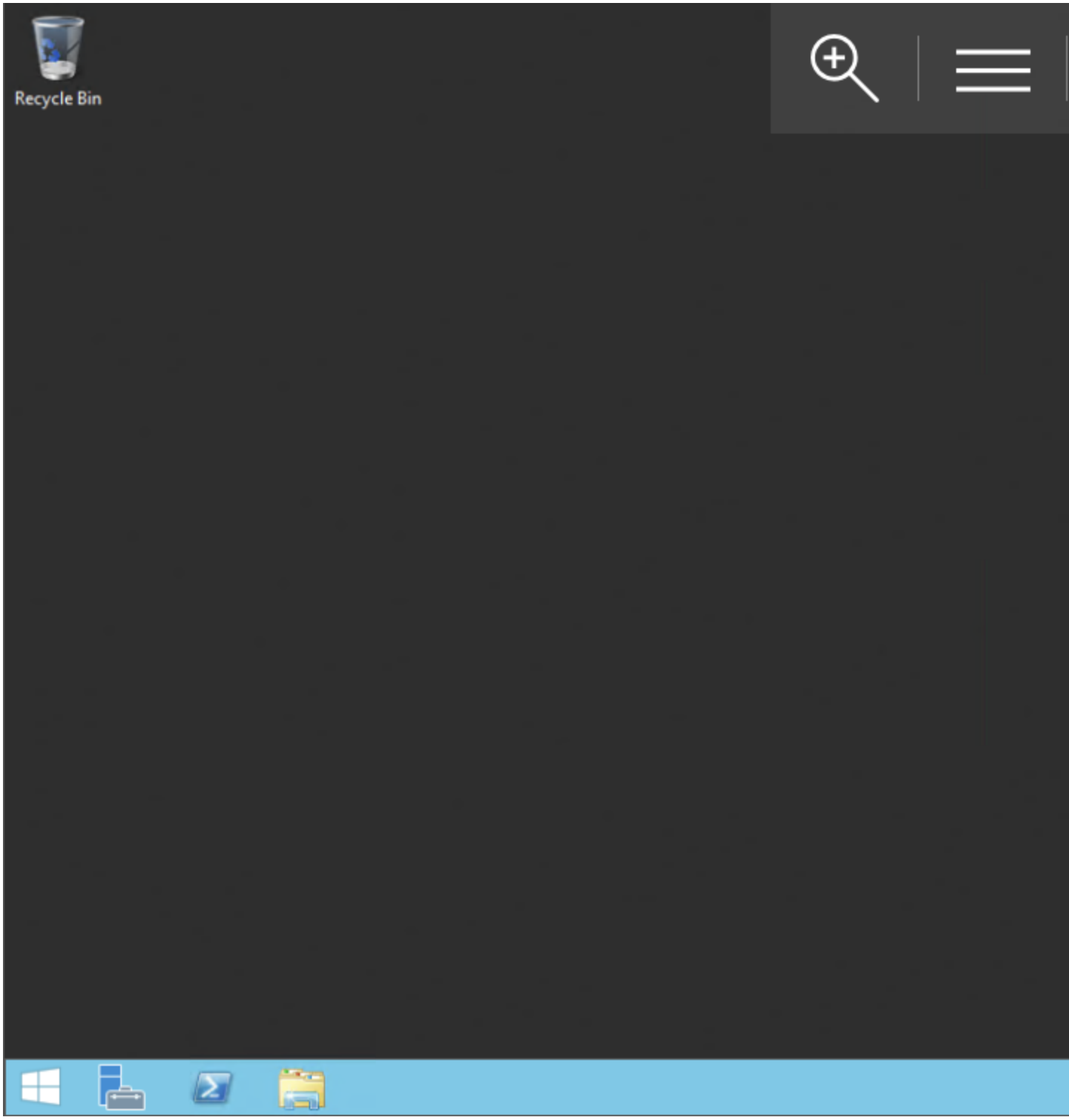
Figure 1-17 CONNECT



You have logged in to the Windows HECS.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-18 Successful login



 Copyright © Huawei Technologies Co., Ltd.

1.7 Logging In to a Windows HECS from a Mac

Scenarios

This section describes how to use a remote login tool to log in to a Windows HECS from a Mac. In this section, the remote login tool Microsoft Remote Desktop for Mac and the HECS running Windows Server 2012 R2 Data Center 64bit are used as an example.

Prerequisites

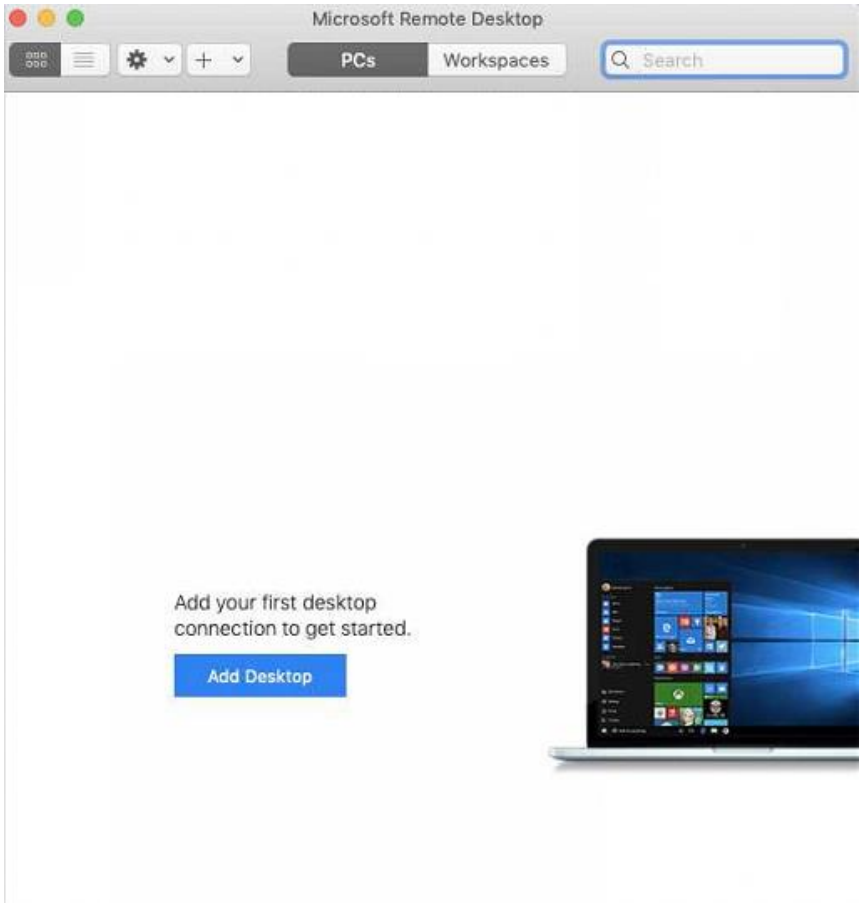
- The target HECS is running.
- You have obtained the username and password for logging in to the Windows HECS. If you have forgotten the password, reset it on the management console.
- The HECS has an EIP bound.
- Access to port 3389 is allowed in the inbound direction of the security group to which the HECS belongs.
- The remote access tool supported by Mac, such as Microsoft Remote Desktop for Mac has been installed. For details, see Download Microsoft Remote Desktop for Mac.

Procedure

1. Start Microsoft Remote Desktop.
2. Click **Add Desktop**.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-19 Add Desktop



3. On the **Add PC** page, set login information.
   - **PC name**: Enter the EIP bound to the target Windows HECS.
   - **User account**: Select **Add user account** from the drop-down list.

     The **Add user account** dialog box is displayed.

     Enter username **administrator** and password for logging in to the Windows HECS and click **Add**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-20 Setting the login information

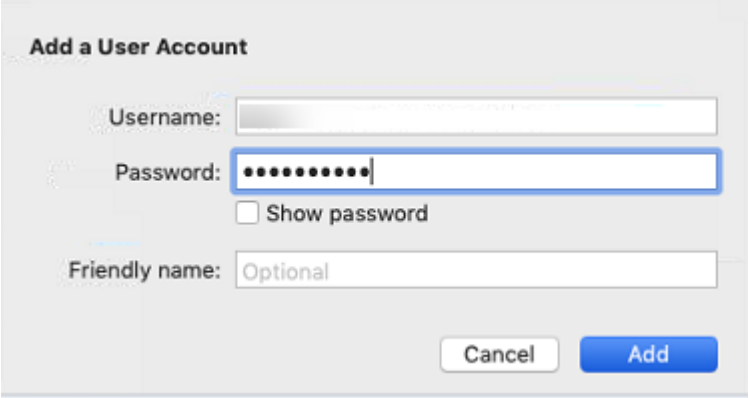
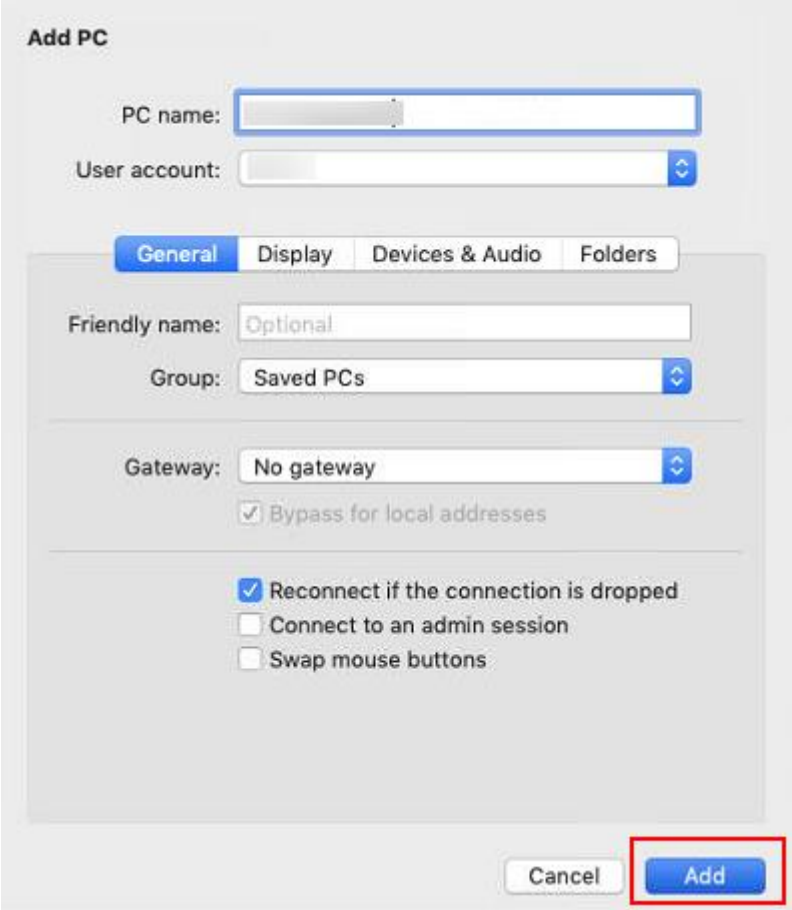


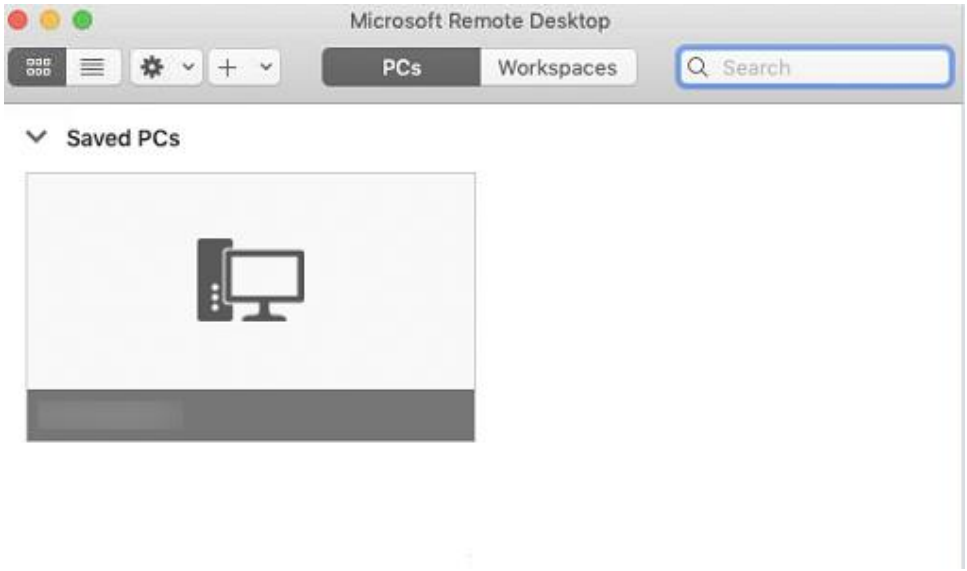
Figure 1-21 Saving the settings



4. On the **Remote Desktop** page, double-click the icon of the target Windows HECS.

 Copyright © Huawei Technologies Co., Ltd.

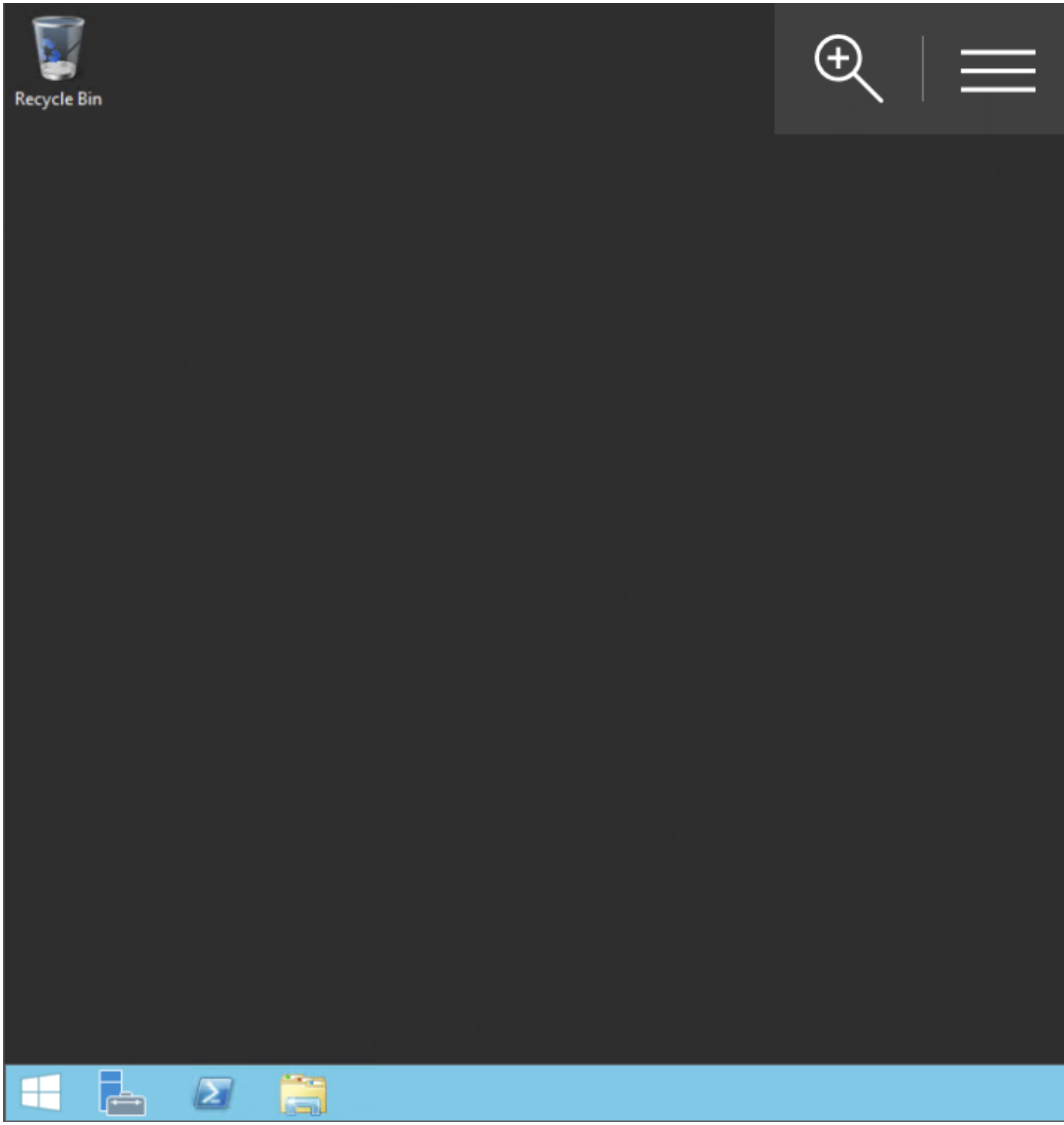
Figure 1-22 Logging in to the Windows HECS



5. Confirm the information and click **CONNECT**.
   You have logged in to the Windows HECS.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-23 Successful login



 Copyright © Huawei Technologies Co., Ltd.

2 Logging In to a Linux HECS

2.1 Login Overview

Notes and Constraints

- Only a running HECS can be logged in.
- The username for logging in to a Linux HECS is **root**.
- If you log in to an HECS for the first time or want to reset a password, locate the row containing the target HECS and click **Reset Password** in the **Operation** column.

Login Modes

Select a login method and log in to the HECS.

Table 2-1 Linux HECS login modes

HECS OS	Local OS	Connection Method	Remarks
Linux	Windows	Use a remote connection tool, such as PuTTY or XShell, to log in to the HECS. Download PuTTY. 2.3 Logging In to a Linux HECS Using an SSH Password	The HECS has an EIP bound. (If you communicate with an HECS through the private network, for example, through VPN or Direct Connect, the HECS does not require an EIP.)
	Mobile terminal	Use an SSH client tool, such as Termius or JuiceSSH, to log in to the HECS. 2.4 Logging In to a Linux HECS from a Mobile Terminal	
	Windows	Use the remote login function available on the management console. For details, see 2.2 Login Using VNC.	No EIP is required.

Copyright © Huawei Technologies Co., Ltd.

Helpful Links

- Can I Retrieve My Remote Login Password?
- Why Can't Log In to My Linux HECS?

2.2 Login Using VNC

Scenarios

This section describes how to use VNC provided on the management console to log in to an HECS.

For instructions about how to copy and paste data on VNC pages after the HECS login, see Follow-up Procedure.

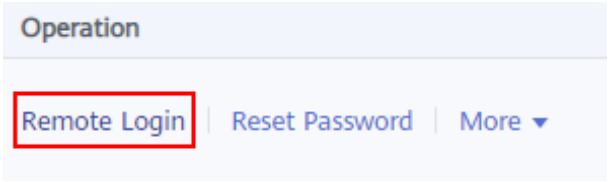
Prerequisites

The HECS has an EIP bound.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. In the **Operation** column of the target HECS, click **Remote Login**.

   Figure 2-1 Remote Login

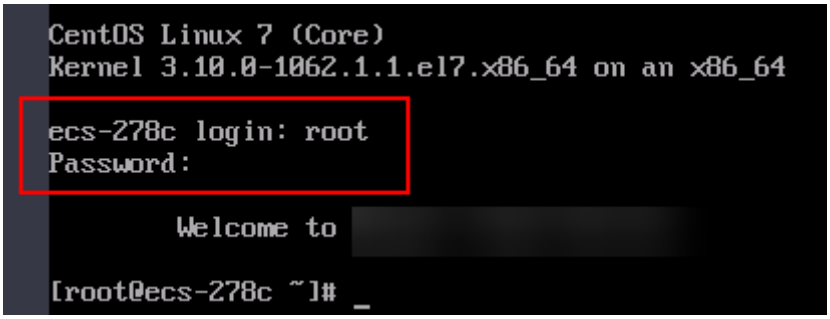
5. In the **Log In to a Linux HECS** dialog box, click **Log In** in **VNC-based Login**.
6. (Optional) When the system displays "Press CTRL+ALT+DELETE to log on", click **Ctrl+Alt+Del** in the upper part of the remote login page to log in to the HECS.

   NOTE

   Do not press **CTRL+ALT+DELETE** on the physical keyboard because this operation does not take effect.
7. Enter the HECS password as prompted.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Username (root as an example) and password

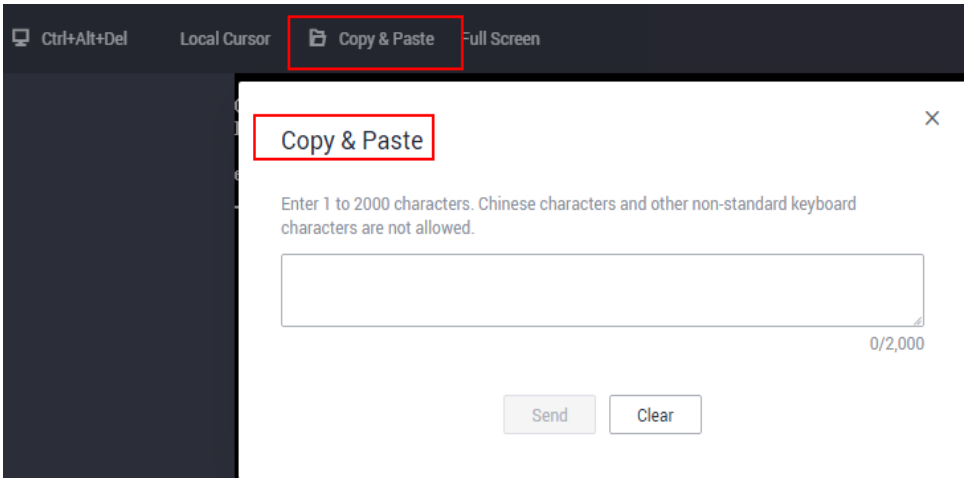


Follow-up Procedure

Local commands can be copied to an HECS. To do so, perform the following operations:

1. Log in to the HECS using VNC.
2. Click **Input Commands** in the upper right corner of the page.

Figure 2-3 Copy & Paste



3. Press **Ctrl+C** to copy data from the local computer.
4. Press **Ctrl+V** to paste the local data to the **Copy Commands** window.
5. Click **Send**.

   Send the copied data to the CLI.

NOTE

There is a low probability that data will be lost when you use the command input function on the VNC page of a GUI-based Linux HECS. This is because the number of HECS vCPUs fails to meet GUI requirements. In this case, you are advised to send a maximum of 5 characters at a time or switch from GUI to CLI (also called text interface), and then use the command input function.

 Copyright © Huawei Technologies Co., Ltd.

2.3 Logging In to a Linux HECS Using an SSH Password

Scenarios

This section describes how to remotely log in to a Linux HECS using an SSH password from Windows and Linux.

Prerequisites

- The target HECS is running.
- The HECS has an EIP bound.
- Access to port 22 is allowed in the inbound direction of the security group to which the HECS belongs. For details, see 8.4 Configuring Security Group Rules.
- The network connection between the login tool (PuTTY) and the target HECS is normal. For example, the default port 22 is not blocked by a firewall.

