



*User Guide*

*Cloud Portal*

Version	Issue Date	Revision Description
2.0	2-Aug-2016	<ul style="list-style-type: none"><li>- Complete rewrite for new release of Service Portal</li></ul>
2.2	11-May-2017	<ul style="list-style-type: none"><li>- Add Section 7.5, 7.6, 7.7 for template, ISO and volume management</li><li>- Add Section 9 Monitoring guide</li></ul>

## Table of Contents

1	Overview .....	6
2	Getting Started .....	6
3	Cloud Portal .....	6
3.1	First time sign in.....	6
3.2	Sign in Cloud Portal .....	9
3.3	Forgot password .....	10
3.4	Using your Backup Code to Sign In .....	11
3.5	Set up 2FA on a new phone .....	12
4	Dashboard .....	15
4.1	User Profile .....	16
5	Launch .....	17
6	Instance .....	20
6.1	Listing all VMs .....	20
6.1.1	Change Grouping Display and Search.....	20
6.1.2	VM Operations on Instance Listing page .....	22
6.2	VM Details page .....	22
6.2.1	Overview Tab .....	23
6.2.2	Volumes Tab .....	25
6.2.3	VM Snapshot Tab.....	27
6.3	VM Operation .....	28
6.3.1	Stop VM.....	28
6.3.2	Start VM .....	29
6.3.3	Reboot VM .....	29
6.3.4	Terminate VM.....	30
6.3.5	Remote Console.....	32
6.3.6	Change VM Display Name.....	32
6.3.7	VM Password .....	33
6.3.8	Resize VM (Compute Offering).....	34
6.3.9	Manage VM Network Interface .....	35
6.3.10	Manage Volume.....	39
6.3.11	Manage VM Snapshot .....	44
6.3.12	Attach / Detach ISO .....	45
7	Resource.....	47
7.1	Resource Pools .....	47

7.2	Regions .....	47
7.3	Usage & Limits.....	47
7.4	Networking.....	48
7.4.1	VPC Network.....	48
7.4.2	Flat Network .....	61
7.4.3	Public IP .....	70
7.5	Templates.....	73
7.5.1	Upload Templates .....	73
7.5.2	Download Templates .....	74
7.5.3	Delete Templates .....	75
7.6	Volumes .....	75
7.7	ISOs .....	76
8	Settings.....	78
8.1	My User Profile .....	78
8.2	My Account.....	79
8.2.1	My Account - General .....	79
8.2.2	My Account - Preferences.....	79
8.3	Users.....	81
8.3.1	Add New User .....	81
9	Monitoring .....	84
9.1	Login the Monitoring tool.....	84
9.2	View your device information & detail .....	85
9.2.1	Launch more status & resource usage.....	85
9.2.2	View the performance data by chart .....	85
9.3	Manage your device monitoring setting.....	86
9.3.1	Edit the Device setting .....	86
9.3.2	Suspend device monitoring.....	88
9.4	Review or download historic data .....	89
9.5	Add report (Support html format only) .....	91
9.5.1	Create the report .....	92
9.5.2	Select Sensors Manually .....	96
9.6	Manage your saved report .....	97
9.6.1	View and run your saved report .....	97
9.6.2	Delete your report.....	98
9.6.3	Edit your report .....	99
9.6.4	Clone your report.....	100
9.7	VM resource warning /error status & email notification.....	101
9.7.1	Setup the warning /error status.....	101

9.7.2 Setup email notification.....103

## 1 Overview

HKBN Infinite Server Cloud Portal is an advanced cloud management platform which offers an easy-to-use experience for delivering self-service Infrastructure-as-a-Service to customers. Users can do all of the following through the Portal: manage their resource pools, perform VM operations, manage user accounts, setup roles & permissions, etc.

## 2 Getting Started

After subscribing Infinite Server service, customer's admin contact will receive an email with link and instruction to activate the account. After account activation, customer will receive a 'Welcome Email' with all the information of subscribed services including the login credential of the Cloud Portal, where customer can manage its cloud services.

All required VM & VAS on supplementary form submitted by customer, including VPC and vLANs, were pre-provisioned and ready for use when the welcome email is received. Customer could manage the subscribed cloud services anytime via the cloud portal when needed.