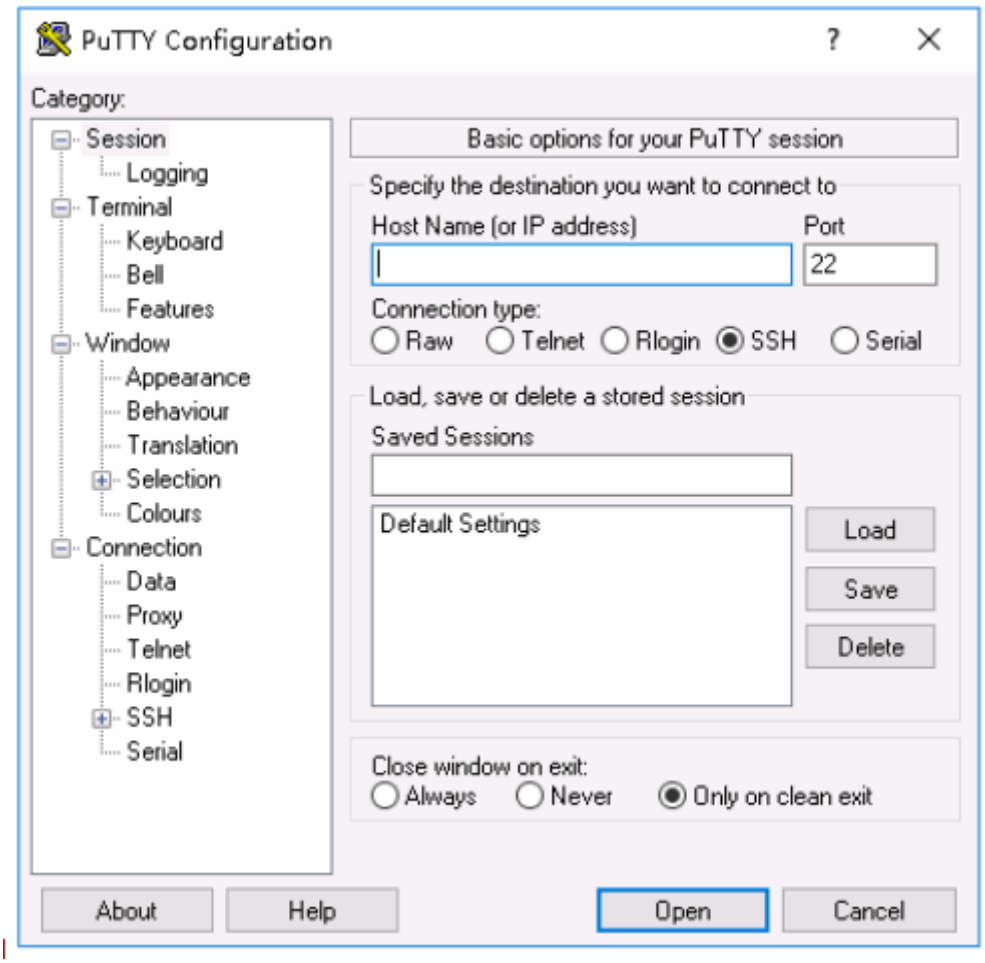
Logging In to the Linux HECS from Local Windows

To log in to the Linux HECS from local Windows, perform the operations described in this section.

The following example shows how to access a Linux HECS using an SSH password.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-4 Accessing a Linux HECS using an SSH password

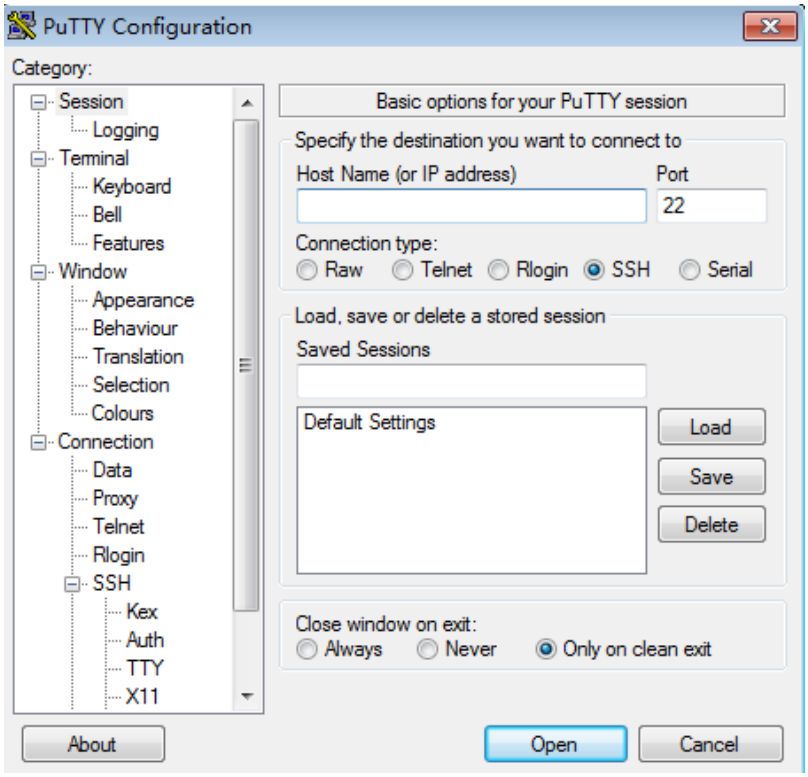


The following operations use PuTTY as an example for logging in to the HECS.

1. Visit the following website and download PuTTY and PuTTYgen:
   https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Run PuTTY.
3. Click **Session**.
   a. **Host Name (or IP address)**: EIP bound to the HECS
   b. **Port**: **22**
   c. **Connection type**: **SSH**
   d. **Saved Sessions**: task name, which can be clicked for remote connection when you use PuTTY the next time

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-5 Session



4. Click **Window**. Then, select **UTF-8** for **Received data assumed to be in which character set:** in **Translation**.
5. Click **Open**.

   If you log in to the HECS for the first time, PuTTY displays a security warning dialog box, asking you whether to accept the HECS security certificate. Click **Yes** to save the certificate to your local registry.
6. After the SSH connection to the HECS is set up, enter the username and password as prompted to log in to the HECS.

NOTE

The username and password for the first login to the HECS created using a public image (including CoreOS) are as follows:

- Username: **root**
- Password: the one you set when you purchased the HECS

Logging In to the Linux HECS from Local Linux

To log in to the Linux HECS from local Linux, run the following command:

ssh *EIP bound to the HECS*

 Copyright © Huawei Technologies Co., Ltd.

2.4 Logging In to a Linux HECS from a Mobile Terminal

Scenarios

This section describes how to access a Linux HECS from a mobile terminal.

- For instructions on how to log in to a Linux HECS from an iOS terminal through iTerminal-SSH Telnet, see Logging In to a Linux ECS from an iOS Terminal.
- For instructions on how to log in to a Linux HECS from an Android terminal through JuiceSSH, see Logging In to a Linux HECS from an Android Terminal.

Prerequisites

- The target HECS is running.
- You have obtained the username and password for logging in to the Linux HECS. If you have forgotten the password, reset it by following the instructions provided in 6.1 Resetting an HECS Password on the Management Console.
- The HECS has had an EIP bound.
- Access to port 22 is allowed in the inbound direction of the security group to which the HECS belongs.

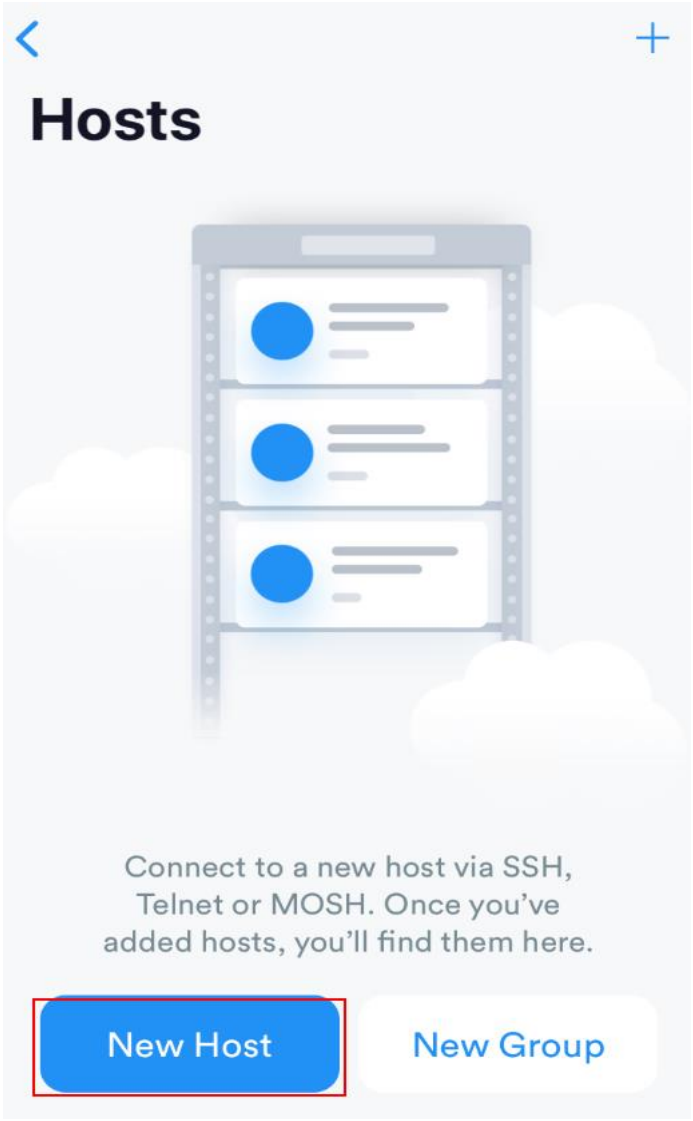
Logging In to a Linux ECS from an iOS Terminal

Before performing the operation, make sure that you have installed an SSH client tool, taking Termius as an example, on the iOS terminal. In this example, the Linux ECS runs CentOS 7.6, and it is authenticated using a username and password.

1. Start Termius and tap **New Host**.

Copyright © Huawei Technologies Co., Ltd.

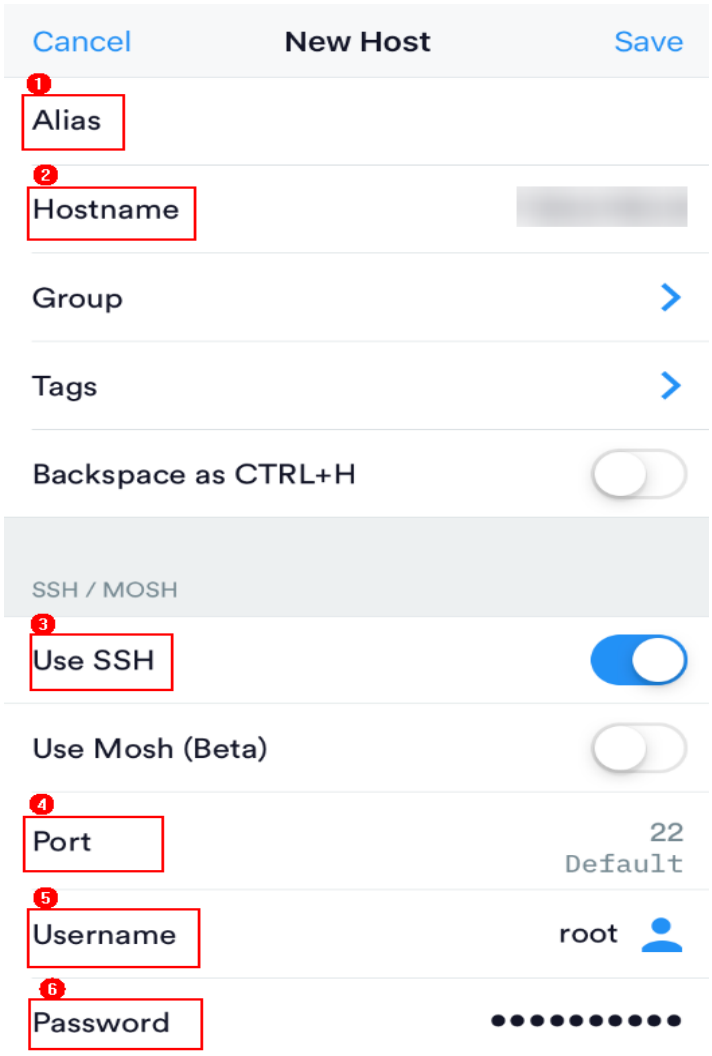
Figure 2-6 New Host



2. On the **New Host** page, set the following parameters:
   - **Alias**: Enter the hostname. In this example, set this parameter to **ecs01**.
   - **Hostname**: Enter the EIP bound to the target ECS.
   - **Use SSH**: Enable it.
   - **Host**: Enter the EIP bound to the target ECS.
   - **Port**: Enter port number **22**.
   - **Username**: Enter **root**.
   - **Password**: Enter the login password.

 Copyright © Huawei Technologies Co., Ltd.

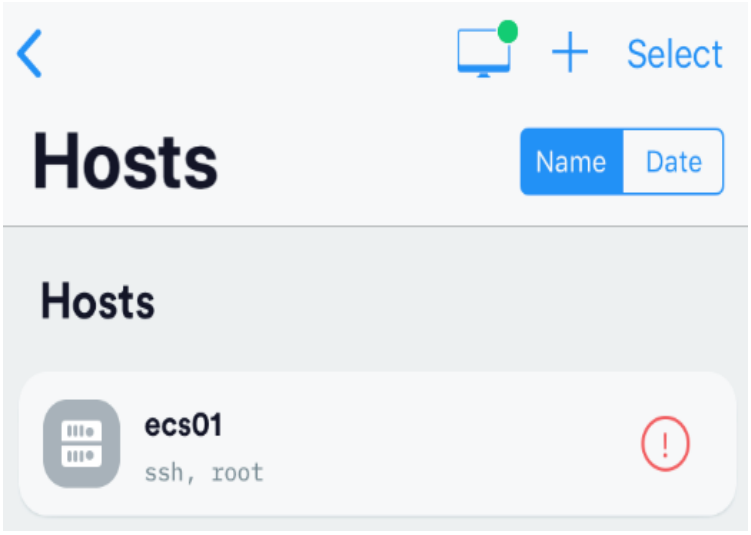
Figure 2-7 Setting parameters



3. Tap **Save** in the upper right corner of the page to save the login settings. On the **Hosts** page, tap the name of the connection.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-8 Login information



If the following page is displayed, you have connected to the Linux ECS.

Figure 2-9 Connected



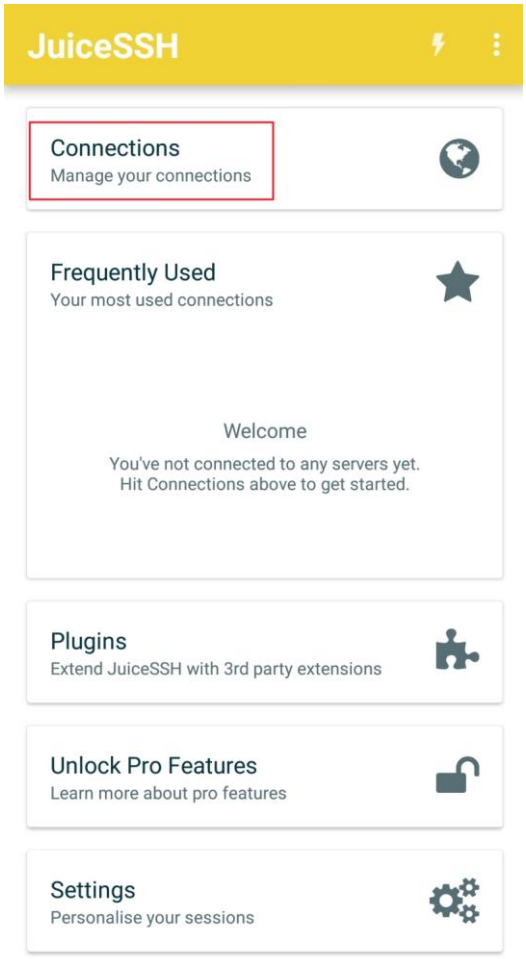
Logging In to a Linux HECS from an Android Terminal

Before performing the operation, ensure that you have installed JuiceSSH on the Android terminal. In this example, the Linux HECS runs CentOS 7.6, and it is authenticated using a username and password.

1. Start JuiceSSH and tap **Connections**.

Copyright © Huawei Technologies Co., Ltd.

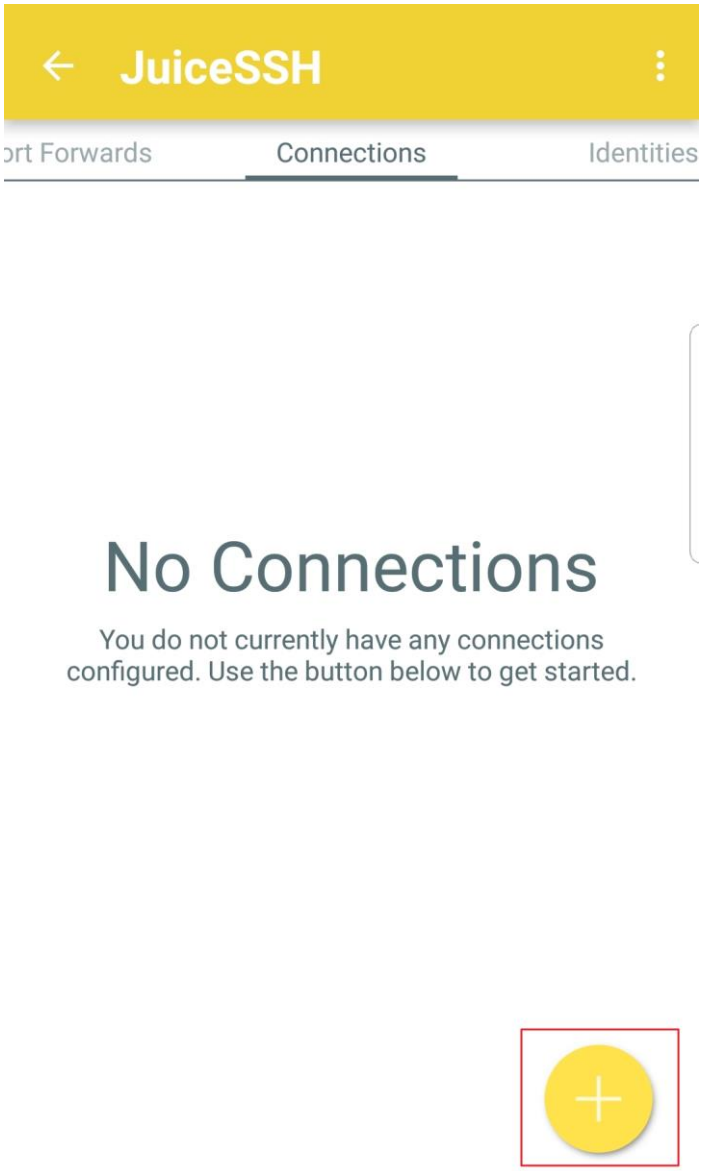
Figure 2-10 Starting JuiceSSH



2. On the **Connections** page, tap .

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-11 Connections

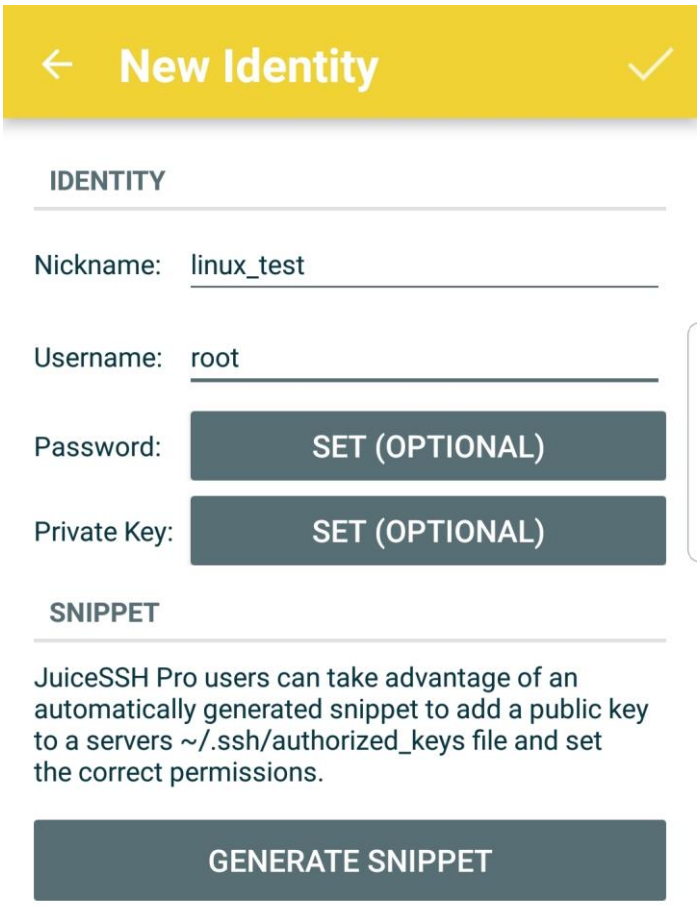


3. On the **New Connection** page, add basic and advanced settings and save the settings. The parameters are as follows:
   - **Nickname**: Set the name of the login session. In this example, set this parameter to **linux_test**.
   - **Type**: Retain the default value **SSH**.
   - **Address**: Enter the EIP bound to the target Linux HECS.
   - Perform the following operations to set **Identity**:
     i. Tap **Identity** and choose **New** from the drop-down list.
     ii. On the **New Identity** page, set the following parameters and tap .

 Copyright © Huawei Technologies Co., Ltd.

- **Nickname**: Set an identity name as required to facilitate subsequent management. This parameter is optional. In this example, set it to **linux_test**.
- **Username**: Enter **root**.
- **Password**: Tap **SET (OPTIONAL)**, enter the login password, and tap **OK**.

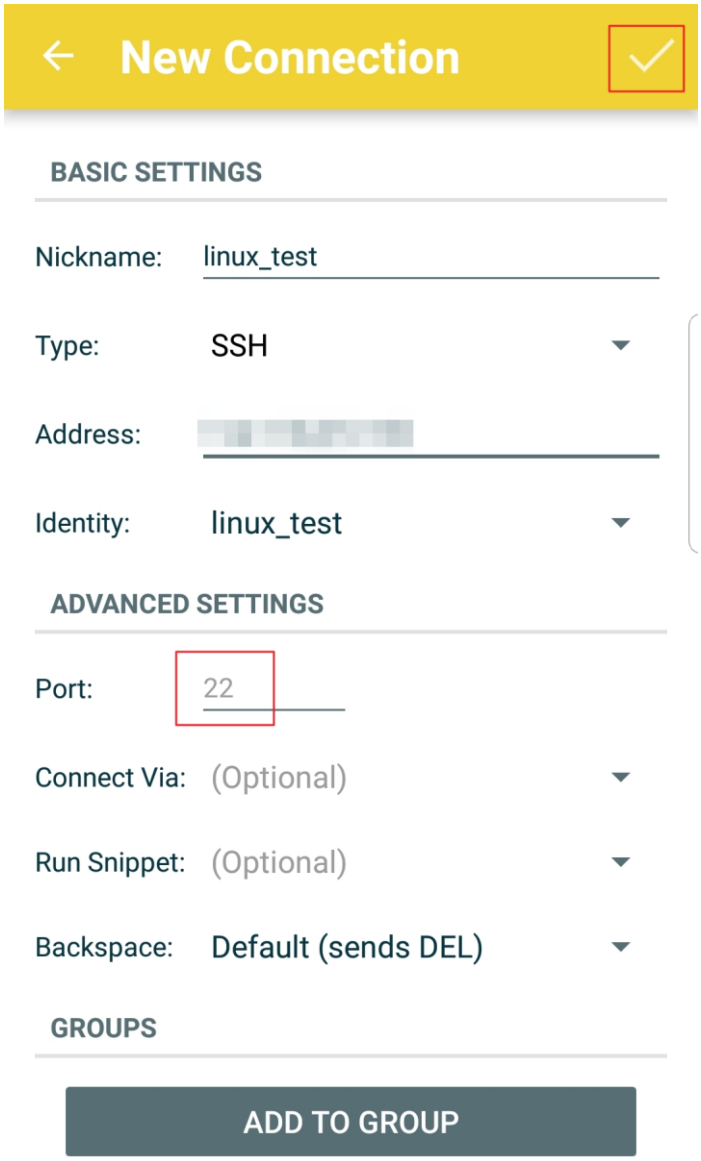
Figure 2-12 New Identity



- **Port**: Enter port number **22**.

 Copyright © Huawei Technologies Co., Ltd.

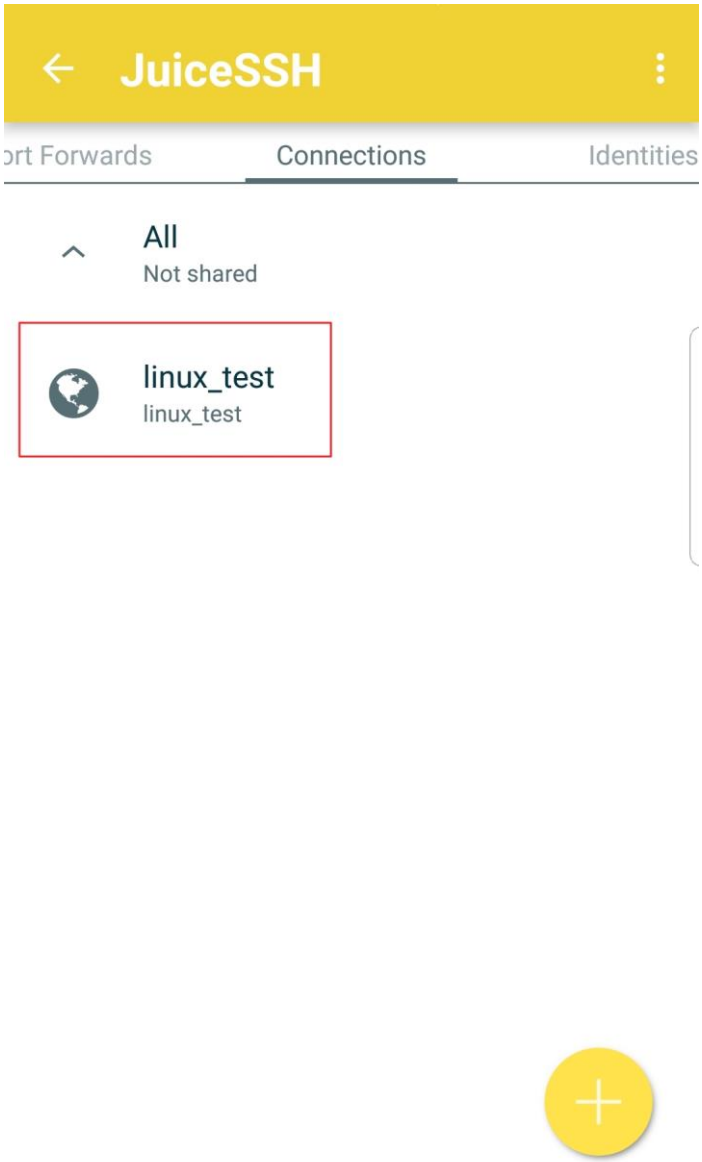
Figure 2-13 Port number



4. On the **Connections** page, tap the created connection.

 Copyright © Huawei Technologies Co., Ltd.

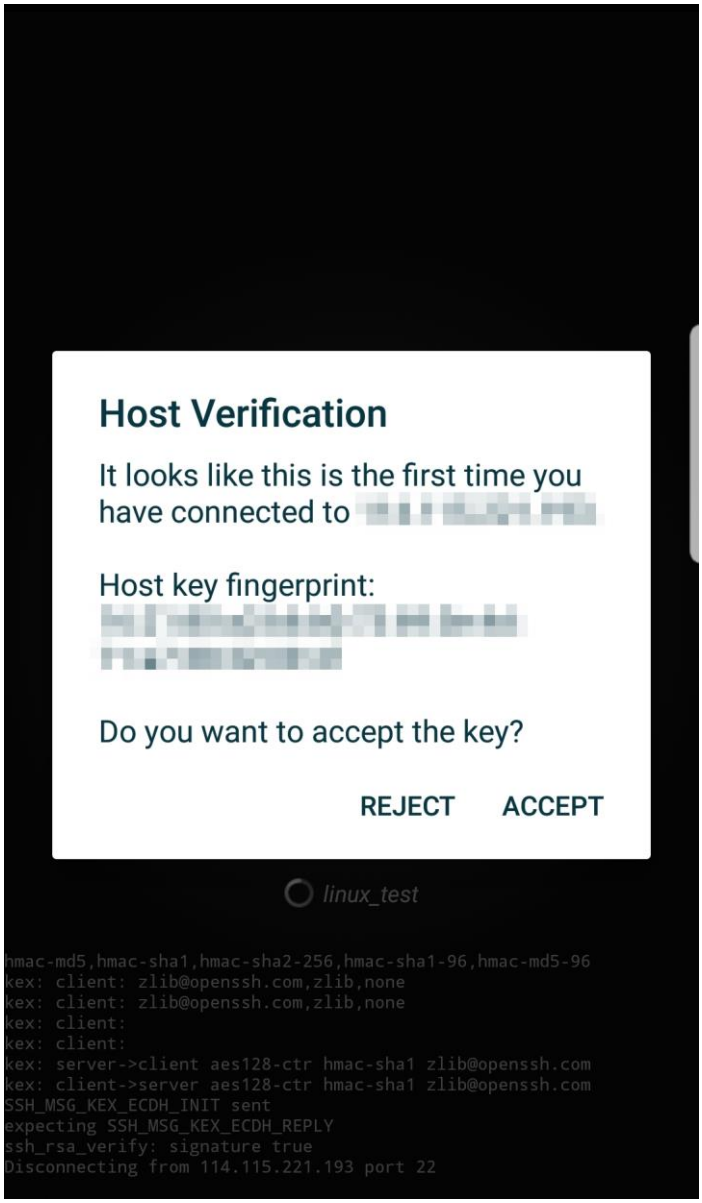
Figure 2-14 Connection



5. Confirm the information that is displayed and tap **ACCEPT**.

 Copyright © Huawei Technologies Co., Ltd.

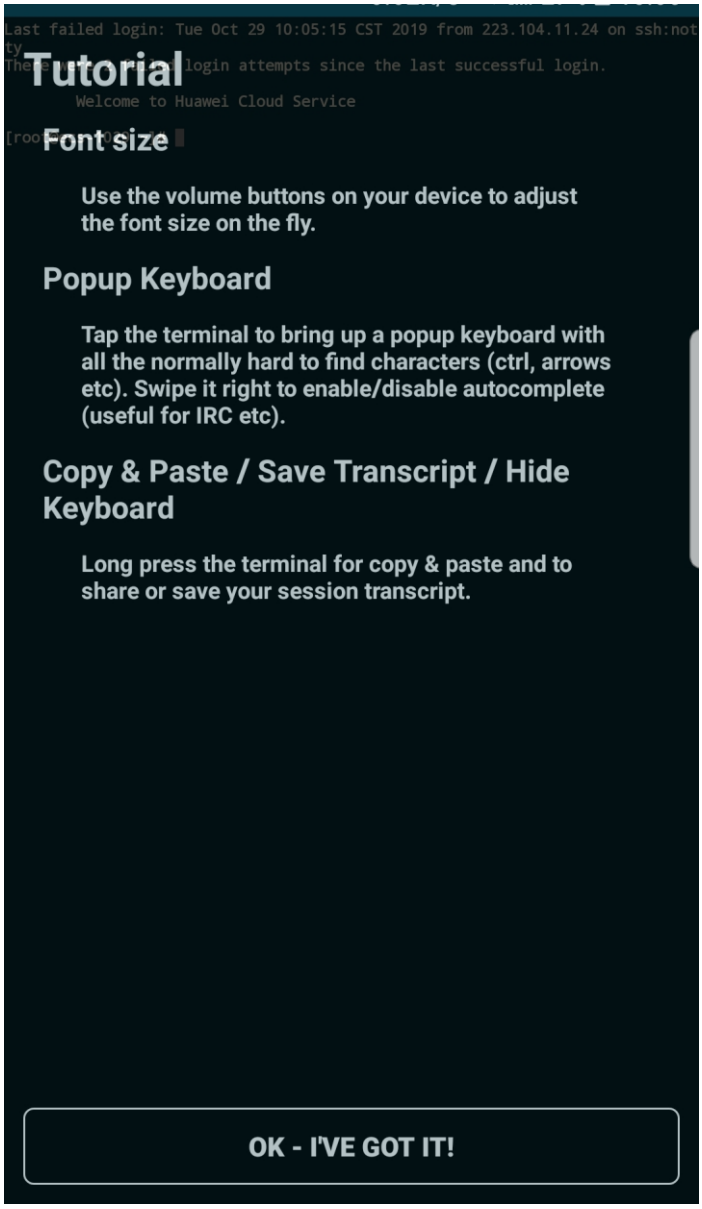
Figure 2-15 Confirming the information



6. (Optional) When you log in to the HECS for the first time, JuiceSSH displays a tutorial for you, which includes setting the font size and popping up the keyboard. Tap **OK - I'VE GOT IT**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-16 Tutorial



You have logged in to the Linux HECS.

Figure 2-17 Successful login



 Copyright © Huawei Technologies Co., Ltd.

3 Managing HECSs

3.1 Viewing Details About an HECS

Scenarios

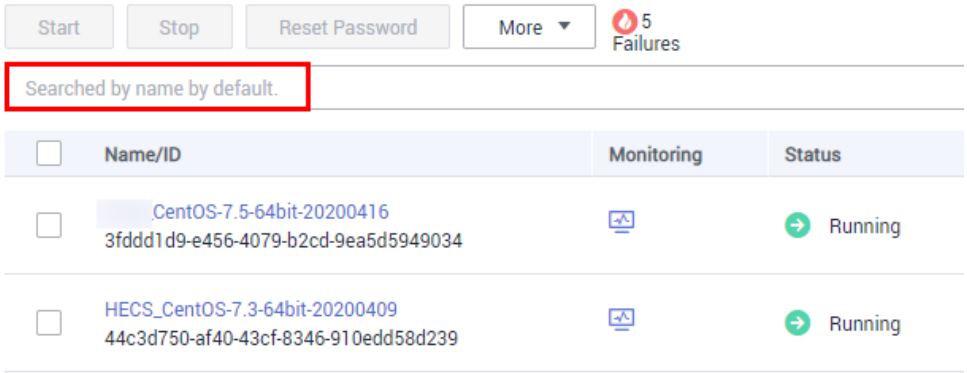
After purchasing HECSs, you can view and manage them on the management console. This section describes how to view detailed configuration of an HECS, including its name, image, system disk, data disks, security group, and EIP.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.

   The **Hyper Elastic Cloud Server** page is displayed. On this page, you can view your HECSs and their basic information, such as their private IP addresses.
4. In the search box above the upper right corner of the HECS list, enter the HECS name, IP address, or ID, and click for search.

   Figure 3-1 Searching for an HECS



5. Click the name of the target HECS.

 Copyright © Huawei Technologies Co., Ltd.

The page providing details about the HECS is displayed.

6. View details about the HECS.

   You can click your desired tab to view HECS information, such as basic HECS information or monitoring results, change a security group, and add disks or NICs.

3.2 Changing an HECS Name

Scenarios

The name of a created HECS can be changed to meet your service requirements.

Multiple HECS names can be changed in a batch. The HECS names stay the same after the batch change.

Procedure for a Single HECS

1. Log in to management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Halo ECS**.
4. Click the name of the target HECS.
5. On the page providing details about the HECS, click  following the HECS name. Then, change the name as prompted.

   Allow duplicate HECS names: allows HECS names to be duplicate. If **Allow duplicate HECS names** is not selected and the target name is the same as an existing HECS name, the system displays a message indicating that the name is already in use and you need to change it.
6. Click **OK**.

Procedure for Batch Operations

1. Log in to management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Halo ECS**.
4. Select the target HECSs.
5. Click **More** in the upper part of the HECS list and select **Change HECS Name** from the drop-down list.
6. Enter the new name.
7. Click **OK**.

   If you change HECS names in a batch, the new HECS names are the same, for example, all are **lightserver-test**.

 Copyright © Huawei Technologies Co., Ltd.

3.3 Reinstalling the OS

Scenarios

If the OS of an HECS fails to start or requires optimization, reinstall the OS.

Prerequisites

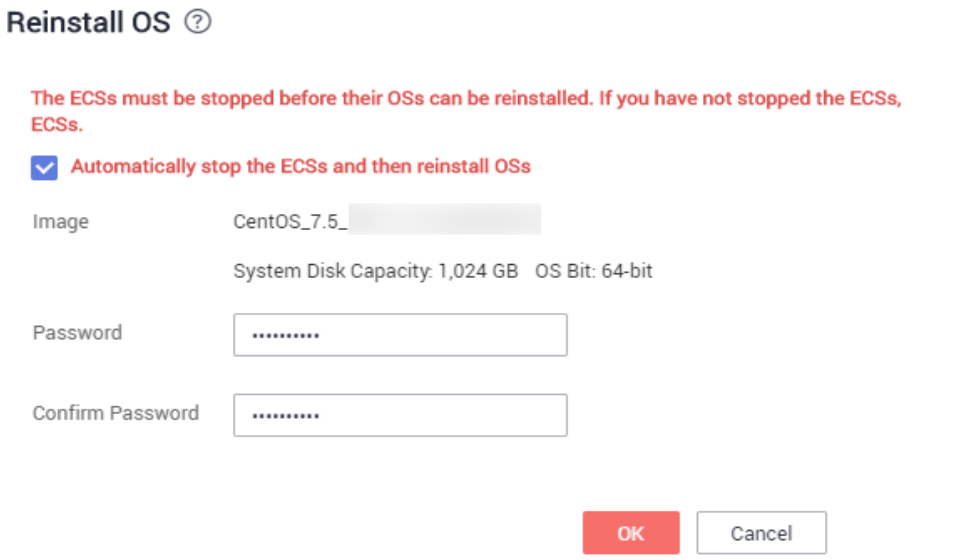
- If the HECS is not in **Stopped** state, stop the HECS before proceeding with reinstallation. Before reinstalling the OS, stop the HECS or select **Automatically stop the HECSs and then reinstall OSs**.
- The target HECS has a system disk attached.
- Desired data has been backed up. (Reinstalling the OS clears the data in all partitions of the EVS system disk, including the system partition.)

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. Locate the row containing the target HECS. Click **More** in the **Operation** column and select **Reinstall OS**.

   If the HECS is not in **Stopped** state, stop the HECS before proceeding with reinstallation. Before reinstalling the OS, stop the HECS or select **Automatically stop the HECSs and then reinstall OSs**.
5. Set a login password.

   Figure 3-2 Reinstall OS

6. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

7. On the **HECS OS Reinstallation** page, confirm the specifications, read and select the service agreement, and click **Submit**.

   After the request is submitted, the HECS status changes to **Reinstalling**. The reinstallation is complete when the HECS status changes to **Running**.

NOTE

A temporary HECS is created during the reinstallation process. After reinstallation, this HECS will automatically be deleted. Do not perform any operation on the temporary HECS during the reinstallation process.

Follow-up Procedure

If the reinstallation is unsuccessful, perform steps 3 to 7 again to retry reinstalling the OS.

If the second reinstallation attempt is unsuccessful, contact customer service for manual recovery at the backend.

3.4 Changing an OS

Scenarios

Changing an HECS OS will change the system disk attached to the HECS. After the changing, the original system disk will be deleted.

If the OS running on an HECS fails to meet service requirements, for example, a higher OS version, you can change the HECS OS.

Constraints

- The HECSs created using a Marketplace image do not support changing of their OSs.
- Only system disk images or full-HECS images can be used to change OSs with private images.
- The EVS disk quota must be greater than 0.
- Switching between the HECSs in BIOS boot mode and in UEFI boot mode is not allowed.

Notes

- After the OS is changed, the original OS is not retained and the original system disk is deleted.
- Desired data has been backed up. (Changing the OS clears the data in all partitions of the system disk, including the system partition.)
- After the OS is changed, your service running environment must be deployed in the new OS again.
- After the OS is changed, the HECS will be automatically started.
- After the OS is changed, the system disk type of the HECS cannot be changed.
- After the OS is changed, the IP and MAC addresses of the HECS remain unchanged.
- After the OS is changed, customized configurations, such as DNS and hostname of the original OS will be reset and require reconfiguration.

 Copyright © Huawei Technologies Co., Ltd.

- It takes about 10-20 minutes to change the OS. During this process, the HECS is in **Changing OS** state.

Billing Rules

- You are not billed for changing an OS. After the OS of an HECS is changed, it will be billed based on the new configuration (system disk and specifications).
- After the OS of an HECS is changed, its fees may be different because the system disk capacity specified by the image of the changed OS may increase. For details, see Product Pricing Details.

Notes on Cross-OS Changing

Cross-OS changing indicates that the OS is changed between Windows and Linux.

- To change from Windows to Linux, install an NTFS partition tool, such as NTFS-3G for data reading and writing on the Windows HECS.
- To change from Linux to Windows, install software, such as Ext2Read and Ext2Fsd to identify ext3 or ext4.

NOTE

You are not advised to change from Linux to Windows. If there are LVM partitions on the Linux HECS, these partitions may not be identified after the OS is changed to Windows.

Prerequisites

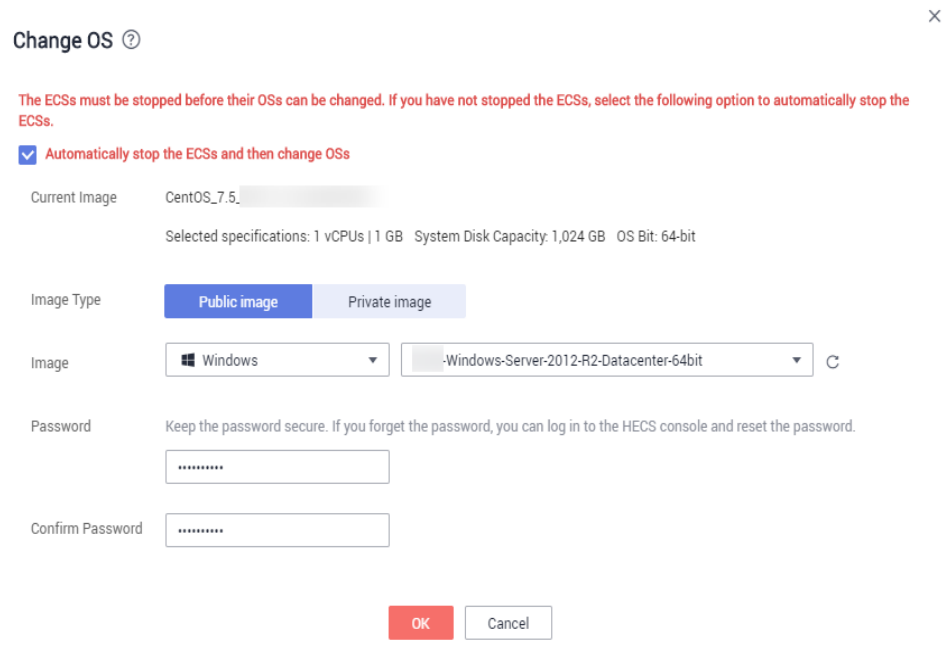
- Before changing the OS, stop the HECS or select **Automatically stop the HECSs and then change OSs**.
- The target HECS has a system disk attached.
- Desired data has been backed up. (Changing the OS clears the data in all partitions of the system disk, including the system partition.)
- If a private image is required for changing the HECS OS, create the desired private image by following the instructions provided in *Image Management Service User Guide*.
  - If the image of a specified HECS is required, make sure that a private image has been created using this HECS.
  - If a local image file is required, make sure that the image file has been imported to the cloud platform and registered as a private image.
  - If a private image from another region is required, make sure that the image has been copied to the target region.
  - If a private image from another user account is required, make sure that the image has been shared with you.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. Locate the row containing the target HECS. Click **More** in the **Operation** column and select **Change OS**.
4. Select the image type, OS and version to change to.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Changing an OS



5. Set a login password.
   - If you use a public image to change the OS, you can reset the password after changing.
   - If you use a private image to change the OS, you can use the image password. Ensure that a password has been set for the selected private image.
6. Click **Change OS**.

   Before changing the OS, stop the HECS or select **Automatically stop the HECSs and then change OSs**.
7. Set a login password.
8. Click **OK**.

   If the system displays a message indicating insufficient system disk capacity, the possible cause is that the system disk capacity is less than the size of the image to change to. In this case, expand the system disk capacity and then change OSs.

   For instructions about how to expand the system disk capacity, see Expanding an EVS Disk.
9. On the **Change HECS OS** page, confirm the specifications, read and select the service agreement, and click **Submit**.

   After the application is submitted, the HECS status becomes **Changing OS**. The OS change is complete when the HECS status becomes **Running**.

NOTE

A temporary HECS is created during the OS changing process. When the process is complete, this HECS is automatically deleted. Do not perform any operation on the temporary HECS during the OS changing process.

Follow-up Procedure

If the OS change is unsuccessful, perform steps 2 to 9 again to retry changing the OS.

 Copyright © Huawei Technologies Co., Ltd.

If the second OS change attempt is unsuccessful, contact customer service for manual recovery at the backend.

3.5 Changing the Time Zone for an HECS

Scenarios

The time zone for an HECS is the one you selected when creating the image used to create the HECS. This section describes how to change the time zone for an HECS to your local one or to another time zone in your network.

After you log in to your HECS, if you find that the time on the HECS is different from the local time, change the time zone for the HECS so that the time on the HECS is the same as the local time.

The default time zone for HECSs in all regions is GMT +08:00. Perform the operations described in this section to change the time zone if necessary.

For Linux

The process of changing the time zone for a Linux HECS depends on the OS. In this section, the CentOS 6.x 64bit OS is used to demonstrate how to change the time zone for a Linux HECS.

1. Log in to the HECS.
2. Run the following command to switch to user **root**:

   su - root
3. Run the following command to obtain the time zones supported by the HECS:

   ls /usr/share/zoneinfo/

   In the terminal display, the **/user/share/zoneinfo** directory contains a hierarchy of time zone data files. Use the directory structure to obtain your desired time zone file.

   The directory structure shown in **/user/share/zoneinfo** includes both time zones and directories. The directories contain time zone files for specific cities. Locate the time zone for the city in which the HECS is located.

   For example:

   - If you are to use the time zone for Shanghai, China, run the **ls /usr/share/zoneinfo/Asia** command to obtain the directory **/usr/share/zoneinfo/Asia/Shanghai**.
   - If you are to use the time zone for Paris, France, run the **ls /usr/share/zoneinfo/Europe** command to obtain the directory **/usr/share/zoneinfo/Europe/Paris**.
4. Set the target time zone.
   a. Run the following command to open the **/etc/sysconfig/clock** file:

      vim /etc/sysconfig/clock

   b. Locate the **ZONE** entry and change its value to the name of the desired time zone file.

      For example:

      - If the target time zone is for Shanghai, China, change the **ZONE** entry value as follows:

 Copyright © Huawei Technologies Co., Ltd.

ZONE="Asia/Shanghai"

- If the target time zone is for Paris, France, change the **ZONE** entry value as follows:

  ZONE="Europe/Paris"

5. Press **Esc**. Then, run the following command to save and exit the **/etc/sysconfig/clock** file:

   :wq

6. Run the following command to check whether the **/etc/localtime** file is available on the HECS:

   ls /etc/localtime

   - If the file is available, go to step 7.
   - If the file is not available, go to step 8.