## 3 Cloud Portal

URL for Login: <https://iserver.hkbnes.net/>

Username: <Remark: Customer will receive this information in welcome email>

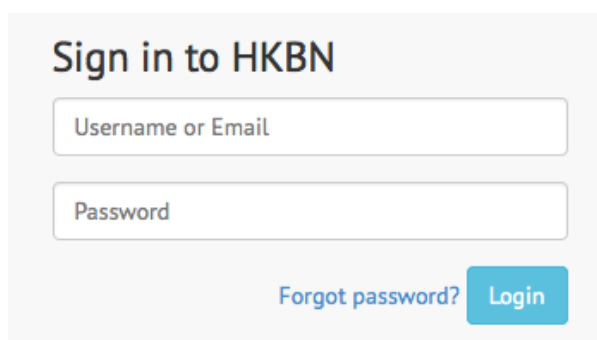
Password: <Remark: Customer will receive this information in welcome email>

2 Factor Authentication Token: <Remark: Customers will need to register their smartphone as 2 Factor Authentication token>

Note: For 2 factor authentication, users will need to install Google Authenticator App on their smart phone. Apple IOS, Andriod & Blackberry are supported.

### 3.1 First time sign in

1. Go to **Login** page.



The screenshot shows a login form titled "Sign in to HKBN". It contains two input fields: "Username or Email" and "Password". Below the "Password" field, there is a link "Forgot password?" and a blue "Login" button.

2. Enter your **Username** or **Email**.
3. Enter **Password**.
4. Click **Login** button.
5. If you have entered your Username and Password correctly, you should see the following screen to **enable Two-Step Verification**.

Home / My User Profile / Enable Two-Step Verification

Please enable Two step verification ✕

## Enable Two-Step Verification

Two-step verification adds an extra layer of protection to your account. Whenever you sign in to the system, you'll need to enter both your password and also a verification code. This verification code will be sent to your mobile device via text message or an authenticator app.

With Two-Step Verification enabled you will always need your password and one of the following to access your account:

- A verification code (via text message or an authenticator app)
- A backup code

**Warning**

If you are unable to provide a verification or backup code, you will lose access to your account.

How do you want to receive the verification code?

Google Authenticator App

Cancel, maybe next time.

6. **Google Authenticator App** is used for 2FA, click the **Google Authenticator App** button.
7. You should see the **Enable Two-Step Verification** page.

Home / My User Profile / Enable Two-Step Verification

## Enable Two-Step Verification

1. Install the App


For iOS

For Android

For Blackberry

2. Scan barcode below

Once in the app, tap the + button and scan the barcode with your phone camera.



3. Enter your code

Enter the 6-digit verification code generated by the Authenticator app in the box below.

Code

Submit

8. Install Google Authenticator App on your smart phone. For app installation procedure, please click the option corresponding to your mobile operating system.

## Apple Store

### Google Authenticator

[View More by This Developer](#)

By Google, Inc.

Open iTunes to buy and download apps.



[View in iTunes](#)

#### Description

Google Authenticator works with 2-Step Verification for your Google Account to provide an additional layer of security when signing in.

[Google, Inc. Web Site](#) [Google Authenticator Support](#)

[...More](#)

#### What's New in Version 2.1.0

- Includes a link to allow users to send anonymous feedback to Google
- Displays the website associated with a verification code (for websites that support this feature)
- Minor visual improvements

## Google Play Store

Google play

Search

Apps

Categories | Home | Top Charts | New Releases

My apps

Shop

Games

Editors' Choice

Google Authenticator

Google Inc. - December 12, 2013

Tools

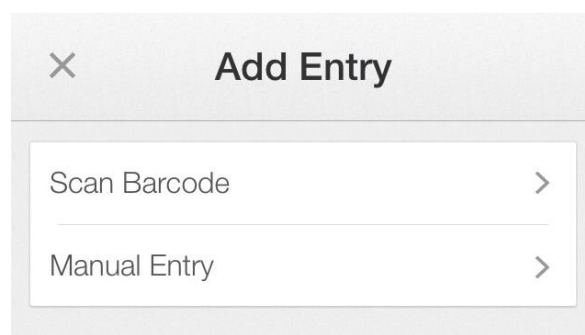
Install

Add to Wishlist

★★★★☆ (73,172)

Top Developer

9. Open your Google Authenticator App on your smart phone.
10. Use your Google Authenticator App to **scan the QR code** shown on the Enable Two-Step Verification page.





11. Enter the **6-digit code** generated by your Google Authenticator App. Please note that the code is refreshed in every 30 seconds.
12. Click **Submit** button.
13. If the code is correct, you will be redirected to the **Manage Two-Step Verification** page.