7. Run the following command to delete the existing **/etc/localtime** file:

   rm /etc/localtime

8. Run the following command to create a symbolic link between **/etc/localtime** and your time zone file so that the HECS can find this time zone file when it references the local time:

   ln -sf /usr/share/zoneinfo/*Asia/Shanghai* /etc/localtime

9. Run the following command to restart the HECS so that all services and applications running on the HECS use the new time zone:

   reboot

10. Log in to the HECS again and run the following command as user **root** to check whether the time zone has been changed:

    ls -lh /etc/localtime

    The following information is displayed:

```
# ls -lh /etc/localtime
lrwxrwxrwx 1 root root 33 Nov 27 11:01 /etc/localtime ->
/usr/share/zoneinfo/Asia/Shanghai
```

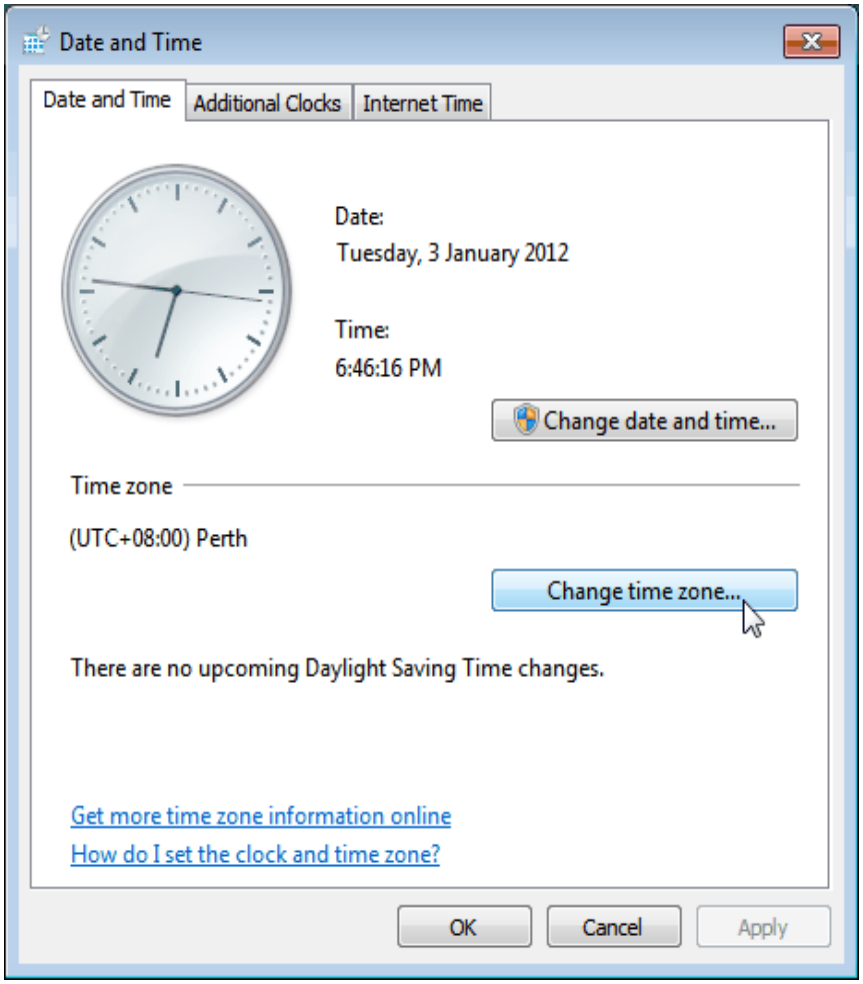
For Windows

1. Log in to the HECS.
2. Click the time display on the far right side of the task bar located at the bottom of your screen. In the dialog box that is displayed, click **Change date and time settings**.

   The **Date and Time** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Date and Time



3. Click **Change time zone**.

   The **Time Zone Settings** page is displayed.

4. In the **Set the time zone** pane, choose the target time zone from the **Time zone** drop-down list.
5. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

4 Modifying HECS Specifications

Scenarios

You can modify the HECS specifications, including vCPUs and memory, if they do not meet service requirements. Certain HECSs allow you to change their types.

Notes

- When modifying the specifications of an HECS, you are not allowed to select sold-out vCPU and memory resources.
- If HECS specifications are downgraded, the HECS performance is deteriorated.
- When the disk status is **Expanding**, you are not allowed to modify the specifications of the HECS where the disk is attached.
- Before modifying the specifications of a Windows HECS, modify the SAN policy by following the instructions provided in What Should I Do If a Disk Is Offline? to prevent offline disks after the specifications are modified.
- Before modifying the specifications, stop the HECS or select **Automatically stop the HECSs and then modify specifications**.

Billing Description

Modifying specifications will lead to price changes. For details, see Pricing of a Changed Specification.

Preparations

After HECS specifications are modified, NIC flapping may occur. To prevent NIC flapping from affecting dependency configurations, perform the following operations before modifying the specifications:

- Linux

  Run the following commands on the HECS to delete the files with **persistent** and **net** included in their names in the network rule directory:

  rm -fr /etc/udev/rules.d/*net*persistent*.rules

  rm -fr /etc/udev/rules.d/*persistent*net*.rules
- Windows

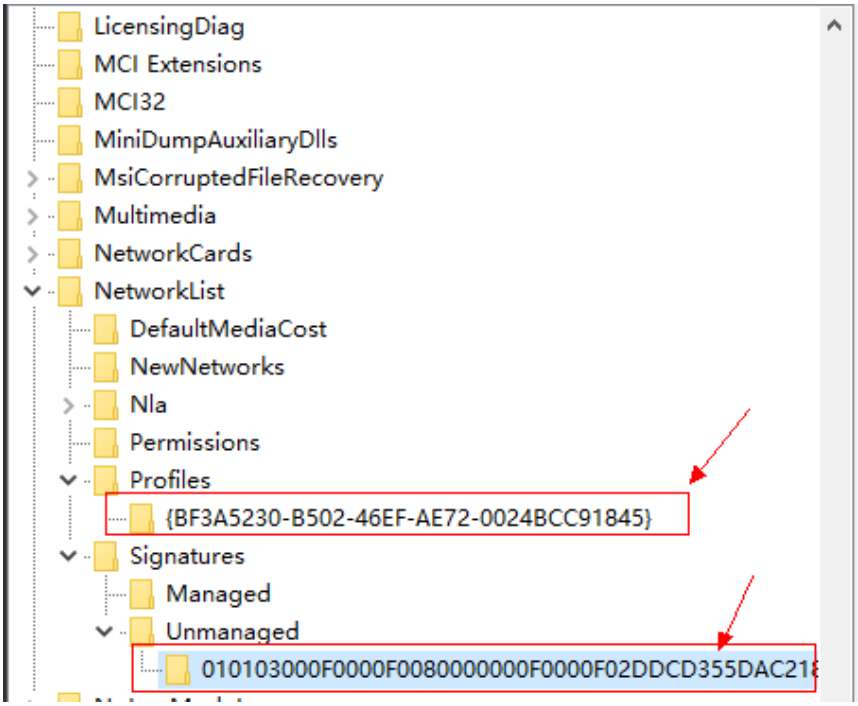
  Delete the following directories in the registry on the HECS:

 Copyright © Huawei Technologies Co., Ltd.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

Figure 4-1 Registry



Step 1: Modify Specifications

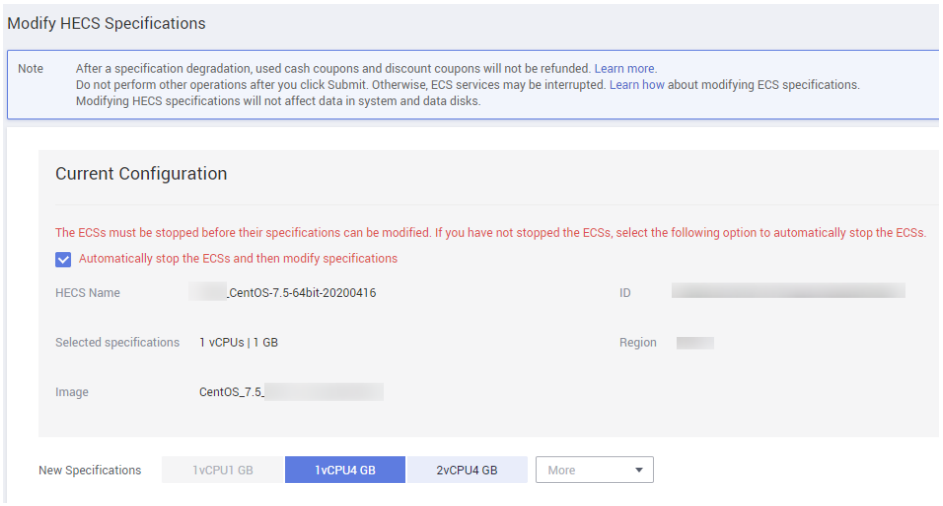
1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. Locate the row that contains the target HECS, click **More** in the **Operation** column, and select **Modify Specifications**.

   The **Modify HECS Specifications** page is displayed.
4. Set the new vCPUs and memory as prompted.

   Before modifying the specifications, stop the HECS or select **Automatically stop the HECSs and then modify specifications**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-2 Modifying specifications



5. click **Next**.
6. Confirm the modified configuration. Read and select the service agreement, and then click **Submit**.
7. Check whether the specifications have been modified.

   After modifying the specifications, you can check whether the specifications have been modified in **Failures**.

   a. Check whether **Failures** is displayed on the management console.
      - If yes, go to step 7.b.
      - If no, the specifications have been modified.

   b. Click **Failures**. Then, check whether the task is contained in the list by **Name/ID**, **Operated At**, or **Task**.
      - If yes, the specification modification failed. See Follow-up Procedure for failure causes.
      - If no, the specifications have been modified.

Step 2: Check Disk Attachment

Disk attachment may fail after specifications are modified. Therefore, check disk attachment after specification modification. If disks are properly attached, the specification modification is successful.

- Windows

  For details, see What Should I Do If the Data Disk of a Windows HECS Becomes Offline After the HECS Specifications Are Modified?

- Linux

  For details, see What Should I Do If the Disk of a Linux HECS Becomes Offline After the HECS Specifications Are Modified?

Follow-up Procedure

In the event of a specification modification failure, view the failure cause using the Cloud Trace Service by performing the following operations:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console.
2. Under **Management & Deployment**, click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List**.
4. In the **Trace Name** column, locate the **resizeServer** event by resource ID.
   The resource ID is the ID of the HECS on which the specification modification failed.
5. Click **View Trace** in the **Operation** column to view the failure cause.
   If the fault cannot be rectified based on logs, contact technical support.

 Copyright © Huawei Technologies Co., Ltd.

5 EVS Disks

5.1 Overview

What Is Elastic Volume Service?

Elastic Volume Service (EVS) offers scalable block storage for HECSs. With high reliability, high performance, and rich specifications, EVS disks can be used for distributed file systems, development and testing environments, data warehouse applications, and high-performance computing (HPC) scenarios to meet diverse service requirements.

Disk Types

HECSs support the following EVS disk types:

- High I/O: EVS disks of this type deliver a maximum of 5,000 IOPS and a minimum of 1 ms read/write latency. This disk type is designed to meet the needs of mainstream high-performance, high-reliability application scenarios, such as enterprise applications, small- and medium-scale development and testing, and web server logs.
- Ultra-high I/O: EVS disks of this type deliver a maximum of 33,000 IOPS and a minimum of 1 ms read/write latency. This disk type is excellent for ultra-high I/O, ultra-high bandwidth, and read/write-intensive application scenarios, such as distributed file systems in HPC scenarios or NoSQL/RDS in I/O-intensive scenarios.

EVS disks differ in performance and price. Choose the disk type most appropriate for your applications. For more information about EVS disk specifications and performance, see Disk Types and Performance.

5.2 Adding Disks to an HECS

Scenarios

Disks attached to an HECS are classified into system disks and data disks. A system disk is automatically created and attached when an HECS is created. You do not need to purchase the system disk separately.

Data disks can be purchased during or after the HECS creation. If you add a data disk when creating an HECS, the system automatically attaches the data disk to the HECS. You can also add data disks after creating an HECS.

 Copyright © Huawei Technologies Co., Ltd.

This section describes how to add data disks.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. In the upper right corner of the HECS list, enter the HECS name, IP address, or ID in the search box.
5. Locate the row containing the target HECS, click **More** in the **Operation** column, and choose **Add Disk**.

   The **Buy Disk** page is displayed.
6. Configure parameters for the new EVS disk as prompted. Table 5-1 shows the description of all parameters.

Table 5-1 Parameter description

Parameter	Sub-Parameter	Description	Example Value
Billing Mode	-	Mandatory Yearly/monthly is a prepaid billing mode. You will be charged based on the usage duration that you specified. This mode provides lower prices and is ideal when the usage duration is predictable. Only yearly/monthly EVS disks can be added to an HECS, and the disks have the same expiration time as the HECS.	Yearly/Monthly
Region	-	Optional Resources are region-specific and resources in different regions cannot communicate with each other over a private network. For lower network latency and faster access to your resources, select the region nearest to your target users. The newly added disk is located in the same region as the HECS by default.	-
Disk Specifications	Disk Type	Mandatory You can select the following disk types: • High I/O • Ultra-high I/O For more information about EVS disk specifications and performance, see Disk Types and Performance.	Ultra-high I/O
	Disk Size (GB)	Mandatory It refers to the EVS disk size. Set the disk size. **NOTE**	100 GB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Sub-Parameter	Description	Example Value
		The system shows you the remaining disk space you can purchase. If the disk size you need exceeds the upper limit, click **Increase Quota** to obtain a higher quota. You can purchase more disk size after the request is approved.	
Auto Backup	-	Optional If auto backup is enabled, the system automatically creates backups for the disk data at specified time points and deletes outdated backups according to the configured backup policy. When **Enable** is selected, a backup policy must be configured. You can either use the default backup policy or customize the policy based on your service requirements.	Enable
More	Advanced Settings • Share • SCSI • Encryption	Optional • Share If you select **Share**, a shared disk is created. A shared disk can be attached to up to 16 servers. If you do not select **Share**, a non-shared disk is created, and the disk can be attached to one server only. When you select both **SCSI** and **Share**, a shared SCSI disk is created. **NOTE** The sharing attribute of a disk cannot be changed after the disk has been created. • SCSI If you select **SCSI**, a SCSI disk is created. Such disks allow the server OS to directly access the underlying storage media and send SCSI commands to the disks. If you do not select **SCSI**, a VBD disk is created. That said, the disk device type is VBD, the default device type. **NOTE** The device type of a disk cannot be changed after the disk has been created. • Encryption The encryption function on this console is used for data disk encryption only. To use the disk encryption function, select **Encryption**. The displayed dialog box contains the following parameters: – KMS Key Name A KMS Key Name is displayed only after KMS access rights have been granted to	-

Parameter	Sub-Parameter	Description	Example Value
		EVS. **KMS Key Name** is the identifier of the key, and you can use **KMS Key Name** to specify the KMS key that is to be used for encryption. You can select one of the following keys: Default Master Key: After the KMS access rights have been granted to EVS, the system automatically creates a Default Master Key and names it **evs/default**. CMKs: Existing or newly created CMKs. For details, see **Key Management Service** > **Creating a CMK** in the *Data Encryption Workshop User Guide*. **NOTE** • Before you use the disk encryption function, KMS access rights need to be granted to EVS. If you have the right to grant the permission, grant the KMS access rights to EVS directly. If you do not have this permission, contact a user with the security administrator rights to grant KMS access rights to EVS, then repeat the preceding operations. • The encryption attribute of a disk cannot be changed after the disk is created.	
	Tag	Optional During the EVS disk creation, you can tag the EVS resources. Tags identify cloud resources for purposes of easy categorization and quick search. Tags are composed of key-value pairs. • Key: Mandatory if the disk is going to be tagged A tag key can contain a maximum of 36 characters. It consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). • Value: Optional if the disk is going to be tagged A tag value can contain a maximum of 43 characters. It consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). **NOTE** • A maximum of 10 tags can be added for an EVS disk. • Tag keys of the same EVS disk must be unique.	-
Disk	-	Mandatory	For example, if

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Sub-Parameter	Description	Example Value
Name		• If you create disks individually, this parameter value is used as the actual disk name. The name can contain a maximum of 64 characters. • If you create disks in a batch, this parameter value is used as the prefix of disk names, and one disk name will be composed of this parameter value and a four-digit number or letter. The name can contain a maximum of 59 characters.	you create two disks and set **volume** for **Disk Name**, the EVS disk names will be **volume-0001** and **volume-0002**.
Quantity	-	The default value is set to **1**, which means one disk will be created. Currently, you can create up to 100 disks at a time. **NOTE** The system shows you the maximum number of disks allowed to purchase. To ensure effective resource usage, if the number of disks you need exceeds the upper limit, click **Increase Quota** to obtain a higher quota. You can purchase the disks you need after the request is approved.	Disk quantity: 1
Bound Server	-	After the new disk is created, the system automatically attaches the disk to the HECS.	-
Expires	-	The expiration time of the newly added EVS disks is the same as that of the HECS.	-

7. Click **Buy Now** to confirm the order details and complete the payment.

Follow-up Procedure

If the attached disk is newly created, the disk can be used only after it is initialized. For instructions about how to initialize a data disk, see Initialize an EVS Data Disk.

5.3 Attaching a Disk to an HECS

Scenarios

After you created an HECS, if the disk space is not enough or does not meet your requirements, you can attach an existing EVS disk to the HECS, or choose **Storage** > **Elastic Volume Service** to purchase a new disk and attach it to the HECS.

Prerequisites

- There are EVS disks available.

 Copyright © Huawei Technologies Co., Ltd.

For instructions on how to purchase an EVS disk, see Purchasing an EVS Disk.

- The EVS disk is not being used by other resources.

  A disk that is being used by other resources cannot be attached.

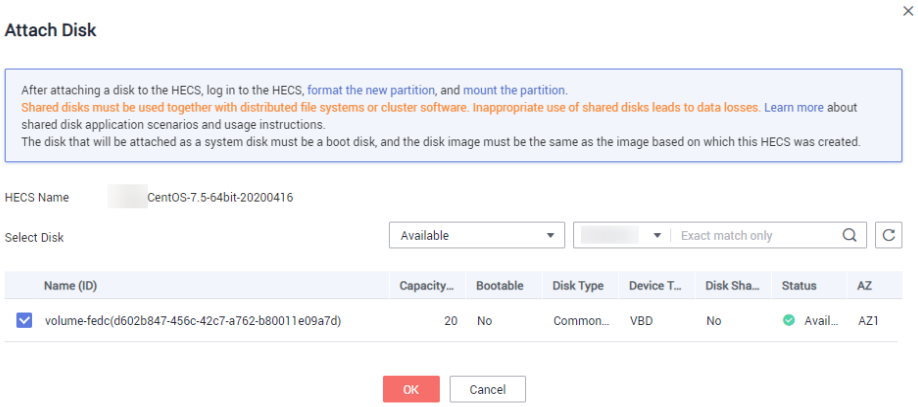
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. In the upper right corner of the HECS list, enter the HECS name, IP address, or ID in the search box.
5. Click the name of the target HECS to which you want to attach the disk.

   The HECS details page is displayed.
6. Click the **Disks** tab. Then, click **Attach Disk**.

   The **Attach Disk** dialog box is displayed.

   Figure 5-1 Attach Disk



7. Select the target disk and set disk function as prompted.

   NOTE

   - You can specify the disk as a system disk or data disk, but cannot specify the mount point.
   - For details about attachment restrictions, see What Are the Restrictions on Attaching an EVS Disk to an HECS?
8. Click **OK**.

   After the disk is attached, you can view the disk information on the **Disks** tab.

Follow-up Procedure

If the attached disk is newly created, the disk can be used only after it is initialized. For instructions about how to initialize a data disk, see Initialize an EVS Data Disk.

 Copyright © Huawei Technologies Co., Ltd.

5.4 Detaching a Disk from an HECS

Scenarios

Detach an EVS disk from an HECS.

- Disks mounted on **/dev/sda** or **/dev/vda** function as system disks. Before detaching a system disk from an HECS, you must stop the HECS.
- Disks mounted on other mount points functions as data disks. In addition to detaching a data disk from a stopped HECS, a data disk can also be detached from a running HECS if the HECS OS supports online detachment.

This section describes how to detach a disk from a running HECS.

Constraints

- The disk must be mounted on a mount point other than **/dev/sda** or **/dev/vda**.

  Disks mounted on **/dev/sda** or **/dev/vda** are system disks and cannot be detached from running HECSs.
- Before detaching an EVS disk from a running Windows HECS, make sure that VMware Tools has been installed on the HECS and is running properly.

  For how to install VMTools, see Optimization Process.
- Before detaching an EVS disk from a running Windows HECS, ensure that no program is reading data from or writing data to the disk. Otherwise, data will be lost.
- SCSI EVS disks cannot be detached from running Windows HECSs.
- Before detaching an EVS disk from a running Linux HECS, you must log in to the HECS and run the **umount** command to cancel the association between the disk and the file system. In addition, ensure that no program is reading data from or writing data to the disk. Otherwise, the disk will fail to detach.
- The disk is not locked.

  A locked disk cannot be detached.

Precautions

- On a running Windows HECS, if the disk is not in the offline state, the system forcibly detaches the disk. If this occurs, the system may generate a xenvbd alarm. You can ignore this alarm.

  NOTE

  To view the disk status, perform the following operations:

  1. Click **Start** in the task bar. In the displayed **Start** menu, right-click **Computer** and choose **Manage** from the shortcut menu.

     The **Server Manager** page is displayed.
  2. In the navigation tree, choose **Storage** > **Disk Management**.

     The disk list is displayed in the right pane.
  3. View the status of each disk.
- Do not detach a disk from a running HECS that is being started, stopped, or restarted.
- Do not detach a disk from a running HECS whose OS does not support this feature. OSs supporting EVS disk detachment from a running HECS are listed in OSs Supporting EVS Disk Detachment from a Running HECS.

Copyright © Huawei Technologies Co., Ltd.

- For a running Linux HECS, the drive letter may be changed after an EVS disk is detached from it and then attached to it again. This is a normal case due to the drive letter allocation mechanism of the Linux system.
- For a running Linux HECS, the drive letter may be changed after an EVS disk is detached from it and the HECS is restarted. This is a normal case due to the drive letter allocation mechanism of the Linux system.

OSs Supporting EVS Disk Detachment from a Running HECS

OSs supporting EVS disk detachment from a running HECS include two parts:

- For the first part, see Formats and OSs Supported for External Image Files.
- For the second part, see Table 5-2.

Table 5-2 OSs supporting disk detachment from a running HECS

OS	Version
CentOS	7.3 64-bit
	7.2 64-bit
	6.8 64-bit
	6.7 64-bit
Debian	8.6.0 64-bit
	8.5.0 64-bit
Fedora	25 64-bit
	24 64-bit
SUSE	SUSE Linux Enterprise Server 12 SP2 64-bit
	SUSE Linux Enterprise Server 12 SP1 64-bit
	SUSE Linux Enterprise Server 11 SP4 64-bit
	SUSE Linux Enterprise Server 12 64-bit
openSUSE	42.2 64-bit
	42.1 64-bit
Oracle Linux Server release	7.3 64-bit
	7.2 64-bit
	6.8 64-bit
	6.7 64-bit
Ubuntu Server	16.04 64-bit
	14.04 64-bit
	14.04.4 64-bit

 Copyright © Huawei Technologies Co., Ltd.

OS	Version
Windows (SCSI EVS disks cannot be detached from a running HECS.)	Windows Server 2008 R2 Enterprise 64-bit
	Windows Server 2012 R2 Standard 64-bit
	Windows Server 2016 R2 Standard 64-bit
Red Hat Enterprise Linux	7.3 64-bit
	6.8 64-bit

NOTE

For HECSs running OSs not listed in the preceding table, stop the HECSs and then detach the disks to prevent any possible problems that may occur.

Procedure

1. On the **Hyper Elastic Cloud Server** page, click the name of the target HECS. The HECS details page is displayed.
2. Click the **Disks** tab. Locate the target disk and click **Detach**.

5.5 Expanding Disk Capacity

Scenarios

When your disk capacity is not enough, you can handle it by expanding the disk capacity.

Procedure

The disk space can be expanded in either of the following ways:

- Create a disk and attach it to an HECS.
- Expand the capacity of an existing disk. Both system disks and data disks can be expanded.

  You can expand the disk capacities when the disks are in the **In-use** or **Available** state.

  - Expanding an **In-use** disk means that the to-be-expanded disk has been attached to an HECS. Currently, only some HECS OSs support the expansion of **In-use** disks. Therefore, ensure that the HECS OS meets the requirements before you expand an **In-use** disk. For details, see Expanding Capacity for an In-use EVS Disk.
  - Expanding an **Available** disk means that the to-be-expanded disk has not been attached to any server. For details, see Expanding Capacity for an Available EVS Disk.

Related Operations

For more information, see Expansion Overview.

Copyright © Huawei Technologies Co., Ltd.

5.6 Initializing a Windows Data Disk Using a Script

Scenarios

When a data disk is attached to an HECS, you must log in to the HECS and initialize the disk before you can use the disk.

The method of initializing data disks for an HECS is the same as that of initializing disks for an ECS. This section describes how to use scripts to initialize data disks for a Windows HECS. For more information, see Introduction to Data Disk Initialization Scenarios and Partition Styles.

This section uses Windows Server 2012 R2 Standard 64bit as an example to describe how to automatically initialize data disks attached to a Windows HECS.

The way to initialize a disk varies with the HECS OS. The operations described in this section are for reference only. For detailed operations and differences, see the product documentations of the HECS OSs.

NOTE

When using a disk for the first time, if you have not initialized it, including creating partitions and file systems, the additional space added to this disk in an expansion later may not be normally used.

Prerequisites

- A data disk has been attached to the HECS and has not been initialized.
- You have logged in to the HECS.

Constraints

- This script uses the NTFS file system and MBR partition style by default.
- This script does not support the initialization of disks that form Windows logical volume groups.
- This script supports the initialization of up to 23 Windows data disks.

Manually Executing the Script to Initialize Windows Data Disks

Step 1 Log in to the HECS, download the script for automatically initializing disks, and save the script to **C:\Windows\System32**.

Step 2 Run Windows PowerShell as administrator.

Step 3 In the displayed dialog box, run the following command to set the script execution policy:

Set-ExecutionPolicy -ExecutionPolicy Bypass -Force

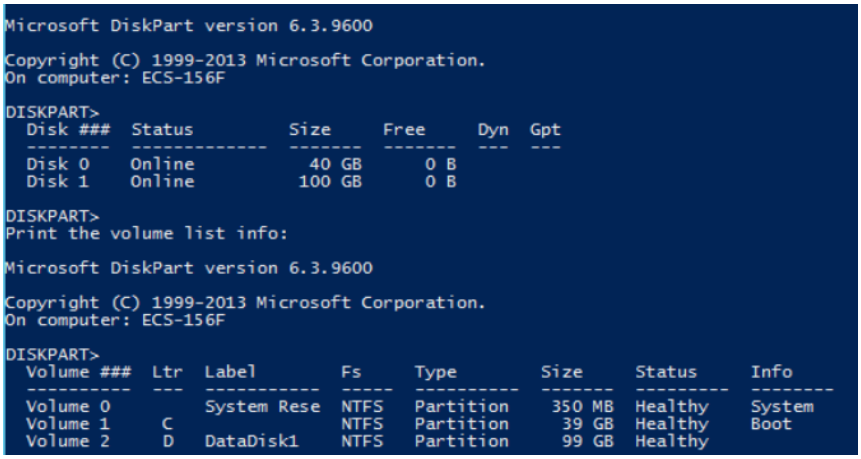
Step 4 Run the following command in the dialog box to execute the initialization script:

C:\Windows\System32\WinVMDataDiskAutoInitialize.ps1

Information similar to the following is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-2 Executing the automation script



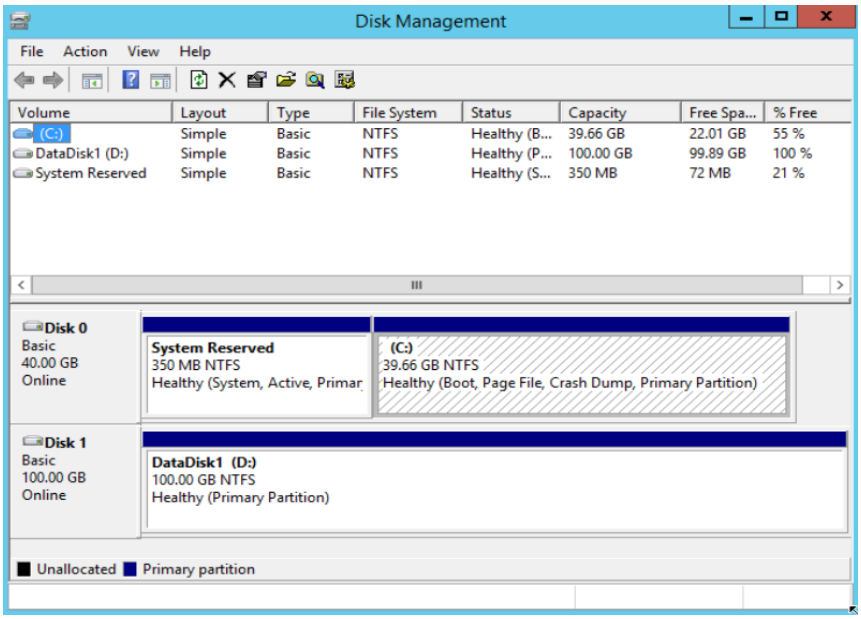
NOTE

If the command output shows that PowerShell cannot load the file, this is because the Windows system policy does not allow the PowerShell script downloaded from the network to be executed if the script is not signed.

To resolve this issue, run the **set-ExecutionPolicy RemoteSigned** command and restart PowerShell.

Step 5 (Optional) On the **Disk Management** page, view the initialization result.

Figure 5-3 Disk Management



----End

Configuring Automatic Initialization of Windows Data Disks

Step 1 On the HECS desktop, click **Start** and choose **Server Manager**.

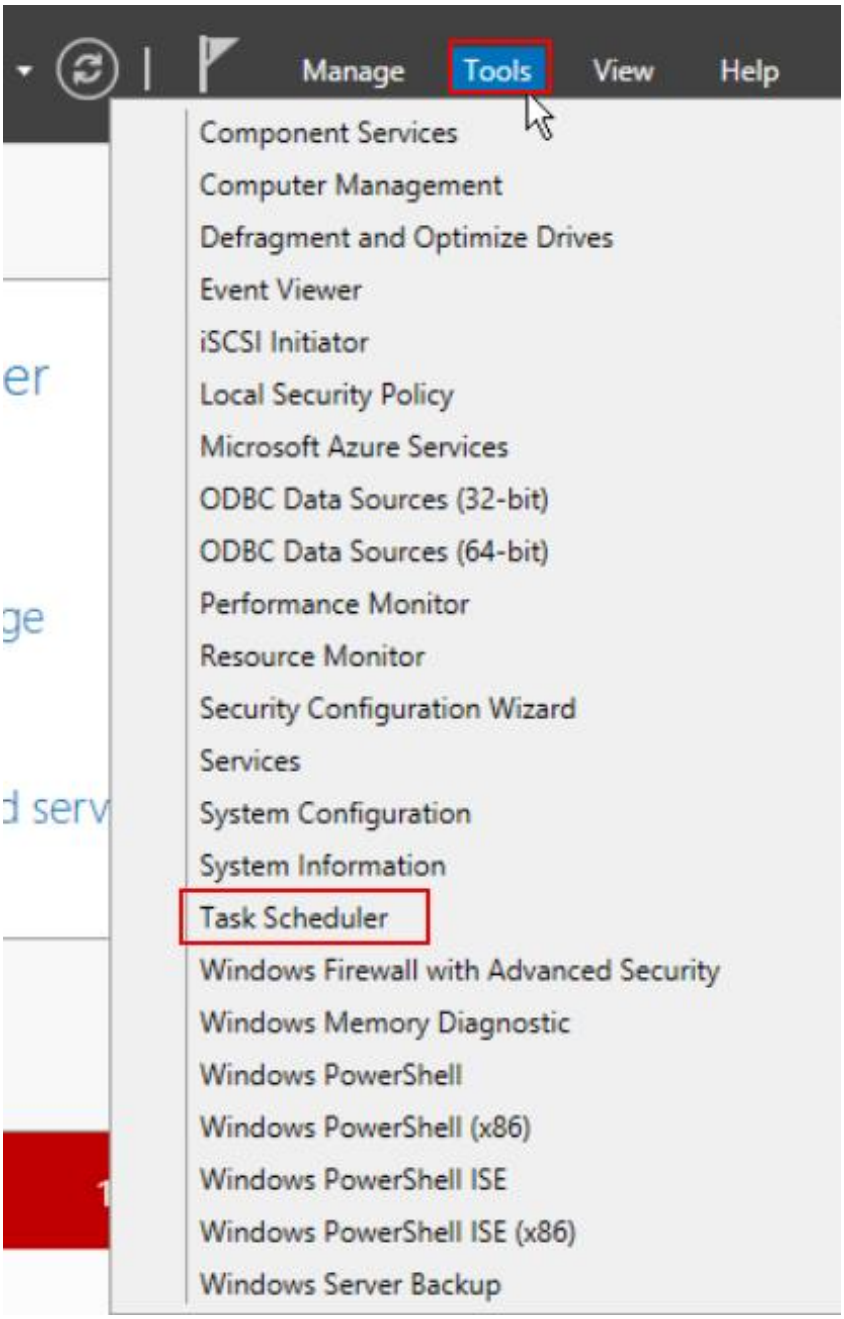
 Copyright © Huawei Technologies Co., Ltd.

The **Server Manager** page is displayed.

Step 2 In the navigation pane on the left, choose **Tools** > **Task Scheduler**, then right-click **Task Scheduler Library** and choose **Create Task** from the shortcut menu.

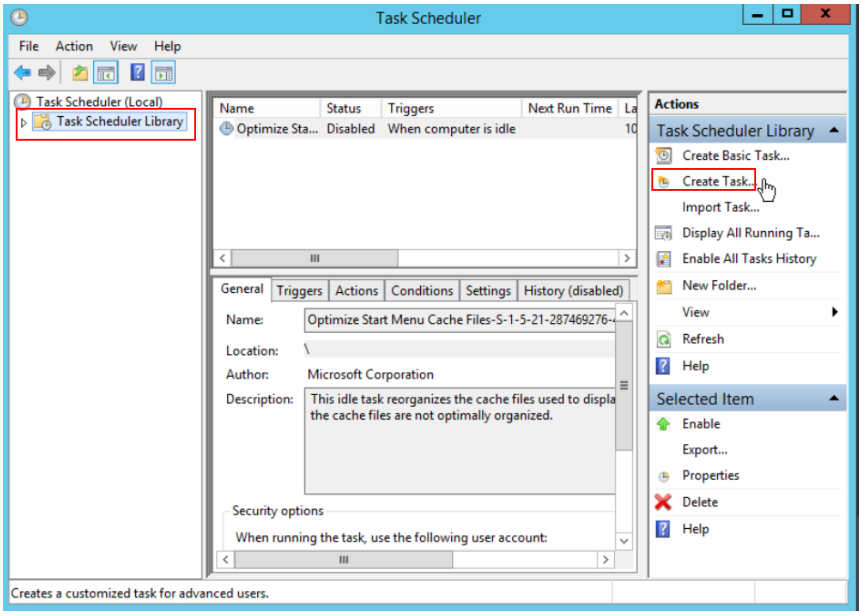
The **Create Task** page is displayed.

Figure 5-4 Tools



 Copyright © Huawei Technologies Co., Ltd.

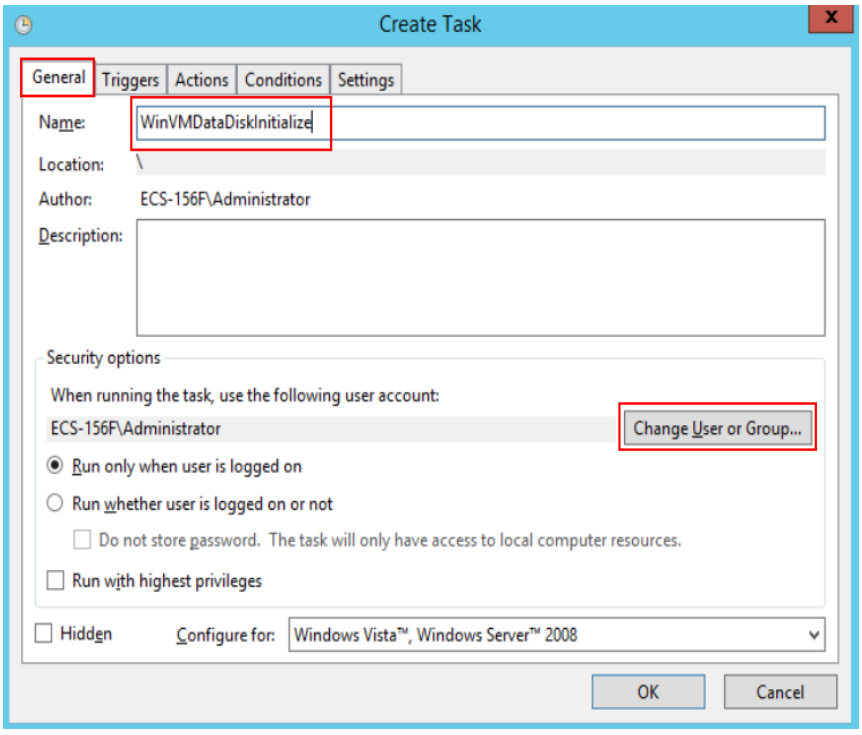
Figure 5-5 Task Scheduler



Step 3 On the displayed page, click the **General** tab, enter **WinVMDataDiskInitialize** in the **Name** text box, and click **Change User or Group**.

The **Select User or Group** page is displayed.

Figure 5-6 Create Task



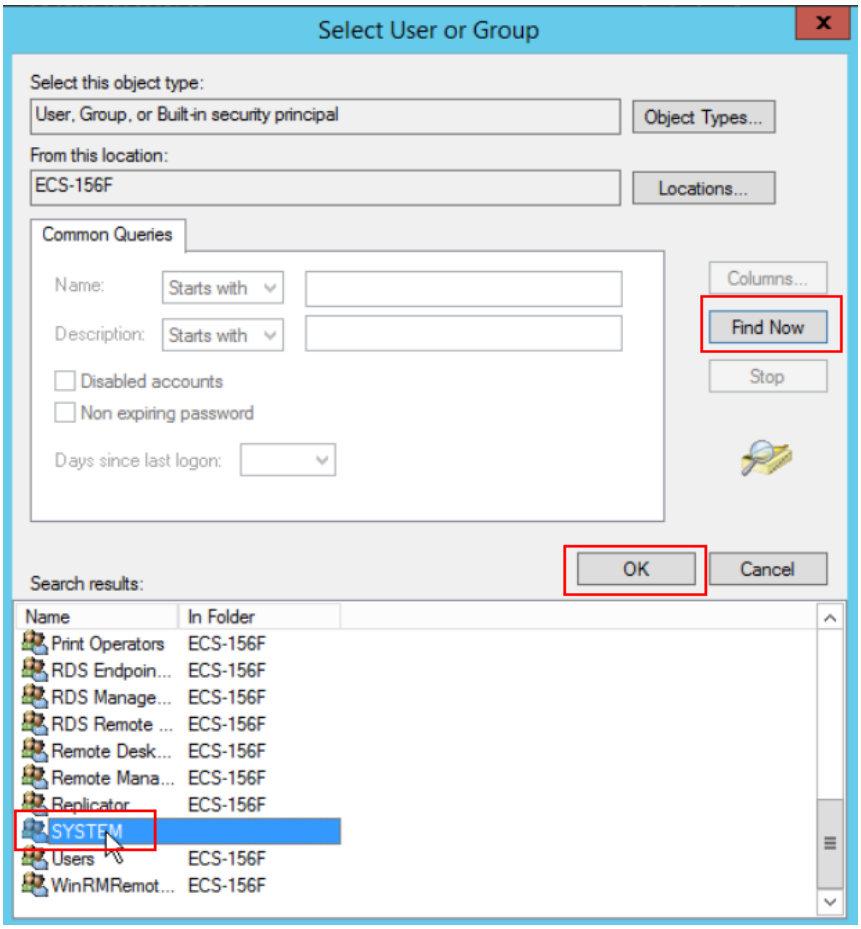
Step 4 Click **Advanced** in the lower left corner of the page.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Click **Find Now** on the right side of the page. In the search result list, select **SYSTEM** and click **OK**.

The **Select User or Group** page is displayed.

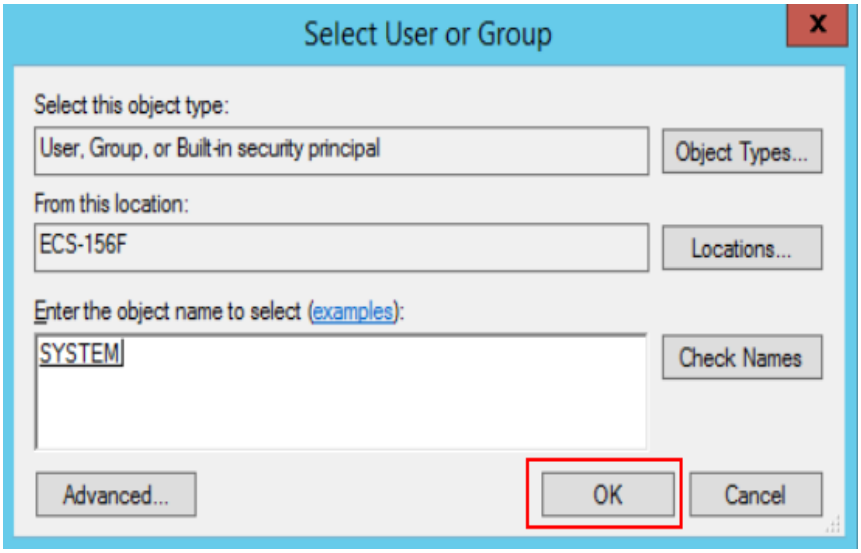
Figure 5-7 Selecting **SYSTEM**



Step 6 Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

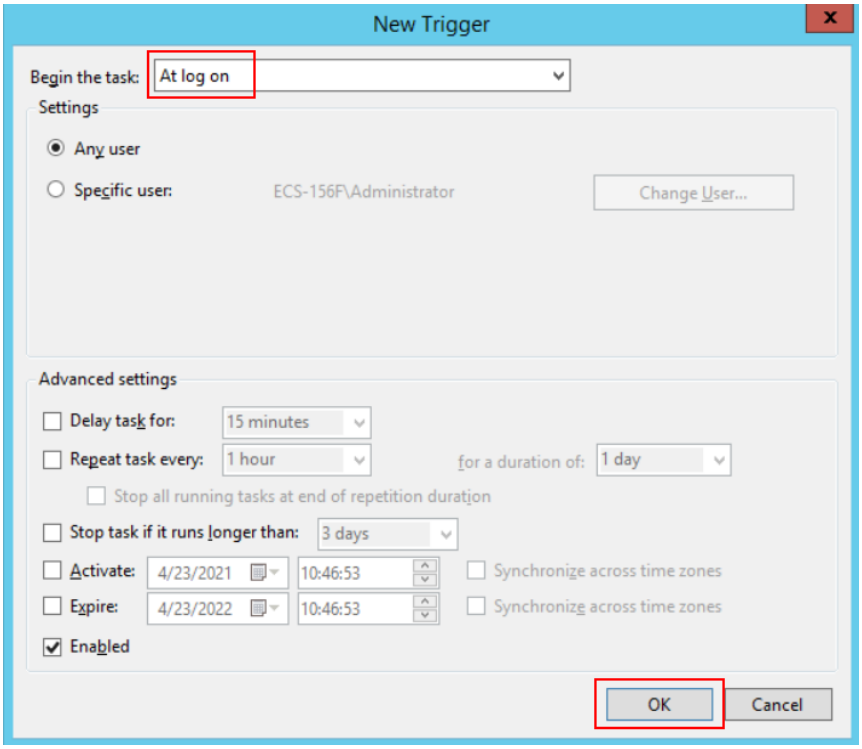
Figure 5-8 Clicking **OK**



Step 7 Click the **Triggers** tab and click **New** in the lower left corner of the page.

Step 8 On the **New Trigger** page, choose **At log on** for **Begin the task**, retain the default settings for other parameters, and click **OK**.

Figure 5-9 New Trigger



Step 9 Click the **Actions** tab and click **New** in the lower left corner of the page.

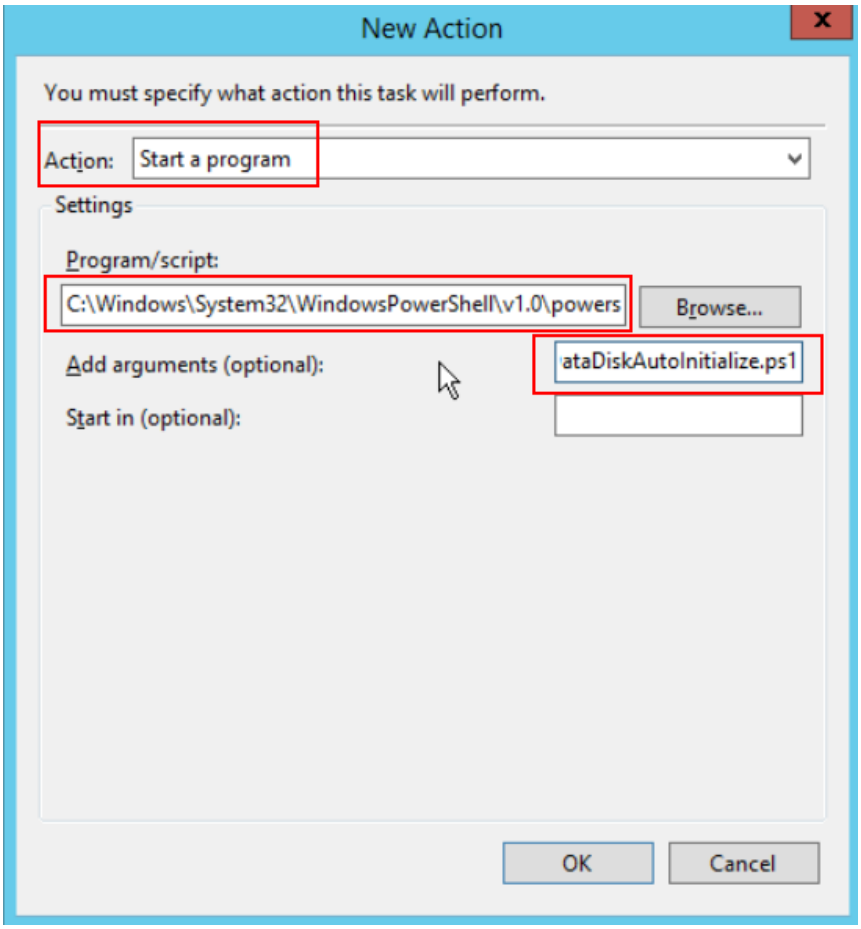
Step 10 On the **New Action** page, set the following parameters:

 Copyright © Huawei Technologies Co., Ltd.

- **Action**: Select **Start a program**.
- **Program/script**: Select **powershell.exe**.
- **Add arguments (optional)**: Enter **-ExecutionPolicy Bypass C:\Windows\System32\WinVMDataDiskAutoInitialize.ps1**.

Click **OK**.

Figure 5-10 New Action



Step 11 On the **Create Task** page, click **OK**.

After the configuration is complete, new EVS disks attached to this HECS will be automatically initialized when the HECS is logged in to again.

NOTE

To enable automatic initialization of Windows data disks on multiple HECSs, configure automatic initialization on one HECS, create a private image for this HECS, and use the image to batch create HECSs.

----End

 Copyright © Huawei Technologies Co., Ltd.

5.7 Initializing a Linux Data Disk Using a Script

Scenarios

When a data disk is attached to an HECS, you must log in to the HECS and initialize the disk before you can use the disk.

The method of initializing data disks for an HECS is the same as that of initializing disks for an ECS. This section describes how to use scripts to initialize data disks for a Windows HECS. For more information, see Introduction to Data Disk Initialization Scenarios and Partition Styles.