## Manage Two-Step Verification

### Two-step verification is **Enabled**

Each time you log in to HKBN with your username and password, you must enter a verification code displayed by **Google Authenticator**.

### Single-use Backup Codes

Backup codes allow you to access your account whenever you are unable to provide a verification code, which may happen if you are traveling or if you lose your mobile phone. Please print these backup codes or save them in a safe place. If you are unable to provide a verification code and you do not have a backup code, you will be unable to sign in to your account.

- GK873RXGWZ091TDK
- 59IUOWP1LR9LH6UQ
- QI2W19TFRI1P2JRS
- 79A1NOSTRO6W9QDB
- 1TNGFL6E1C9L0TKP

### Reset two-step verification

By clicking the below button, two-step verification will be reset. You may log in to the system with only username and password.

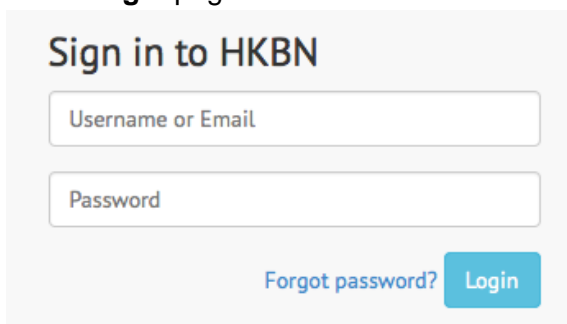
Reset two-step verification

14. In the Manage Two-Step Verification page, you should see 5 **Single-use Backup Codes**. Each backup-code can only be used for one time. These Backup Codes should be saved for emergencies, such as when you lose your phone and need to access to App360. After you have logged in, you can re-enable Two-Step Verification with your new phone.

**Notes :** In case you do not have your smartphone and the Single-use Backup Codes with you, please contact HKBN hotline 128180 to raise request for account reset.

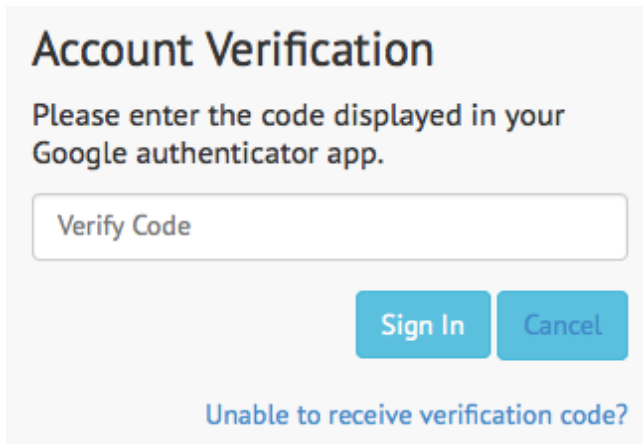
## 3.2 Sign in Cloud Portal

1. Go to **Login** page.



The screenshot shows the 'Sign in to HKBN' login form. It features two input fields: 'Username or Email' and 'Password'. Below the password field, there is a link for 'Forgot password?' and a blue 'Login' button.

2. Enter your **Username** or **Email**.
3. Enter **Password**.
4. Click **Login** button.
5. If you have entered your Username and Password correctly, you should see the following screen to **enter Account Verification code**.

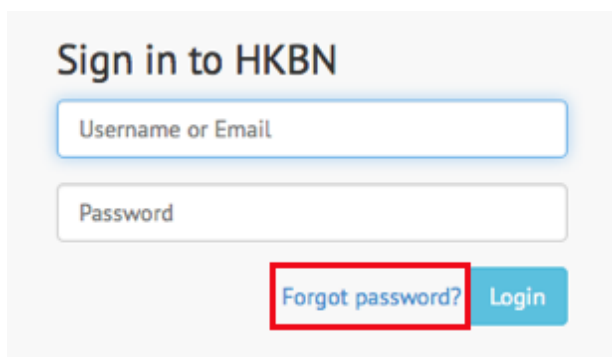


The screenshot shows a light gray box titled "Account Verification". Below the title, it says "Please enter the code displayed in your Google authenticator app." There is a text input field with the placeholder "Verify Code". Below the field are two blue buttons: "Sign In" and "Cancel". At the bottom of the box, there is a link that says "Unable to receive verification code?"