This section uses CentOS 7.4 64bit as an example to describe how to initialize data disks attached to a Linux HECS using an initialization script.

The way to initialize a disk varies with the HECS OS. The operations described in this section are for reference only. For detailed operations and differences, see the product documentations of the HECS OSs.

Prerequisites

- A data disk has been attached to the HECS and has not been initialized.
- You have logged in to the HECS.

Constraints

This script uses the EXT4 file system by default. This script cannot be used to create LVM or VG partitions.

Initializing New Disks

1. Log in to the HECS and run the following command to obtain the automatic disk initialization script:

   wget https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/datadisk/LinuxVMDataDiskAutoInitialize.sh

2. Run the following command to change the permission of the script:

   chmod -x LinuxVMDataDiskAutoInitialize.sh

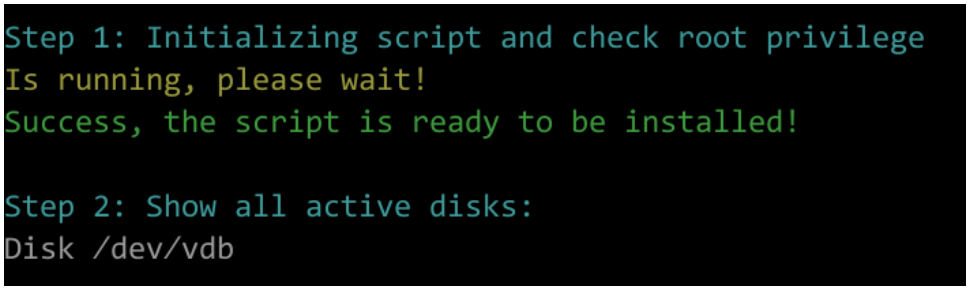
3. Execute the following script to automatically detect the data disks to be initialized:

   sh LinuxVMDataDiskAutoInitialize.sh

   The script automatically detects and displays the drive letters (for example, **/dev/vdb**) except the system disk on the HECS. Then, you need to enter the drive letter to be initialized, for example, **/dev/vdb**.

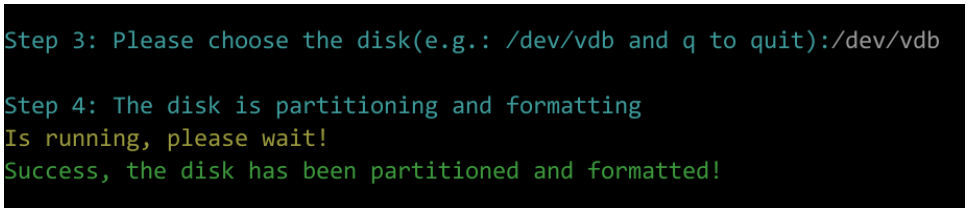
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-11 Automatically detecting disks



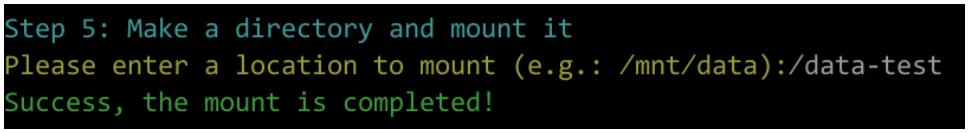
4. Enter the drive letter and press **Enter**. The script automatically creates the partition for the disk and formats it.

Figure 5-12 Entering the drive letter



5. Enter the directory on which you want to mount the partition, for example, **/data-test**.

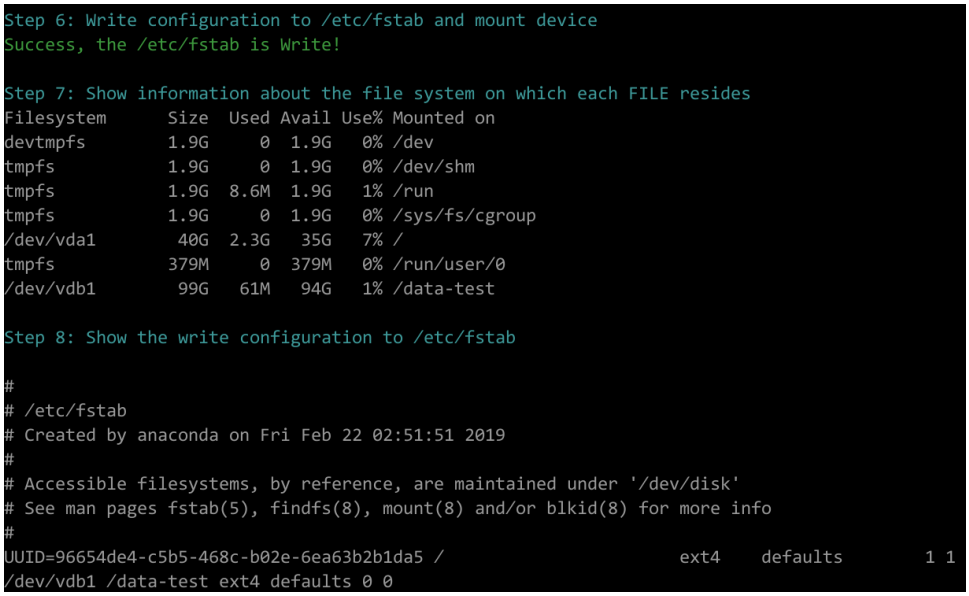
Figure 5-13 Entering the mounting directory



The initialization is complete until the script has mounted the partition and configured automatic mounting upon HECS startup.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-14 Disk initialization completed



Initializing Existing Disks

1. Log in to the HECS and run the following command to obtain the automatic disk initialization script:

   wget https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/datadisk/LinuxVMDataDiskAutoInitialize.sh

2. Run the following command to change the permission of the script:

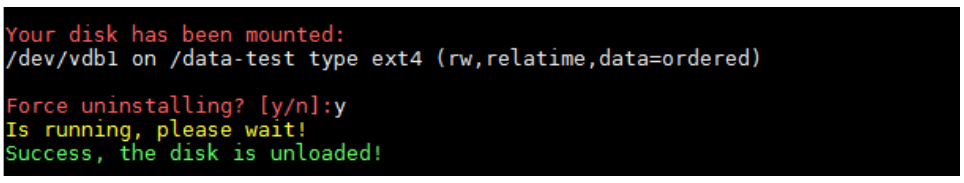
   chmod -x LinuxVMDataDiskAutoInitialize.sh

3. Execute the following script to automatically detect the data disks to be initialized:

   sh LinuxVMDataDiskAutoInitialize.sh

4. The script automatically detects that the disk partition has been mounted and displays the mounting directory. Determine whether to unmount the partition. Enter **y** to unmount the partition, or enter **n** to exit the script. In this example, enter **y** to continue the initialization.

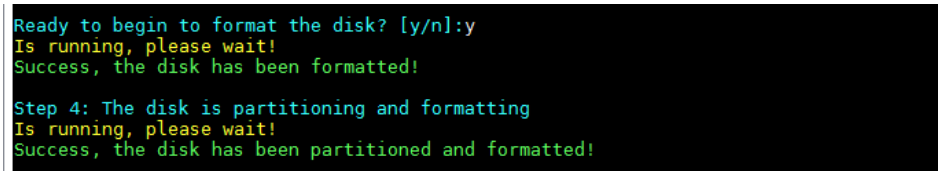
   Figure 5-15 Unmounting the disk partition

5. After the disk partition is unmounted, determine whether to format the disk. Enter **y** to format the disk, or enter **n** to exit the script.

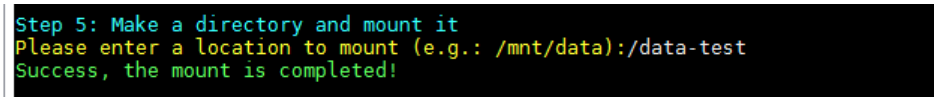
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-16 Formatting the disk



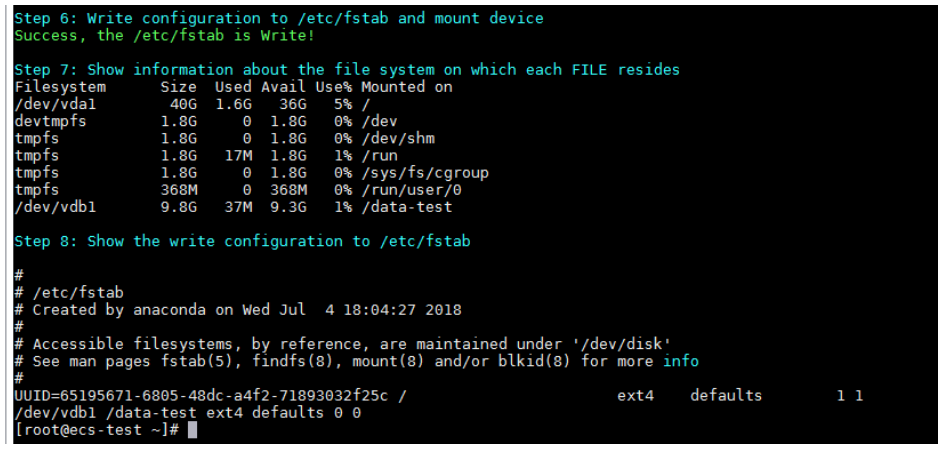
6. After the disk is formatted, the system automatically creates a partition and completes the formatting. Enter the directory on which you want to mount the partition, for example, **/data-test**.

Figure 5-17 Entering the mounting directory



The initialization is complete until the script has mounted the partition and configured automatic mounting upon HECS startup.

Figure 5-18 Disk formatting and partition mounting completed



 Copyright © Huawei Technologies Co., Ltd.

6 Password

6.1 Resetting an HECS Password on the Management Console

Scenarios

If you did not set a password when creating an HECS, or the password is forgotten or expired, reset the password by following the instructions provided in this section.

NOTE

If you reset the password for a running HECS, the new password takes effect only after the HECS is restarted. You can select **Auto Restart**.

Prerequisites

- You have installed password reset plug-ins before your HECS password is forgotten or expires.
  - The password reset plug-ins have been installed on the HECSs created using a public image by default.
  - If you use a private image to create an HECS (for example, using a private image to change the OS), install the password reset plug-in first.
- Do not delete the CloudResetPwdAgent or CloudResetPwdUpdateAgent process. Otherwise, one-click password reset will not be available.
- DHCP is enabled in the VPC to which the HECS belongs.
- The HECS network is accessible.

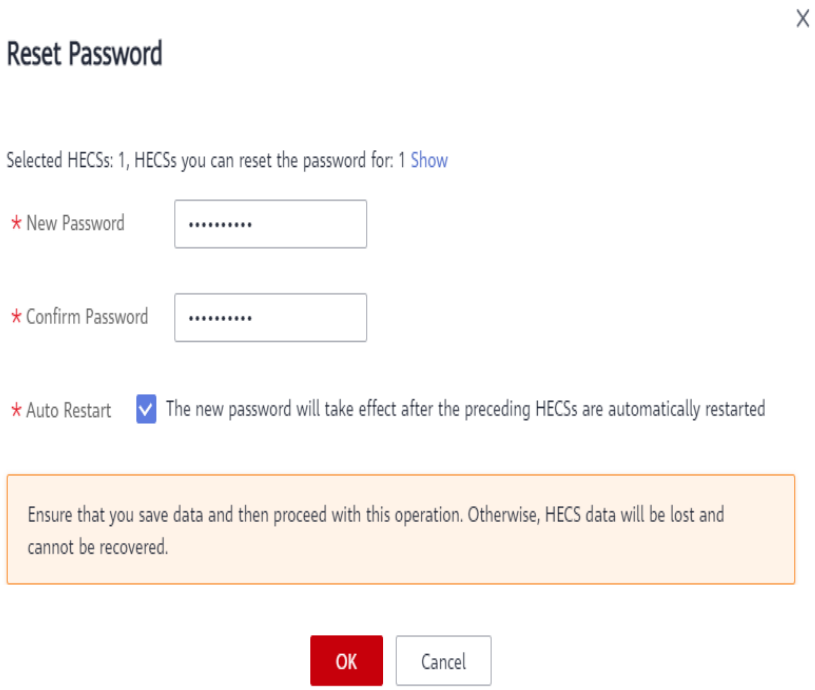
Procedure

Perform the following operations to change the login password of one or multiple HECSs in a batch on the management console.

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. Locate the row containing the target HECS, click **More** in the **Operation** column, and select **Reset Password** from the drop-down list.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Reset Password



NOTE

The HECSs with one-click password reset plug-ins installed support batch resetting of passwords. To batch reset passwords, perform the following operations:

1. Select the target HECSs.
2. Click **Reset Password** in the upper part of the HECS list.
3. Set a new password as prompted.

   After the resetting, the login passwords of these HECSs are the same.

4. Set and confirm a new password as prompted.

   If you reset the password for a running HECS, the new password takes effect only after the HECS is restarted. You can select **Auto Restart**.

   The new password must meet the complexity requirements listed in Table 6-1.

Table 6-1 Password complexity requirements

Parameter	Requirement	Example Value
Password	• Consists of 8 characters to 26 characters. • Contains at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters for Windows: $!@%-_=+[]:./,?	YNbUwp!dUc9MClnv **NOTE** The example password is generated randomly. Do not copy this example password.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Requirement	Example Value
	– Special characters for Linux: !@%-_=+[]:./^,{}? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)	

5. Click **OK**.

   It takes about 10 minutes for the system to reset the password. Do not repeatedly perform this operation.

   The new password takes effect after the HECS is started.

6.2 Changing the Login Password on an HECS

Scenarios

This section describes how to change the password for logging in to an HECS when the password is about to expire, the password is forgotten, or you log in to the HECS for the first time. You are advised to change the initial password upon the first login.

Resetting an HECS Password on the Management Console is preferentially recommended.

Prerequisites

The target HECS can be logged in.

Background

Table 6-2 shows the HECS password complexity requirements.

Table 6-2 Password complexity requirements

Parameter	Requirement	Example Value
Password	• Consists of 8 characters to 26 characters. • Contains at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters for Windows: $!@%-_=+[]:./,? – Special characters for Linux: !@%-_=+[]:./^,{}?	YNbUwp!dUc9MClnv **NOTE** The example password is generated randomly. Do not copy this example password.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Requirement	Example Value
	• Cannot contain the username or the username spelled backwards. • Cannot contain more than two characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)	

Windows

1. Log in to the HECS.

   For details, see Login Overview.
2. Press **Win+R** to start the **Run** dialog box.
3. Enter **cmd** to open the CLI window.
4. Run the following command to change the password (the new password must meet the requirements described in Table 6-2):

   net user Administrator *New password*

Linux

1. Log in to the HECS as user **root**.

   For details, see 2.1 Login Overview.
2. Run the following command to reset the password of user **root**:

   passwd

   To reset the passwords of other users, replace **passwd** with **passwd** *username*.
3. Enter the new password as prompted. Ensure that the new password meets the requirements described in Table 6-2.

   ```
   New password:
   Retype new password:
   ```

   If the following information is displayed, the password has been changed:

   ```
   passwd: password updated successfully
   ```

 Copyright © Huawei Technologies Co., Ltd.

7 NICs

7.1 Overview

VPC

Virtual Private Cloud (VPC) allows you to create customized virtual networks in your logically isolated AZ. These networks are dedicated zones that are logically isolated for your HECSs. You can define security groups, virtual private networks (VPNs), IP address segments, and bandwidth for a VPC. This facilitates internal network configuration and management as well as secure and convenient network modification. You can also customize the cloud server access rules within a security group and between security groups to strengthen cloud server security protection.

For more information about VPC, see *Virtual Private Cloud User Guide*.

NICs

A NIC is a virtual one that can be bound to an HECS in a VPC. Through the NIC, you can manage the HECS network. A NIC can be a primary NIC or an extension NIC.

- Primary NIC

  When you create an HECS, the NIC automatically created with the HECS is the primary NIC. The primary NIC cannot be unbound. It is preferentially used for the default route generally.
- Extension NIC

  A NIC that can be separately added is an extension NIC, which can be bound to or unbound from an HECS.

7.2 Adding a NIC

Scenarios

If more NICs are required for your HECSs, perform the following steps to add a NIC to the HECS:

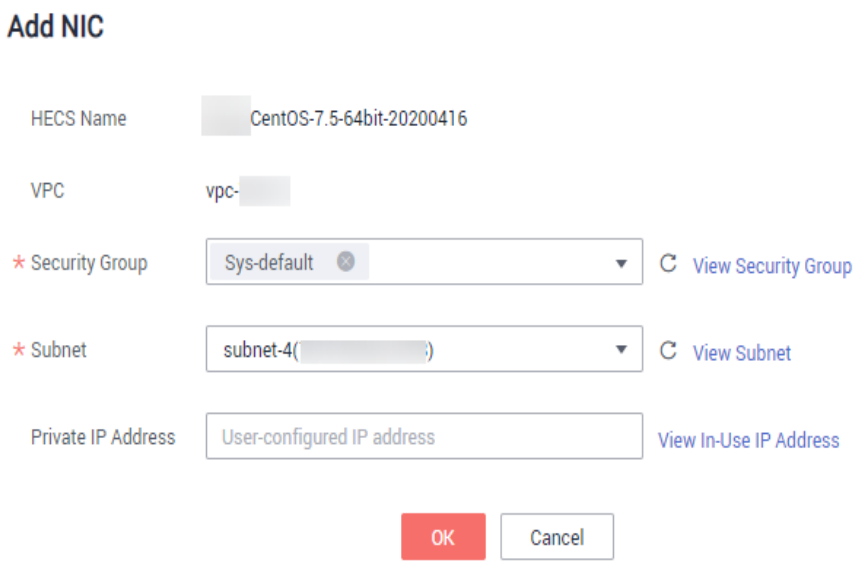
 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Halo ECS**.
4. Click the name of the HECS to which a NIC is to be added.

   The page providing details about the HECS is displayed.
5. Click the **NICs** tab. Then, click **Add NIC**.
6. Select the security group and subnet to be added on the page shown in the following figure. Select the subnet and security group to be added.

   Figure 7-1 Selecting the security group and subnet

   - **Security Group**: You can select multiple security groups at a time. In this case, the access rules of all the selected security groups apply to the HECS.
   - **Private IP Address**: If you need to add a NIC with a specified IP address to the HECS, enter a private IP address.
7. Click **OK**.

Follow-up Operations

Some OSs cannot identify newly added NICs. In this case, you must manually activate the NICs. Ubuntu is used as an example in the following NIC activation procedure. Required operations may vary among systems. For additional information, see the documentation for your OS.

1. Locate the row that contains the HECS, and click **Remote Login** in the **Operation** column.

   Log in to the HECS.
2. Run the following command to view the NIC name:

 Copyright © Huawei Technologies Co., Ltd.

ifconfig -a

In this example, the NIC name is **eth2**.

3. Run the following command to switch to the target directory:

   cd /etc/network

4. Run the following command to open the **interfaces** file:

   vi interfaces

5. Add the following information to the **interfaces** file:

   auto *eth2*

   iface *eth2* inet dhcp

6. Run the following command to save and exit the **interfaces** file:

   :wq

7. Run either the **ifup eth2** command or the **/etc/init.d/networking restart** command to make the newly added NIC take effect.

   X in the preceding command indicates the NIC name and SN, for example, **ifup eth2**.

8. Run the following command to check whether the NIC name obtained in step 2 is displayed in the command output:

   ifconfig

   For example, check whether **eth2** is displayed in the command output.

   - If yes, the newly added NIC has been activated, and no further action is required.
   - If no, the newly added NIC failed to be activated. Go to step 9.

9. Log in to the management console, locate the row that contains the HECS. In the **Operation** column, click **More** and then click **Restart**.

10. Run the following command to check whether the NIC name obtained in step 2 is displayed in the command output:**ifconfig**

    - If they are the same, no further action is required.
    - If no, contact customer service.

7.3 Deleting an Extension NIC

Scenarios

Each HECS can have one primary NIC and multiple extension NICs, and the primary NIC cannot be deleted.

This section describes how to delete an extension NIC on the console.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Hyper ECS**.
4. Click the name of the target HECS.

   The page providing details about the HECS is displayed.

5. Click the **NICs** tab. Then, click **Delete** in the row of the target NIC.

 Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> You are not allowed to delete the primary NIC. By default, the primary NIC is the first NIC displayed in the NIC list.

6. Click **Yes** in the displayed dialog box.

> **NOTE**
>
> Certain HECSs do not support NIC deletion when they are running. For details about these HECSs, see the GUI display. Before you delete an extension NIC from such an HECS, stop the HECS.

7.4 Changing a VPC

Scenarios

This section describes how to change a VPC.

Constraints

- A VPC can be changed on a single NIC only.
- Changing a VPC will interrupt HECS network connections.
- During the change process, do not perform operations on the HECS, including its EIP.
- After the VPC is changed, the subnet, private IP address, and MAC address of the HECS will change.
- After the VPC is changed, the source/destination check and virtual IP address must be configured again.
- After the VPC is changed, you are required to reconfigure network-related application software and services, such as ELB, VPN, NAT, and DNS.

Procedure

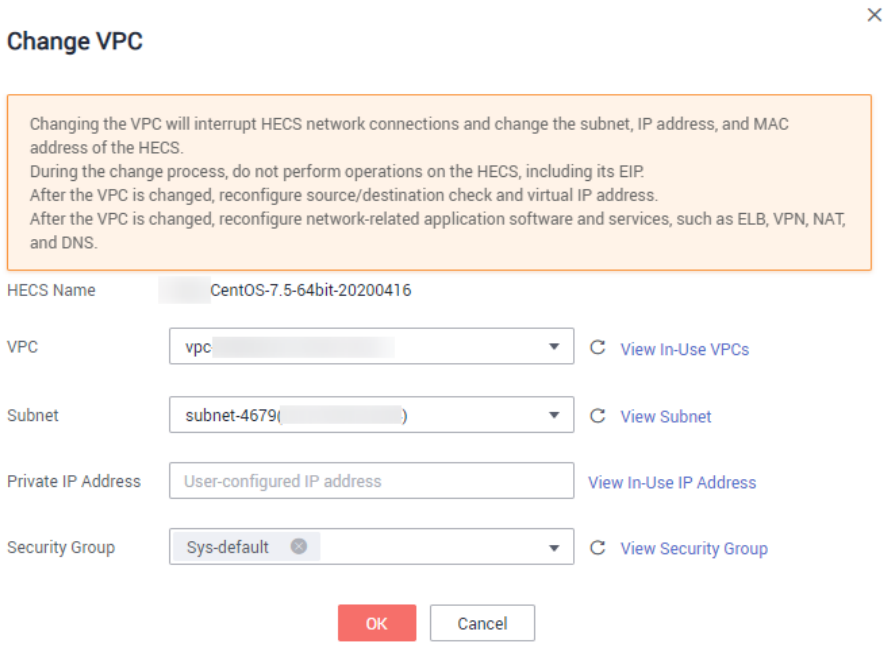
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Halo ECS**.
4. Click the name of the target HECS.

   The page providing details about the HECS is displayed.
5. Click the **NICs** tab and click **Change VPC**.

   The **Change VPC** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-2 Change VPC



6. Select an available VPC and subnet from the drop-down lists, and set the private IP address and security group as prompted.

   You can select multiple security groups. In this case, the access rules of all the selected security groups apply on the HECS.

NOTE

Using multiple security groups may deteriorate HECS network performance. You are recommended to select no more than five security groups.

7. Click **OK**.

7.5 Modifying a Private IP Address

Scenarios

You can modify the private IP address of the primary NIC. If you want to modify the private IP address of an extension NIC, delete the NIC and attach a new NIC.

Notes and Constraints

- The HECS has been stopped.
- If a virtual IP address or DNAT rule has been configured for the NIC, cancel the configuration before modifying the private IP address.
- If the NIC has an IPv6 address, its private IP address (including IPv4 or IPv6 address) cannot be modified.
- Before changing the private IP address of a backend server of a load balancer, remove the backend server from the backend server group.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. Click the name of the target HECS.