6. Enter the **6-digit code** generated by your Google Authenticator App. Please note that the code renews every 30 seconds.
7. Click **Sign In** button.
8. If the code is correct then you should see the **Dashboard** page.

### 3.3 Forgot password

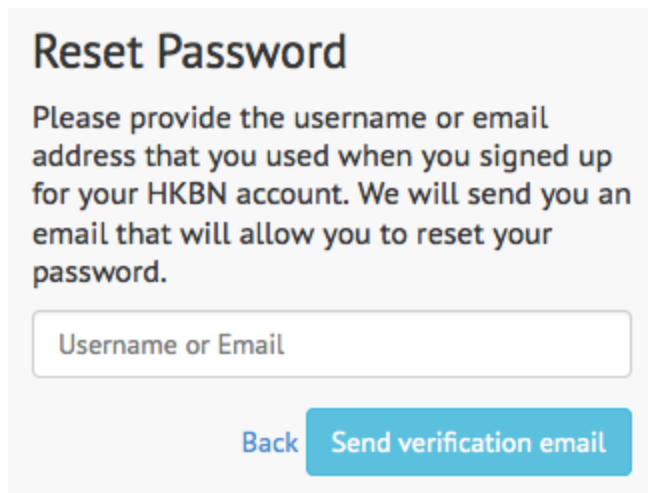
If you have forgotten your password, you can click the **Forgot password** link on the login page and follow the steps to reset your password.



The screenshot shows a light gray box titled "Sign in to HKBN". It contains two text input fields: "Username or Email" and "Password". Below the fields are two buttons: "Forgot password?" (highlighted with a red box) and "Login".

Reset Password steps:

1. Go to the **Login** page then click the **Forgot password** link.
2. You should see the **Reset Password** page. Please enter your **Username** or **Email** and click the **Send Verification email** button.

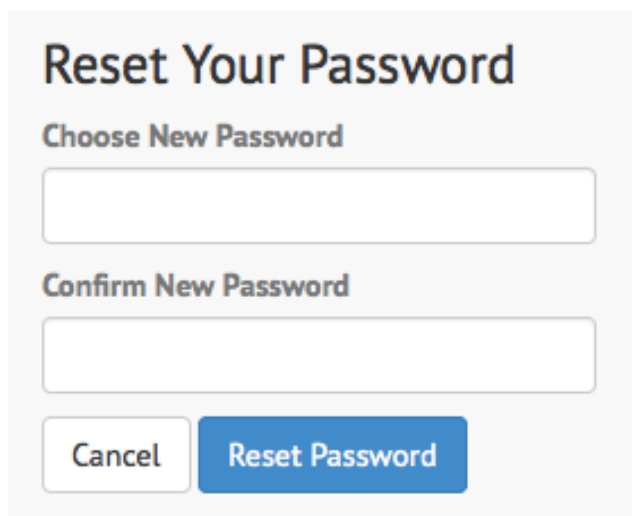


**Reset Password**

Please provide the username or email address that you used when you signed up for your HKBN account. We will send you an email that will allow you to reset your password.

[Back](#) [Send verification email](#)

3. After clicking the button, you should see a message showing that the Reset Password link has been sent to your email.
4. Check your email and click the **Reset Password** link.
5. Your browser will open the **Reset Your Password** page.



**Reset Your Password**

**Choose New Password**

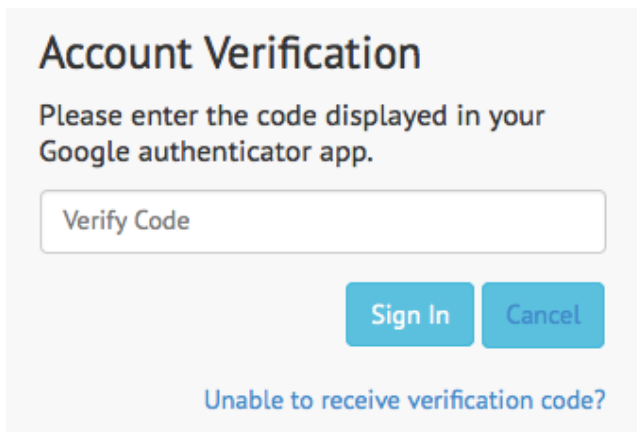
**Confirm New Password**

[Cancel](#) [Reset Password](#)

6. Enter your new password twice and click the **Reset Password** button to reset your password. Now you can login with your new password.

### 3.4 Using your Backup Code to Sign In

1. Go to **Login** page.
2. Enter your **Username** (or **Email**) and **Password**, then click **Sign In** button.
3. Click **Unable to receive verification code** link.



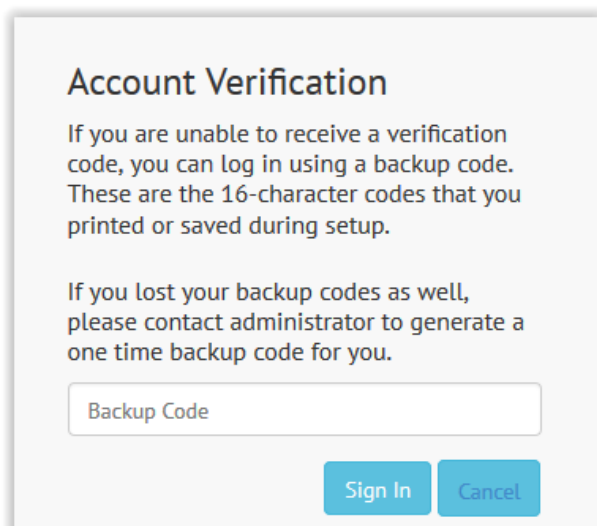
**Account Verification**

Please enter the code displayed in your Google authenticator app.

[Sign In](#) [Cancel](#)

[Unable to receive verification code?](#)

4. Enter one of your backup codes then click **Sign In** button.



**Account Verification**

If you are unable to receive a verification code, you can log in using a backup code. These are the 16-character codes that you printed or saved during setup.

If you lost your backup codes as well, please contact administrator to generate a one time backup code for you.

[Sign In](#) [Cancel](#)

### 3.5 Set up 2FA on a new phone

When you want to set up 2FA on a new phone, you will need to use your new Google Authenticator app to scan the QR code again. Here are the steps:

1. Login to **Cloud Portal**.
2. From the **top nav** bar, click **Settings** then click the **My User Profile** link.
3. Click **Manage Settings** in the **Edit My User Profile** page under the **General** tab.

Home / Users / My User Profile

## Edit My User Profile

General Preferences Access History

Login Name admin\_hkbn1955

\* First Name

\* Last Name

\* Email

[Save](#)

Two-step verification Enabled at 2016-07-05T07:23:06+00:00 (app). [Manage Settings](#)

Password Password never changed  
[Change Password](#)

4. Now you are on the Manage Two-Step Verification page.

Home / My User Profile / Enable Two-Step Verification

## Manage Two-Step Verification

Two-step verification is **Enabled**

Each time you log in to HKBN with your username and password, you must enter a verification code displayed by **Google Authenticator**.

### Single-use Backup Codes

Backup codes allow you to access your account whenever you are unable to provide a verification code, which may happen if you are traveling or if you lose your mobile phone. Please print these backup codes or save them in a safe place. If you are unable to provide a verification code and you do not have a backup code, you will be unable to sign in to your account.

- GK873RXGWZ091TDK
- 59IUOWP1LR9LH6UQ
- QI2W19TFRI1P2JRS
- 79A1NOSTRO6W9QDB
- 1TNGFL6E1C9L0TKP

### Reset two-step verification

By clicking the below button, two-step verification will be reset. You may log in to the system with only username and password.

[Reset two-step verification](#)

5. Click the **Reset two-step verification** button then you should see the following **Enable Two-Step Verification** page.

Trial V Admin  
hkbni955[Home](#) / [My User Profile](#) / [Enable Two-Step Verification](#)

## Enable Two-Step Verification

Two-step verification adds an extra layer of protection to your account. Whenever you sign in to the system, you'll need to enter both your password and also a verification code. This verification code will be sent to your mobile device via an authenticator app.

With Two-Step Verification enabled you will always need your password and one of the following to access your account:

- A verification code (via text message or an authenticator app)
- A backup code

### Warning

If you are unable to provide a verification or backup code, you will lose access to your account.

How do you want to receive the verification code?

[Google Authenticator App](#)

[Cancel, maybe next time.](#)

6. Click the **Google Authenticator App** button.
7. You should see the **Enable Two-Step Verification** page.
8. Please repeat **step 8 to 14** in **Section 4.1 - First time Sign In**.