   The page providing details about the HECS is displayed.
4. Click the **NICs** tab. Locate the row containing the primary NIC and click **Modify Private IP**.

   The **Modify Private IP** dialog box is displayed.
5. Change the subnet and private IP address of the primary NIC as required.

   NOTE

   Yon can only select a subnet within the same VPC.

   If you do not specify the private IP address, the system will automatically assign one to the primary NIC.

7.6 Managing Virtual Private IP Addresses

Scenarios

A virtual IP address provides the second IP address for one or multiple HECS NICs, improving high availability between the HECSs.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Halo ECS**.
4. Click the name of the HECS to which the virtual IP address is to be bound.

   The page providing details about the HECS is displayed.
5. Click the **NICs** tab. Then, click **Manage Virtual IP Address**.
6. In the **Manage Virtual IP Address** dialog box, select **Bind virtual IP address**.
7. Set the IP address.

   This IP address is a virtual one. Multiple HECSs deployed to work in active/standby mode can be bound to the same virtual IP address for disaster recovery.
8. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

8 Security Groups

8.1 Overview

Security Group

A security group is a collection of access control rules for HECSs that have the same security protection requirements and that are mutually trusted. You can create various access rules for the security groups you create. These rules will apply to all HECSs added to this security group.

You can customize a security group or use the default one provided by the system that permits all outbound traffic and denies inbound traffic. HECSs in a security group are mutually accessible. For details about the default security group, see 8.2 Default Security Group and Rules.

NOTE

If two HECSs are in the same security group but in different VPCs, the security group does not take effect. You can use a VPC peering connection to connect the two VPCs. For details, see VPC Connection.

Security Group Rules

You can add rules to the security groups you create. A rule applies either to inbound traffic (ingress) or outbound traffic (egress). HECSs added to a security group are protected by the rules of the group.

Each security group has default rules. For details, see 8.2 Default Security Group and Rules. You can also customize security group rules. For details, see 8.4 Configuring Security Group Rules.

Security Group Constraints

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, each security group can have a maximum of 50 security group rules.
- By default, an HECS or an HECS extension NIC can be added to a maximum of five security groups.
- A maximum of 20 HECSs can be added to a security group at a time.
- A security group can be associated with a maximum of 1,000 HECSs.

 Copyright © Huawei Technologies Co., Ltd.

Helpful Links

- Default Security Group and Rules
- Security Group Configuration Examples
- Configuring Security Group Rules
- Changing a Security Group

8.2 Default Security Group and Rules

Your account automatically comes with a default security group that allows all outbound traffic and denies all inbound traffic. Your HECSs in the security group can communicate with each other without the need to add rules.

Figure 8-1 shows the default security group.

Figure 8-1 Default Security Group

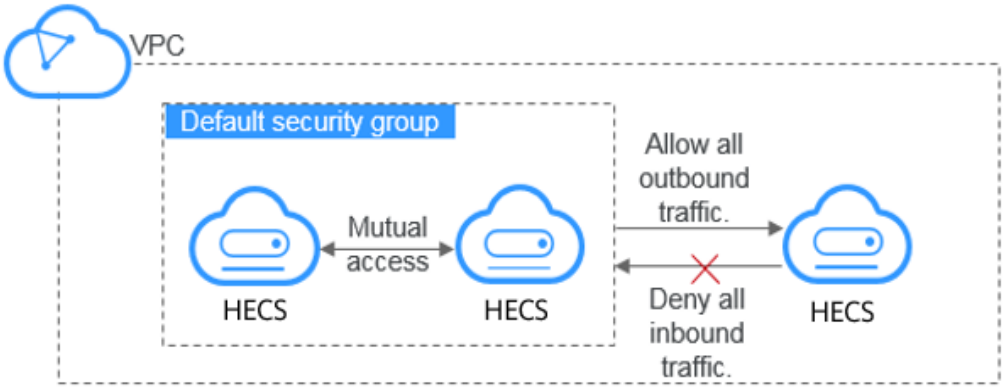


Table 8-1 describes default security group rules.

Table 8-1 Default security group rules

Direction	Protocol	Port Range	Source/Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: ID of the current security group (for example, sg-*xxxxx*)	Allows communication among HECSs within the security group and denies all inbound traffic.
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux HECSs through SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows HECSs through RDP.

Copyright © Huawei Technologies Co., Ltd.

8.3 Security Group Configuration Examples

This section describes common security group configuration examples. These examples allow all outgoing data packets by default and only describe how to configure the inbound rules of a security group.

- Enabling HECSs in Different Security Groups to Communicate with Each Other Through an Internal Network
- Enabling Specified IP Addresses to Remotely Access HECSs in a Security Group
- Remotely Access a Linux HECS Using SSH
- Remotely Access a Windows HECS Using RDP
- Pinging an HECS from the Internet
- Enabling an HECS to Function as a Web Server
- Enabling an HECS to Function as a DNS Server
- Uploading or Downloading Files Using FTP

Enabling HECSs in Different Security Groups to Communicate with Each Other Through an Internal Network

- Example scenario

  Resources on an HECS in a security group need to be copied to an HECS associated with another security group, and the two HECSs are in the same VPC. We recommend that you enable internal network communication between the HECSs and then copy the resources.

- Security group configuration

  Within a given VPC, HECSs in the same security group can communicate with one another by default. However, HECSs in different security groups cannot communicate with each other by default. To enable these ECSs to communicate with each other, you need to add certain security group rules.

  You can add an inbound rule to the security groups containing the HECSs to allow access from HECSs in the other security group. The required rule is as follows.

Table 8-2 Used for communication through an internal network

Direction	Protocol/Application	Port	Source
Inbound	Protocol used for intranet interworking	Port or port range	ID of the other security group

Enabling Specified IP Addresses to Remotely Access HECSs in a Security Group

- Example scenario

  To prevent HECSs from being attacked, you can change the port number for remote login and configure security group rules that allow only specified IP addresses to remotely access the HECSs.

 Copyright © Huawei Technologies Co., Ltd.

- Security group configuration

  To allow IP address **192.168.20.2** to remotely access Linux HECSs in a security group over SSH and port 22, you can configure the following security group rule.

Table 8-3 Port 22

Direction	Protocol/Application	Port	Source
Inbound	SSH	22	IPv4 CIDR block or ID of another security group For example, 192.168.20.2/32

Remotely Access a Linux HECS Using SSH

- Example scenario

  After creating a Linux HECS, you can add a security group rule to enable remote SSH access to the HECS.

  NOTE

  The default security group comes with this rule. You do not need to configure the rule again if you use the group.

- Security group configuration

Direction	Protocol/Application	Port	Source
Inbound	SSH	22	0.0.0.0/0

Remotely Access a Windows HECS Using RDP

- Example scenario

  After creating a Windows HECS, you can add a security group rule to enable remote RDP access to the HECS.

  NOTE

  The default security group comes with the following rule. If you use the default security group, you do not need to add this rule again.

- Security group configuration

Direction	Protocol/Application	Port	Source
Inbound	RDP	3389	0.0.0.0/0

Pinging an HECS from the Internet

- Example scenario

 Copyright © Huawei Technologies Co., Ltd.

After creating HECSs, you need to add a security group rule so that you can run the **ping** command to test communication between the HECSs.

- Security group configuration

Direction	Protocol/Application	Port	Source
Inbound	ICMP	All	0.0.0.0/0

Enabling an HECS to Function as a Web Server

- Example scenario

  If you deploy a website on your HECS and require that your website be accessed over HTTP or HTTPS, you can add rules to the security group used by the HECS that functions as a web server.

- Security group configuration

Direction	Protocol/Application	Port	Source
Inbound	HTTP	80	0.0.0.0/0
Inbound	HTTPS	443	0.0.0.0/0

Enabling an HECS to Function as a DNS Server

- Example scenario

  If you need to use an HECS as a DNS server, you must enable TCP and UDP access from port 53 to the DNS server. You can add the following rules to the security group associated with the HECS.

- Security group configuration

Direction	Protocol/Application	Port	Source
Inbound	TCP	53	0.0.0.0/0
Inbound	UDP	53	0.0.0.0/0

Uploading or Downloading Files Using FTP

- Example scenario

  If you want to use FTP to upload files to or download files from HECSs, you must add a security group rule.

  NOTE

  You must first install the FTP server program on the HECSs and check whether ports 20 and 21 are working properly. For instructions on how to install the FTP server program, see Setting Up an FTP Site (Windows) or Setting Up an FTP Site (Linux).

 Copyright © Huawei Technologies Co., Ltd.

- Security group configuration

Direction	Protocol/Application	Port	Source
Inbound	TCP	20-21	0.0.0.0/0

8.4 Configuring Security Group Rules

Scenarios

Similar to a firewall, a security group is a logical group used to control network access. You can define access rules for a security group to protect the HECSs that are added to this security group.

- Inbound: Inbound rules allow external network data to be sent to the HECSs in the security group.
- Outbound: Outbound rules allow network traffic from the HECSs in the security group to be sent out of the security group.

For details about the default security group rules, see Default Security Groups and Security Group Rules. For details about configuration examples for security group rules, see 8.3 Security Group Configuration Examples.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. On the **Hyper Elastic Cloud Server** page, click the name of the target HECS.
   The page providing details about the HECS is displayed.
5. Click the **Security Groups** tab and then . View security group rules.
6. Click the security group ID.
   The system automatically switches to the **Security Group** page.
7. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters.
   You can click + to add more inbound rules.

Table 8-4 Inbound rule parameters

Parameter	Description	Example Value
Protocol & Port	Specifies the network protocol. Example values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.	Custom TCP
	Port: specifies the port or port range over which data can	22 or 22-30

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
	reach your HECS. The value ranges from 1 to 65535. For details about common ports, see Common Ports.	
Source	Specifies the source of the security group rule. The value can be another security group or a single IP address. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (subnet CIDR block) • 0.0.0.0/0 (any IP address)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

8. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters.

   You can click + to add more outbound rules.

Figure 8-2 Add Outbound Rule

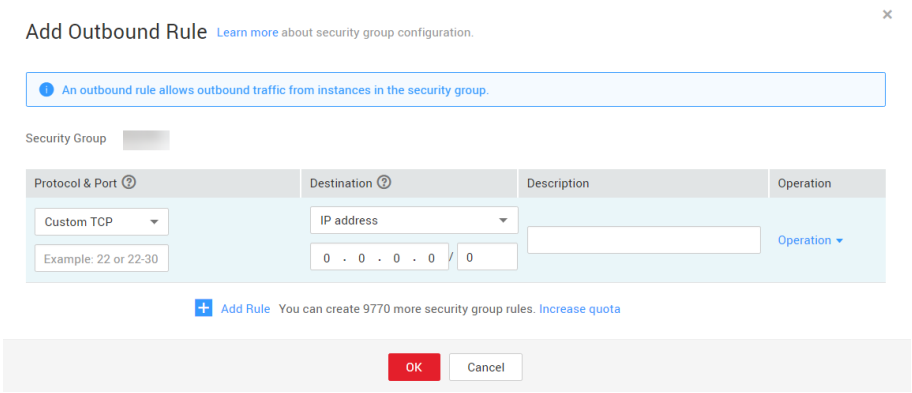


Table 8-5 Outbound rule parameters

Parameter	Description	Example Value
Protocol & Port	Specifies the network protocol. Example values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.	Custom TCP
	Port: specifies the port or port range over which data can leave your HECS. The value ranges from 1 to 65535. For details about common ports, see Common Ports.	22 or 22-30
Source	Specifies the source of the security group rule. The value can be another security group or a single IP address. For example:	0.0.0.0/0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
	• xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (subnet CIDR block) • 0.0.0.0/0 (any IP address)	
Description	Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

9. Click **OK** to complete the security rule configuration.

Verifying Configurations

After adding the security group rules, you can check whether the rules have taken effect. For example, you have deployed a website on an HECS. Users need to access your website over HTTP and port 80, and you have added the security group rule shown in Table 8-6.

Table 8-6 Security group rule

Direction	Protocol/Application	Port	Source
Inbound	TCP	80	0.0.0.0/0

Linux

To verify the security group rule on a Linux HECS:

1. Log in to the HECS.
2. Run the following command to check whether TCP port 80 is listened:

   netstat -an | grep 80

   If command output shown in Figure 8-3 is displayed, TCP port 80 is listened.

   Figure 8-3 Command output for the Linux HECS

   ```
   tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
   ```

3. Enter **http://***EIP bound to the HECS* in the address box of the browser and press **Enter**.

   If the requested page can be accessed, the security group rule has taken effect.

 Copyright © Huawei Technologies Co., Ltd.

8.5 Changing a Security Group

Scenarios

To change the security group of an HECS NIC, perform the operations described in this section.

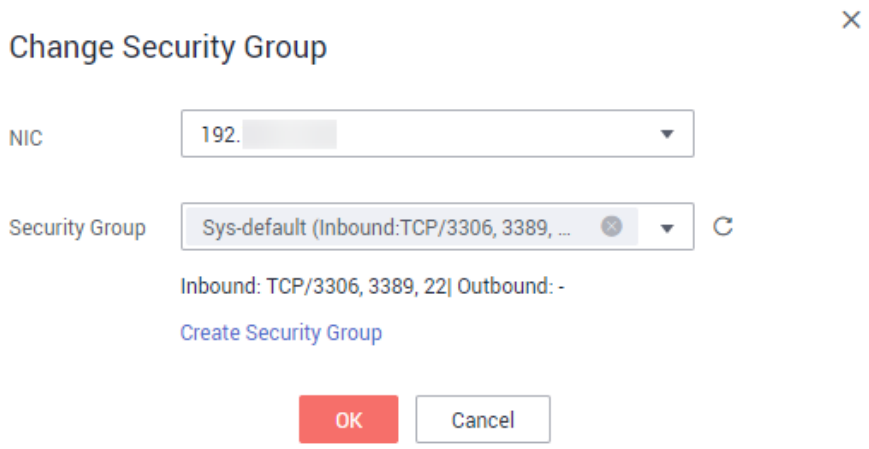
Procedure

1. Log in to the management console.
2. Under **Computing**, click **Halo ECS**.
3. On the **Hyper Elastic Cloud Server** page, click the name of the target HECS.

   The page providing details about the HECS is displayed.
4. Click the **Security Groups** tab. Then, click **Change Security Group**.

   The **Change Security Group** dialog box is displayed.

   Figure 8-4 Change Security Group



5. Select the target NIC and security group as prompted.

   You can select multiple security groups. In this case, the access rules of all the selected security groups apply on the HECS. To create a security group, click **Create Security Group**.

   NOTE

   Using multiple security groups may deteriorate HECS network performance. You are recommended to select no more than five security groups.
6. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

9 Host Security Service

What Is Host Security Service?

Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

After installing the HSS agent on your HECSs, you will be able to check the HECS security status and risks in a region on the HSS console.

How Do I Use HSS?

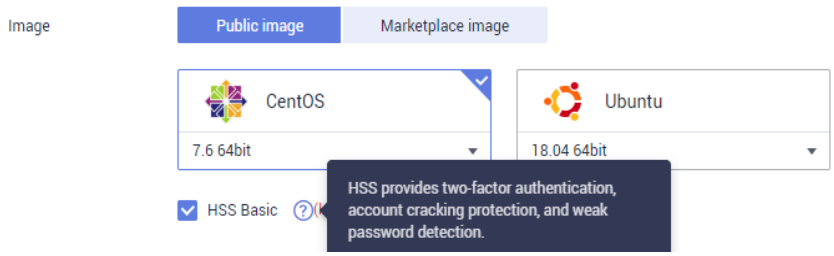
Before using the HSS service, install the HSS agent on your HECS. You can install the agent when creating an HECS, or install the agent on existing HECSs. Specific methods are described as follows:

- Scenario 1: Installing an Agent During HECS Creation

  When creating an HECS, if you enable the basic host security edition for the selected image, the system will automatically install the agent on the HECS and provide basic protection functions for your HECS.

  If the basic edition does not meet your requirements, you can purchase HSS quota in other editions. (You do not need to install the agent again.)

  Figure 9-1 Selecting HSS Basic

- Scenario 2: Installing an Agent on Existing HECSs

  To enable HSS on an existing HECS, manually install the agent on it.

  For details, see Installing an Agent and Enabling Server Protection.

 Copyright © Huawei Technologies Co., Ltd.

How Do I Check the Security Status of HECSs?

On the HECS list page, you can view the security status of HECSs in the current region.

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. In the HECS list, view the security status of HECSs in the **Security Status** column.
   - Agent not installed: The agent is not installed, or the agent is installed but not enabled. If you want to install the agent, refer to Installing an Agent.

     (The security status of a newly purchased HECS may be **Agent not installed**, which is because the agent is being installed. Please check later.)
   - Risky: The HECS is risky.
   - Safe: No risk is found in the HECS.
   - Not scanned: Host security is not enabled for the HECS. For details about how to enable HSS, see Enable Server Protection.
4. Click the name of an HECS. The page providing details about the HECS is displayed.

   Choose **Summary** > **Security and Monitor** to view the agent status and protection status.

For more information about HSS, see Host Security Service.

 Copyright © Huawei Technologies Co., Ltd.

10 Resources and Tags

10.1 Quota Adjustment

What Is Quota?

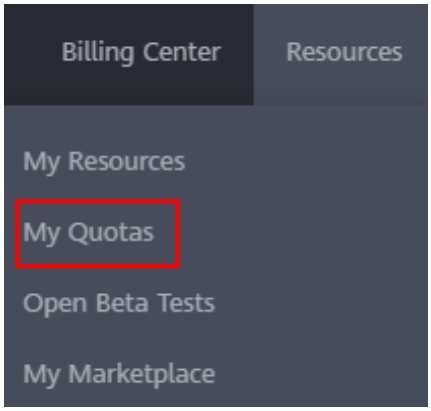
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 10-1 My Quotas

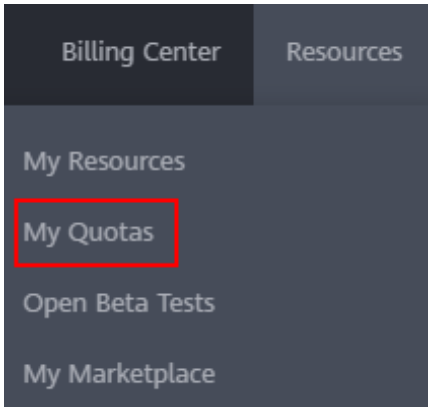
4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

 Copyright © Huawei Technologies Co., Ltd.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 10-2 My Quotas

3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.
   In **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

 Copyright © Huawei Technologies Co., Ltd.

11 Monitoring

11.1 Monitoring HECSs

Monitoring is the key to ensuring HECS performance, reliability, and availability. Using monitored data, you can determine HECS resource usage. HUAWEI CLOUD provides Cloud Eye to help you insight into the running statuses of your HECSs. You can use Cloud Eye to automatically monitor HECSs in real time and manage alarms and notifications to keep track of HECS performance.

Server Monitoring includes **Basic Monitoring** and **OS Monitoring**.

- **Basic Monitoring** automatically reports HECS metrics to Cloud Eye.
- **OS Monitoring** provides system-wide, active, and fine-grained HECS monitoring using the Agent installed on the target HECS.

  For instructions on how to install and configure the Agent, see Server Monitoring.

This section covers the following content:

- 11.2 Basic HECS Metrics
- 11.3 OS Monitoring Metrics Supported by HECSs with the Agent Installed
- 11.4 OS Monitoring Metrics Supported by HECSs with the New Edition of Agent Installed
- 11.5 Setting Alarm Rules
- 11.6 Viewing HECS Metrics

11.2 Basic HECS Metrics

Description

This section describes monitoring metrics reported by HECS to Cloud Eye and their namespaces. You can use Cloud Eye to view these metrics and alarms generated for HECSs.

Namespace

SYS.ECS

 Copyright © Huawei Technologies Co., Ltd.

HECS Metrics

HECS metrics vary depending on HECS OSs and types. For details, see Table 11-1. √ indicates that the metric is supported, and x indicates that the metric is not supported.

Table 11-1 HECS metrics

Metric	Windows	Linux
CPU Usage	√	√
Memory Usage	√	x (Agent must be installed on the HECS. Otherwise, this metric is unavailable.)
Disk Usage	√	x (Agent must be installed on the HECS. Otherwise, this metric is unavailable.)
Disk Read Bandwidth	√	√
Disk Write Bandwidth	√	√
Disk Read IOPS	√	√
Disk Write IOPS	√	√
Inband Incoming Rate	√	x (Agent must be installed on the HECS. Otherwise, this metric is unavailable.)
Inband Outgoing Rate	√	x (Agent must be installed on the HECS. Otherwise, this metric is unavailable.)
Outband Incoming Rate	√	√
Outband Outgoing Rate	√	√

NOTE

- Certain HECS metrics require the installation of VMTools on the image, based on which the HECS is created. For instructions on how to install VMTools, see https://github.com/UVP-Tools/UVP-Tools/.
- Certain HECS metrics require the installation of the Agent on the HECS. When the Agent is installed, log in to the management console and choose **Cloud Eye** under **Management & Deployment**. Then, view HECS metrics, such as **AGT. User Space CPU Usage**, by choosing **HECS Monitoring** > Target HECS > **OS Monitoring**. For details, see 11.3 OS Monitoring Metrics Supported by HECSs with the Agent Installed.
- For instructions on how to install the Agent on a Windows HECS, see Installing and Configuring the Agent (Windows).
- For instructions on how to install the Agent on a Linux HECS, see Installing and Configuring the Agent (Linux).

Table 11-2 describes these HECS metrics.

The monitoring intervals for the following HECSs with raw monitoring metrics are 5 minutes long.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-2 HECS metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
cpu_util	CPU Usage	CPU usage of an HECS This metric is used to show the CPU usage of the physical server accommodating the monitored HECS, which is not as accurate as the CPU usage obtained on the monitored HECS. For details, see Details. Unit: percent Formula: CPU usage of an HECS/Number of vCPUs in the HECS	≥ 0	HECS	5 minutes
mem_util	Memory Usage	Memory usage of an HECS This metric is unavailable if the image has no VMTools installed. Unit: percent Formula: Used memory of an HECS/Total memory of the HECS	≥ 0	HECS	5 minutes
disk_util_inband	Disk Usage	Disk usage of an HECS This metric is unavailable if the image has no VMTools installed. Unit: percent Formula: Used capacity of an HECS disk/Total capacity of the HECS disk	≥ 0	HECS	5 minutes
disk_read_bytes_rate	Disk Read Bandwidth	Number of bytes read from an HECS disk per second Unit: byte/s Formula: Total number of bytes read from an HECS disk/Monitoring interval byte_out = (rd_bytes - last_rd_bytes)/Time difference	≥ 0	HECS	5 minutes
disk_write_bytes_rate	Disk Write Bandwidth	Number of bytes written to an HECS disk per second Unit: byte/s Formula: Total number of bytes written to an HECS disk/Monitoring interval	≥ 0	HECS	5 minutes
disk_read_re	Disk	Number of read requests sent to an	≥ 0	HECS	5 minutes

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
quests_rate	Read IOPS	HECS disk per second Unit: request/s Formula: Total number of read requests sent to an HECS disk/Monitoring interval req_out = (rd_req - last_rd_req)/Time difference			
disk_write_requests_rate	Disk Write IOPS	Number of write requests sent to an HECS disk per second Unit: request/s Formula: Total number of write requests sent to an HECS disk/Monitoring interval req_in = (wr_req - last_wr_req)/Time difference	≥ 0	HECS	5 minutes
network_incoming_bytes_rate_inband	Inband Incoming Rate	Number of incoming bytes on an HECS per second Unit: byte/s Formula: Total number of inband incoming bytes on an HECS/Monitoring interval	≥ 0	HECS	5 minutes
network_outgoing_bytes_rate_inband	Inband Outgoing Rate	Number of outgoing bytes on an HECS per second Unit: byte/s Formula: Total number of inband outgoing bytes on an HECS/Monitoring interval	≥ 0	HECS	5 minutes
network_incoming_bytes_aggregate_rate	Outband Incoming Rate	Number of incoming bytes on an HECS per second on the hypervisor Unit: byte/s Formula: Total number of outband incoming bytes on an HECS/Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	HECS	5 minutes
network_outgoing_bytes_aggregate_rate	Outband Outgoing Rate	Number of outgoing bytes on an HECS per second on the hypervisor Unit: byte/s Formula: Total number of outband outgoing bytes on an	≥ 0	HECS	5 minutes

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
		HECS/Monitoring interval This metric is unavailable if SR-IOV is enabled.			
network_vm_connections	Network connections	Total number of TCP and UDP connections to an HECS Unit: count	≥ 0	HECS	5 minutes

Dimensions

Key	Value
instance_id	Specifies the HECS ID.