## 4 Dashboard

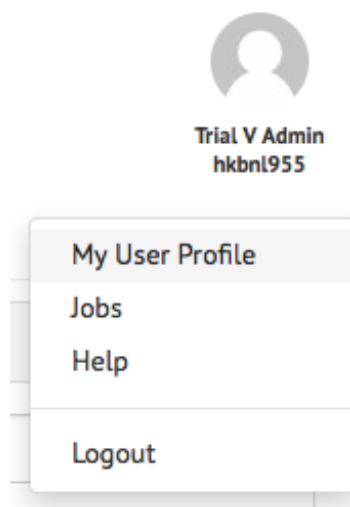
The Dashboard is the landing page upon login. It consists of the following components:

- Quick Launch:
  - User can select “New Order” to jump to the Launch VM page for VM deployment.
- Cloud VM Stats:
  - User can view OS distribution for all and individual cloud.
  - User can view VM state distribution for all and individual cloud.
- Resource Usage & Limit
  - On a per resource pool basis, user can view resource utilization and limits (quota).
- Event Logs
  - All activities within a tenant account are listed.
- Job Pending for My Approval
  - All jobs requiring your approval are listed.
- My Job Status
  - All tasks performed by your account are listed.
- Notification Center (orange arrow button at bottom right corner)
  - It will pop-up automatically where there is any background job started, or you can click the button manually to see the details.

The screenshot displays the Cloud Portal Dashboard interface. At the top, there is a navigation bar with icons for Dashboard, Launch, Instance, Resource, Reports, Settings, Monitoring, and a user profile icon labeled 'Trial V Admin hkbni955'. Below the navigation bar, the main content area is titled 'Welcome' and contains several widgets:

- Quick Launch:** A blue button with a white plus sign and the text 'New Order'.
- Cloud VM Stats (Left):** A widget titled 'Cloud VM Stats' with a dropdown menu set to 'All Clouds'. It displays a pie chart for 'OS Distribution - All Clouds' showing 50% Windows (dark blue) and 50% Centos (light blue).
- Cloud VM Stats (Right):** A widget titled 'Cloud VM Stats' with a dropdown menu set to 'All Clouds'. It displays a pie chart for 'VM State - All Clouds' showing 50% Running (dark blue) and 50% Stopped (light blue).
- Resource Usage & Limit:** A widget showing resource usage for domain 'HKBNI955R / HKS03'. It includes several progress bars:
  - Instances - 2 of 2 (100.0%)
  - vCPU - 3 of 4 (core) (75.0%)
  - RAM - 6144 of 8192 (MB) (75.0%)
  - Public IP - 1 of 2 (50.0%)
  - Primary Storage - 250 of 270 (GB) (92.6%)
  - Secondary Storage - 3 of 250 (GB) (1.2%)
  - Snapshots - 2 used (2 used)
  - Templates - 0 used (0 used)
  - Volumes - 3 used (3 used)
- Event Logs:** A widget at the bottom right with an orange arrow icon pointing up.

## 4.1 User Profile



Click the **User Profile** icon in upper right corner to access:

- **My User Profile** – for updating user personal information, changing password, managing 2FA token and accessing history. Please refer to **Session 8.1** for more details.
- **Jobs** – show all request, approved & pending for approval jobs (if approval chain is enabled)
- **Logout** – to logout the cloud portal session



## 5 Launch

User can launch a VM (virtual server) from the Cloud Portal by clicking the Launch icon on the Top Nav menu. User will be redirected to the Resource Order page.

Home / Resource Order

**+ Launch VM** Load Save

Workload: My Workload 2016-07-05      Life Cycle:

Instance Name:

Host Name:

Lifetime:

Resource Pool:

Location:

Zone:

Launch From:

Template:

Compute Details:

**My Order**

Application: N/A

Target Cloud: Cloud Location: HKS03

**Resource Usage & Limit**

HKS03 ↑

In the Resource Order page, user can design the VM instance by providing the following info:

- **Workload & Life Cycle:** These are optional fields. The purpose of these tags are for user to list all VMs filtered by the Workload or Life Cycle value. Users are recommended to group VMs into different Workload & Life Cycles for easy management.

Workload:       Life Cycle:

- **Instance name:** User can enter a name to identify a VM instance.
- **Hostname:** This is an optional field. Hostname is the server name and must be unique within the same network. If this field is left empty, Cloud Portal will generate a name for this field automatically.
- **Lifetime:** User can set the lifetime of a VM so it can be automatically terminated to avoid unnecessary charges.