11.3 OS Monitoring Metrics Supported by HECSs with the Agent Installed

Description

After installing the Agent on an HECS, you can view its OS monitoring metrics. Monitoring data is collected every minute.

CPU, CPU load, memory, disk, disk I/O, file system, and NIC metrics can be monitored.

OS Monitoring Metrics

After the Agent is installed, you can view the metrics listed in the following table by default, regardless of HECS types and OSs.

Table 11-3 CPU metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage_idle	(Agent) Idle CPU Usage	Percentage of time that CPU is idle Unit: percent • Linux: Check the metric value changes in the file	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		/proc/stat in a collection period. • Windows: Run the **top** command to check the **%Cpu(s) id** value.			
cpu_usage_other	(Agent) Other Process CPU Usage	Percentage of time that the CPU is used by other processes Unit: percent • Linux: **Other Process CPU Usage** = 1- **Idle CPU Usage** - **Kernel Space CPU Usage** - **User Space CPU Usage** • Windows: **Other Process CPU Usage** = 1- **Idle CPU Usage** - **Kernel Space CPU Usage** - **User Space CPU Usage**	0–100%	HECS	1 minute
cpu_usage_system	(Agent) Kernel Space CPU Usage	Percentage of time that the CPU is used by kernel space Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s) sy** value. • Windows: Obtain the metric value using the Windows API **GetSystemTimes**.	0–100%	HECS	1 minute
cpu_usage_user	(Agent) User Space CPU Usage	Percentage of time that the CPU is used by user space Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s) us** value. • Windows: Obtain the metric value using the Windows API	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		GetSystemTimes.			
cpu_usage	(Agent) CPU Usage	CPU usage of the monitored object Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s)** value. • Windows: Obtain the metric value using the Windows API **GetSystemTimes**.	0–100%	HECS	1 minute
cpu_usage_nice	(Agent) Nice Process CPU Usage	Percentage of time that the CPU is in user mode with low-priority processes which can easily be interrupted by higher-priority processes Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s) ni** value. • Windows is not supported.	0–100%	HECS	1 minute
cpu_usage_iowait	(Agent) iowait Process CPU Usage	Percentage of time that the CPU is waiting for I/O operations to complete Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s) wa** value. • Windows does not support this metric.	0–100%	HECS	1 minute
cpu_usage_irq	(Agent) CPU Interrupt	Percentage of time that the CPU is serving interrupts Unit: percent	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
	Time	• Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s) hi** value. • Windows does not support this metric.			
cpu_usage_softirq	(Agent) CPU Software Interrupt Time	Percentage of time that the CPU is serving software interrupts Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s) si** value. • Windows does not support this metric.	0–100%	HECS	1 minute

Table 11-4 CPU load metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
load_average1	(Agent) 1-Minute Load Average	CPU load averaged over the last 1 minute Linux: Obtain the metric value from the number of logic CPUs in **load1/** in the file **/proc/loadavg**. Run the **top** command to check the **load1** value.	≥ 0	HECS	1 minute
load_average5	(Agent) 5-Minute Load Average	CPU load averaged over the last 5 minutes Linux: Obtain the metric value from the number of logic CPUs in **load5/** in the file **/proc/loadavg**. Run the **top** command to check the	≥ 0	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		load5 value.			
load_average15	(Agent) 15-Minute Load Average	CPU load averaged over the last 15 minutes Linux: Obtain the metric value from the number of logic CPUs in **load15/** in the file **/proc/loadavg**. Run the **top** command to check the **load15** value.	≥ 0	HECS	1 minute

NOTE

The Windows OS does not support the CPU load metrics.

Table 11-5 Memory metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mem_available	(Agent) Available Memory	Amount of memory that is available and can be given instantly to processes Unit: GB • Linux: Obtain the metric value from **MemAvailable** in file **/proc/meminfo**. If **MemAvailable** is not available in **/proc/meminfo**, it is equal to **MemFree**+**Buffers**+**Cached**. • Windows: calculated by subtracting used memory from available memory. The value is obtained by calling the Windows API GlobalMemoryStatusEx.	≥ 0 GB	HECS	1 minute
mem_usedPercent	(Agent) Memory	Memory usage of the monitored object	0–100 %	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
	Usage	Unit: percent • Linux: Obtain the metric value from the **/proc/meminfo** file (**MemTotal-MemAvailable)/MemTotal**. • Windows: The calculation formula is as follows: Used memory size/Total memory size*100%.			
mem_free	(Agent) Idle Memory	Amount of memory that is not being used Unit: GB • Linux: Obtain the metric value from **/proc/meminfo**. • Windows does not support this metric.	≥ 0 GB	HECS	1 minute
mem_buffers	(Agent) Buffer	Amount of memory that is being used for buffers Unit: GB • Linux: Obtain the metric value from **/proc/meminfo**. Run the **top** command to check the **KiB Mem:buffers** value. • Windows does not support this metric.	≥ 0 GB	HECS	1 minute
mem_cached	(Agent) Cache	Amount of memory that is being used for file caches Unit: GB • Linux: Obtain the metric value from **/proc/meminfo**. Run the **top** command to check the **KiB Swap:cached Mem** value. • Windows does not support this metric.	≥ 0 GB	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Table 11-6 Disk metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_free	(Agent) Available Disk Space	Free space on the disks Unit: GB • Linux: Run the **df -h** command to check the value in the **Avail** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	≥ 0 GB	HECS	1 minute
mountPointPrefix_disk_total	(Agent) Disk Storage Capacity	Total space on the disks, including used and free space Unit: GB • Linux: Run the **df -h** command to check the value in the **Size** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the	≥ 0 GB	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).			
mountPointPrefix_disk_used	(Agent) Used Disk Space	Used space on the disks Unit: GB • Linux: Run the **df -h** command to check the value in the **Used** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	≥ 0 GB	HECS	1 minute
mountPointPrefix_disk_usedPercent	(Agent) Disk Usage	Percentage of total disk space that is used. It is calculated as follows: **Disk Usage** = **Used Disk Space**/**Disk Storage Capacity**. Unit: percent • Linux: calculated as follows: Used/Size. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters,	0–100%	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		hyphens (-), dots (.), and swung dashes (~). • Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).			

Table 11-7 Disk I/O metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_agt_read_bytes_rate	(Agent) Disks Read Rate	Number of bytes read from the monitored disk per second Unit: byte/s • Linux: The disk read rate is calculated based on the data changes in the sixth column of the corresponding device in the file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: – Use the	≥ 0 bytes/s	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data. – The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). – When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data.			
mountPointPrefix_disk_agt_read_requests_rate	(Agent) Disks Read Requests	Number of read requests sent to the monitored disk per second Unit: request/s • Linux: The disk read requests are calculated based on the data changes in the fourth column of the corresponding device in the file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: – Use the Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the	≥ 0 Requests/s	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		WMI to obtain disk I/O data. – The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). – When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data.			
mountPointPrefix_disk_agt_write_bytes_rate	(Agent) Disks Write Rate	Number of bytes written to the monitored disk per second Unit: byte/s • Linux: The disk write rate is calculated based on the data changes in the tenth column of the corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: – Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data.	≥ 0 bytes/s	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		– The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). – When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data.			
mountPointPrefix_disk_agt_write_requests_rate	(Agent) Disks Write Requests	Number of write requests sent to the monitored disk per second Unit: request/s • Linux: The disk write requests are calculated based on the data changes in the eighth column of the corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: – Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data. – The path of the mount point prefix cannot exceed 64 characters.	≥ 0 Requests/s	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). – When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data.			
disk_readTime	(Agent) Average Read Request Time	Average amount of time that read requests have waited on the disks Unit: ms/count • Linux: The average read request time is calculated based on the data changes in the seventh column of the corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.	≥ 0 ms/count	HECS	1 minute
disk_writeTime	(Agent) Average Write Request Time	Average amount of time that write requests have waited on the disks Unit: ms/count • Linux: The average write request time is calculated based on the data changes in the eleventh column of the	≥ 0 ms/count	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.			
disk_ioUtils	(Agent) Disk I/O Usage	Percentage of the time that the disk has had I/O requests queued to the total disk operation time Unit: percent • Linux: The disk I/O usage is calculated based on the data changes in the thirteenth column of the corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.	0–100%	HECS	1 minute
disk_queue_length	(Agent) Disk Queue Length	Average number of read or write requests queued up for completion for the monitored disk in the monitoring period Unit: count • Linux: The average disk queue	≥ 0 counts	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		length is calculated based on the data changes in the fourteenth column of the corresponding device in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.			
disk_write_bytes_per_operation	(Agent) Average Disk Write Size	Average number of bytes in an I/O write for the monitored disk in the monitoring period Unit: byte/op • Linux: The average disk write size is calculated by using the data changes in the tenth column of the corresponding device to divide that of the eighth column in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.	≥ 0 ms/op	HECS	1 minute
disk_read_bytes_per_operation	(Agent) Average Disk Read Size	Average number of bytes in an I/O read for the monitored disk in the monitoring period	≥ 0 KB/op	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		Unit: byte/op • Linux: The average disk read size is calculated by using the data changes in the sixth column of the corresponding device to divide that of the fourth column in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.			
disk_io_svctm	(Agent) Disk I/O Service Time	Average time in an I/O read or write for the monitored disk in the monitoring period Unit: ms/op • Linux: The average disk I/O service time is calculated by using the data changes in the thirteenth column of the corresponding device to divide the sum of data changes in the fourth and eighth columns in file **/proc/diskstats** in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes	≥ 0 ms/op	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		(~). • Windows does not support this metric.			

Table 11-8 File system metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_fs_rwstate	(Agent) File System Read/Write Status	Read and write status of the mounted file system of the monitored object Possible values are **0** (read and write) and **1** (read only). Linux: Check file system information in the fourth column in the file **/proc/mounts**.	0, 1	HECS	1 minute
disk_inodesTotal	(Agent) Disk inode Total	Total number of index nodes on the disk Linux: Run the **df -i** command to check the value in the **Inodes** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	≥ 0	HECS	1 minute
disk_inodesUsed	(Agent) Total inode Used	Number of used index nodes on the disk Linux: Run the **df -i** command to check the value in the **IUsed** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes	≥ 0	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		(~).			
disk_inodesUsedPercent	(Agent) Percentage of Total inode Used	Number of used index nodes on the disk Unit: percent Linux: Run the **df -i** command to check the value in the **IUse%** column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	0–100%	HECS	1 minute

NOTE

Windows does not support these metrics.

Table 11-9 NIC metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
net_bitRecv	(Agent) Outbound Bandwidth	Number of bits sent by the target NIC per second Unit: bit/s • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI MibIfRow object.	≥ 0 bits/s	HECS	1 minute
net_bitSent	(Agent) Inbound Bandwidth	Number of bits received by the target NIC per second Unit: bit/s • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period.	≥ 0 bits/s	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		• Windows: Obtain the metric value using the WMI MibIfRow object.			
net_packetRecv	(Agent) NIC Packet Receive Rate	Number of packets received by the target NIC per second Unit: count/s • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI MibIfRow object.	≥ 0 counts/s	HECS	1 minute
net_packetSent	(Agent) NIC Packet Send Rate	Number of packets sent by the target NIC per second Unit: count/s • Linux: Check metric value changes in file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI MibIfRow object.	≥ 0 counts/s	HECS	1 minute
net_errin	(Agent) Receive Error Rate	Percentage of receive errors detected by the target NIC per second Unit: percent • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows does not support this metric.	0–100%	HECS	1 minute
net_errout	(Agent) Transmit Error Rate	Percentage of transmit errors detected by the target NIC per second Unit: percent • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period.	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		• Windows does not support this metric.			
net_dropin	(Agent) Received Packet Drop Rate	Percentage of packets received by this NIC which were dropped per second Unit: percent • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows does not support this metric.	0–100%	HECS	1 minute
net_dropout	(Agent) Transmitted Packet Drop Rate	Percentage of packets transmitted by this NIC which were dropped per second Unit: percent • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows does not support this metric.	0–100%	HECS	1 minute

Table 11-10 Process metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
proc_pHashId_cpu	CPU Usage	CPU consumed by a process. **pHashId** (process name and process ID) is the value of **md5**. Unit: percent • Linux: Check the metric value changes in file **/proc/pid/stat**. • Windows: Call the Windows API GetProcessTimes to	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		obtain the CPU usage of the process.			
proc_pHashId_mem	Memory Usage	Memory consumed by a process. **pHashId** (process name and process ID) is the value of **md5**. Unit: percent • Linux: RSS*PAGESIZE/MemTotal Obtain the **RSS** value by checking the second column of file **/proc/pid/statm**. Obtain the **PAGESIZE** value by running the **getconf PAGESIZE** command. Obtain the **MemTotal** value by checking file **/proc/meminfo**. • Windows: Call the Windows API procGlobalMemoryStatusEx to obtain the total memory size. Call GetProcessMemoryInfo to obtain the used memory size. Use the used memory size to divide the total memory size to get the memory usage.	0–100%	HECS	1 minute
proc_pHashId_file	Opened Files	Number of files opened by a process. **pHashId** (process name and process ID) is the value of **md5**. • Linux: Run the **ls -l /proc/pid/fd** command to view the number of opened files. • Windows does not support this metric.	≥ 0	HECS	1 minute
proc_run	Running	Number of processes that	≥ 0	HECS	1

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
ning_count	Processes	are running • Linux: You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Windows does not support this metric.			minute
proc_idle_count	Idle Processes	Number of processes that are idle • Linux: You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Windows does not support this metric.	≥ 0	HECS	1 minute
proc_zombie_count	Zombie Processes	Number of zombie processes • Linux: You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Windows does not support this metric.	≥ 0	HECS	1 minute
proc_blocked_count	Blocked Processes	Number of processes that are blocked • Linux: You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in	≥ 0	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		each state. • Windows does not support this metric.			
proc_sleeping_count	Sleeping Processes	Number of processes that are sleeping • Linux: You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Windows does not support this metric.	≥ 0	HECS	1 minute
proc_total_count	Total Processes	Total number of processes on the monitored object • Linux: You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Windows: Obtain the total number of processes by using the system process status support module **psapi.dll**.	≥ 0	HECS	1 minute

Dimension

Key	Value
instance_id	HECS ID

 Copyright © Huawei Technologies Co., Ltd.

11.4 OS Monitoring Metrics Supported by HECSs with the New Edition of Agent Installed

Description

This section describes the OS metrics supported by HECSs. In the following regions, the agent of the latest version is used with simplified monitoring metrics.

CN East-Shanghai1, CN East-Shanghai2, CN North-Beijing1, CN North-Beijing4, CN South-Guangzhou, CN South-Shenzhen, and CN Southwest-Guiyang1

After installing the Agent on an HECS, you can view its OS monitoring metrics. Monitoring data is collected every minute.

OS Monitoring Metrics

Table 11-11 OS monitoring metrics

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage	(Agent) CPU Usage	CPU usage of the monitored object Unit: percent • Linux: Check the metric value changes in the file **/proc/stat** in a collection period. Run the **top** command to check the **%Cpu(s)** value. • Windows: Obtain the metric value using the Windows API **GetSystemTimes**.	0–100%	HECS	1 minute
load_average5	(Agent) 5-Minute Load Average	CPU load averaged over the last 5 minutes • Linux: Obtain the metric value from the number of logic CPUs in **load5/** in the file **/proc/loadavg**. Run the **top** command to check the **load5** value. • The Windows OS does not support the CPU load metrics.	≥ 0	HECS	1 minute
mem_usedPercent	(Agent) Memory Usage	Memory usage of the monitored object Unit: percent	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		• Linux: Obtain the metric value from the **/proc/meminfo** file (**MemTotal-MemAvailable**)/**MemTotal**. • Windows: Obtain the value using the following formula: Used memory size/Total memory size x 100%.			
mountPointPrefix_disk_free	(Agent) Available Disk Space	Free disk space Unit: GB • Linux: Run the **df -h** command to check the value in the **Avail** column. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows: Obtain the metric value using the WMI API GetDiskFreeSpaceExW. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).	≥ 0 GB	HECS	1 minute
mountPointPrefix_disk_usedPercent	(Agent) Disk Usage	Percentage of total disk space that is used. It is calculated as follows: **Disk Usage** = **Used Disk Space**/**Disk Storage Capacity**. Unit: percent • Linux: Obtain the metric value using following formula: **Disk Usage** = **Used Disk Space**/**Disk Storage Capacity**. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits,	0–100%	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		letters, hyphens (-), dots (.), and swung dashes (~). • Windows: Obtain the metric value using the WMI API GetDiskFreeSpaceExW. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~).			
disk_ioUtils	(Agent) Disk I/O Usage	Percentage of the time that the disk has had I/O requests queued to the total disk operation time Unit: percent • Linux: Obtain the metric value by calculating the data changes in the thirteenth column of the monitored object in file **/proc/diskstats** in a collection period. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes (~). • Windows does not support this metric.	0–100%	HECS	1 minute
disk_inodesUsedPercent	(Agent) Percentage of Total inode Used	Number of used index nodes on the disk Unit: percent • Linux: Run the **df -i** command to check the value in the **IUse%** column. The path of the device name prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), dots (.), and swung dashes	0–100%	HECS	1 minute

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		(~). • Windows does not support this metric.			
net_bitSent	(Agent) Inbound Bandwidth	Number of bits received by the target NIC per second Unit: bit/s • Linux: Check metric value changes in file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI MibIfRow object.	≥ 0	HECS	1 minute
net_bitRecv	(Agent) Outbound Bandwidth	Number of bits sent by the target NIC per second Unit: bit/s • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI MibIfRow object.	≥ 0	HECS	1 minute
net_packetRecv	(Agent) NIC Packet Receive Rate	Number of packets received by the target NIC per second Unit: count/s • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI MibIfRow object.	≥ 0 counts/s	HECS	1 minute
net_packetSent	(Agent) NIC Packet Send Rate	Number of packets sent by the target NIC per second Unit: count/s • Linux: Check metric value changes in the file **/proc/net/dev** in a collection period. • Windows: Obtain the metric value using the WMI	≥ 0 counts/s	HECS	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
		MibIfRow object.			
net_tcp_total	(Agent) TCP TOTAL	Total number of TCP connections of the target NIC	≥ 0	HECS	1 minute
net_tcp_established	(Agent) TCP ESTABLISHED	Number of ESTABLISHED TCP connections of the target NIC	≥ 0	HECS	1 minute

Dimension

Key	Value
instance_id	HECS ID

11.5 Setting Alarm Rules

Scenarios

Setting HECS alarm rules allows you to customize the monitored objects and notification policies and determine the running statuses of your HECSs at any time.

This section describes how to set HECS alarm rules, including alarm rule names, monitoring objects, monitoring metrics, alarm thresholds, monitoring intervals, and notifications.

Setting Alarm Rules on the HECS Console

After an HECS is created, you can quickly configure alarm rules to monitor the CPU usage, memory usage, and disk usage.

1. Log in to the management console.
2. Under **Computing**, click **Hyper ECS**.
3. Locate the row containing the target HECS. Click **More** in the **Operation** column and select **Create Alarm Rule**.
4. Enable alarm rules as required.

   After an HECS is created, alarm rules are disabled by default. You need to manually enable them.
5. Set the threshold.

 Copyright © Huawei Technologies Co., Ltd.

The status of an alarm rule changes based on the threshold you set. Cloud Eye notifies you by sending emails, text messages, or by sending HTTP/HTTPS requests once the status of an alarm rule changes.

a. Select a threshold type.

b. Select an operator (≥, ≤, >, and <) and enter a threshold value.

6. Click **OK**.

   Wait for 5 to 10 minutes and click the **Monitoring** tab to view the monitoring data.

Setting Alarm Rules on the Cloud Eye Console

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Management & Deployment**, click **Cloud Eye**.
4. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** to create an alarm rule, or modify an existing alarm rule.

   The following operations use modifying an existing alarm rule as an example.

   a. Click the target alarm rule.

   b. Click **Modify** in the upper right corner of the page.

   c. On the **Modify Alarm Rule** page, set parameters as prompted.

   d. Click **OK**.

      When an alarm rule is modified, the system automatically notifies you when an alarm corresponding to the rule is generated.

NOTE

For more information about HECS alarm rules, see Introduction to Alarm Rules.

11.6 Viewing HECS Metrics

Scenarios

The public cloud platform provides Cloud Eye, which monitors the running statuses of your HECSs. You can obtain the monitoring metrics of each HECS on the management console.

Prerequisites

- The HECS is running properly.

  Cloud Eye does not display the monitoring data for a stopped, faulty, or deleted HECS. After such an HECS restarts or recovers, the monitoring data is available in Cloud Eye.

  NOTE

  Cloud Eye discontinues monitoring HECSs that remain in the **Stopped** or **Faulty** state for 24 hours and removes them from the monitoring list. However, the alarm rules for such HECSs are not automatically deleted.

- Alarm rules have been configured in Cloud Eye for the target HECS.

  The monitoring data is unavailable for the HECSs without alarm rules configured in Cloud Eye. For details, see 11.5 Setting Alarm Rules.

 Copyright © Huawei Technologies Co., Ltd.

- The target HECS has been properly running for at least 10 minutes.

  There is a short time delay between transmitting and displaying data from monitored metrics, so the Cloud Eye dashboard displays the status of the HECS over the last 5–10 minutes. You can obtain the monitored metrics of a newly created HECS 5–10 minutes later.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Computing**, click **Hyper ECS**.
4. In the search box above the upper right corner of the HECS list, enter the HECS name, IP address, or ID, and click  for search.
5. Click the name of the target HECS. The page providing details about the HECS is displayed.
6. Click the **Monitoring** tab to view the monitoring data.
7. In the HECS monitoring area, select a duration to view the monitoring data.

 Copyright © Huawei Technologies Co., Ltd.

12 Change History

Released On	Description
2021-01-06	This issue is the eighth official release. • Modified the supported regions in 11.4 OS Monitoring Metrics Supported by HECSs with the New Edition of Agent Installed.
2020-09-07	This issue is the seventh official release. • Added 1.5 Logging In to a Windows HECS from a Linux Server. • Optimized 1.1 Login Overview and 2.1 Login Overview.
2020-08-10	This issue is the sixth official release. • Added hecs_03_0066.xml.
2020-07-13	This issue is the fifth official release. • Added description about alarm rule configuration in 11.5 Setting Alarm Rules.
2020-04-30	This issue is the fourth official release. • Added 5.4 Detaching a Disk from an HECS. • Added 5.5 Expanding Disk Capacity. • Modified 5.6 Initializing a Windows Data Disk Using a Script.
2020-03-30	This issue is the third official release. • Added 1.3 Logging In to a Windows HECS Using an RDP File • Added 9 Host Security Service
2020-03-03	This issue is the second official issue. • Added 3.4 Changing an OS, describing the support for changing OSs using a private image. • Added 5.3 Attaching a Disk to an HECS, describing the support for attaching an available disk to an HECS. • Added 5.2 Adding Disks to an HECS, providing the list of parameters for purchasing disks.
2020-02-06	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.

 Copyright © Huawei Technologies Co., Ltd.