Lifetime:

Resource Pool:

Location:

- **Resource pool:** A list of active cloud targets for user to select for deployment.

- **Location:** If a cloud target consists of multiple locations, a list will be provided for selection.
- **Zone:** Similar to Location, if a location consists of multiple zones, a list will be provided for selection.
- **Launch From:** VM can be launched from Template, ISO or Volume Snapshot.

Launch From

✓ Template

- ISO
- Volume Snapshot

Template

Windows 2012 Datacenter (120GB Root Volume)
▼

- **Template:** When launching from Template, select one of the available template from the drop down list.

- **Compute Offering:** A predefined list of VM sizes for users to select.

Compute Offering

Basic (1 x 2 GHz vCPU | 2 GB RAM)
↕

vCPU: 1  
RAM: 2048 MB

- **Network:** User can select existing Network or create new one from the Network drop down list.

Network

HK4-HKBN05-VPC-Network (192.168.105.0/24)

▼
+

**Existing Networks**

- HK4-HKBN05-VPC-Network (192.168.105.0/24)

**For New Network**

- Create New Network

The **Internal IP** field is optional, it will be assigned by DHCP if this field is blank.

Optionally, user can add more than one network for this VM by clicking the + button. Please note the first selected network will be set as default if more than one networks is added for this VM.

**Note:** VPC is pre-provisioned and configured by HKBN, customers are recommended not to add/delete the VPC by themselves on the portal.

- **Data volume:** User can also add additional data volumes to the VM for extra storage space.

Data Volume

VM-1-DB-Vol-1

Disk Offering: T1 Database Layer ↕ 10 GB

The **Volume name** is a required field for adding a new data volume. Also, user must select one of the **Disk Offerings** and set the **size** of this data volume.

- **Tags (optional):** User can add tag(s) for this VM. A tag is a key-valued pair.

Click the + button to add more tags.

User can launch more than one server (VM) at the same time on the Resource Order page. This Resource Order page will update resource utilization in the Resource Usage & Limit section in real time so user can determine whether there are sufficient resources for this deployment.

### Resource Usage & Limit



HKS03

#### Domain Limit

Instances 2 Of 2 Used - To Add 1

100%

vCPU 3 Of 4 core Used - To Add 1 core

75%

RAM 6144 Of 8192 MB Used - To Add 2048 MB


75%

Primary Storage 250 Of 270 GB Used - To Add 120 GB

93%

- Click the green **Provision** button to launch.

Provision

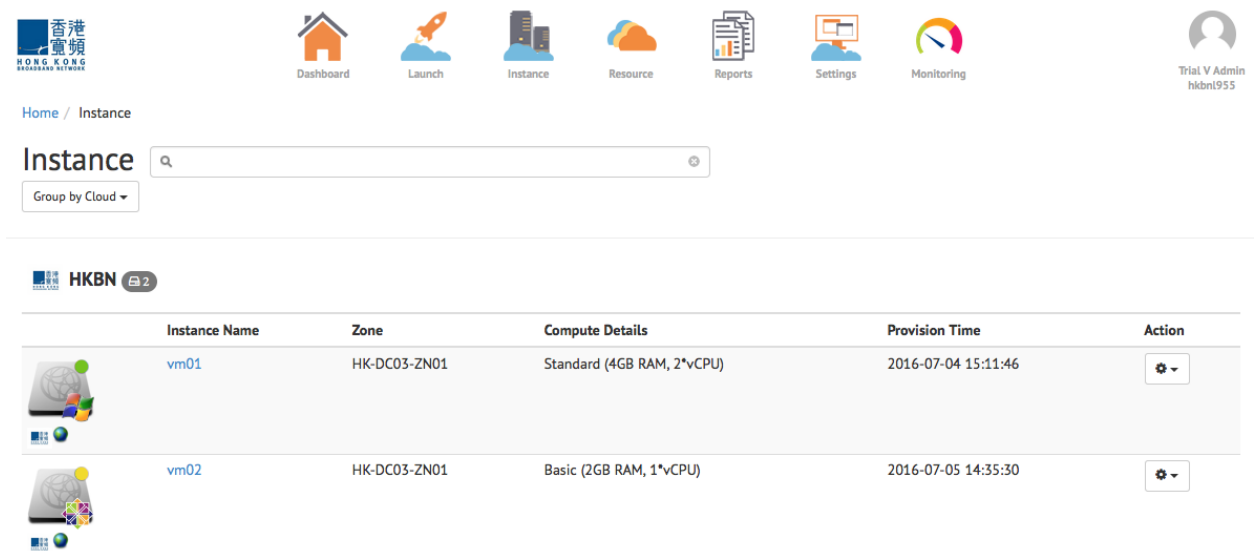
- After clicking the **Provision** button, you should see a **Terms and conditions** dialog box. Click **I have read and agreed the Terms and Conditions** check box after reading it. Then click the green **Agree** button.
- You will be redirected to the **Instance** listing page for monitoring the server launch. The **Notification Center** will pop-up from the bottom of the page to show launch progress.
- You can click the notification text to see the details or click the  button to hide the notification center.

## 6 Instance

The Instance Menu shows a list of deployed VMs with that can be drilled down into for more information. The display list can be grouped by Author, Cloud, Life Cycle, Resource Pool or Workload. User can also search VMs by attributed names or tags. Next to each VM, there is additional information like the VM status, name, zone, offering, location and provision time as well as actions. User can click the VM icon or Instance Name to enter the Server Detail page for detailed server information and change options.

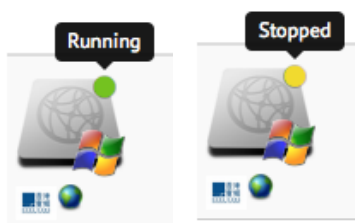
### 6.1 Listing all VMs

1. From the **Top Nav** menu, click **Instance** icon. The **Instance Listing** page shows all VMs.



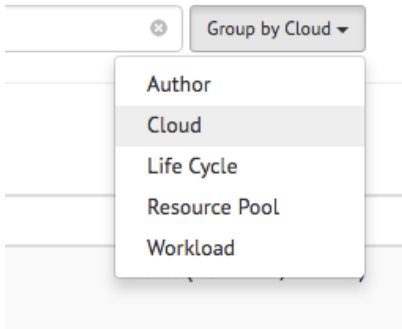
Instance Name	Zone	Compute Details	Provision Time	Action
vm01	HK-DC03-ZN01	Standard (4GB RAM, 2*vCPU)	2016-07-04 15:11:46	[Settings]
vm02	HK-DC03-ZN01	Basic (2GB RAM, 1*vCPU)	2016-07-05 14:35:30	[Settings]

2. Users can mouse over the VM state icon to see real-time VM status. For example:



#### 6.1.1 Change Grouping Display and Search

Click the Group by Cloud drop down menu to show VMs in different groups.



VMs can be grouped by **Author of the VM, Cloud, Life Cycle, Resource Pool** and **Workload**. The following example shows VMs grouped by **Workload**.

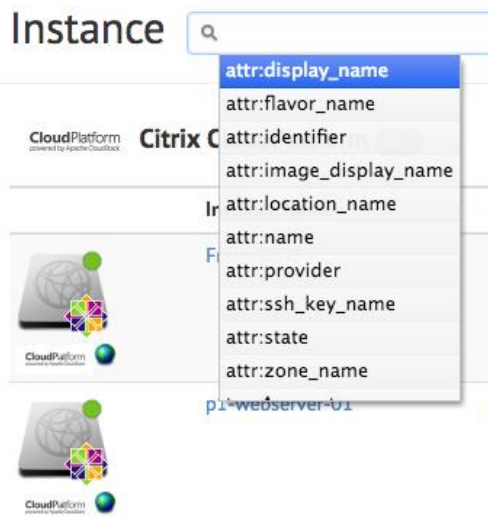
[Home](#) / Instance

Instance  Group by Workload

Group	Instance Name	Zone	Compute Offering	Provision Time	Action
Frank <span>2</span>	Frank-0526-7	AU-HCSC-DC02-ZN01 (Brisbane)	Basic (2GB RAM, 1vCPU)	2016-05-26 14:55:28	
Project-1 <span>1</span>	p1-webserver-01	AU-HCSC-DC02-ZN01 (Brisbane)	Basic (2GB RAM, 1vCPU)	2016-05-30 13:04:33	

You can search for VMs by clicking the search text box, select an attribute type and enter the keywords:

[Home](#) / Instance





It shows a list of searchable attributes and tags. The following example searched for VM display name result:

Home / Instance

Instance  Group by Workload ▾

1 record(s) found. ← Number of records found for this search


Project-1





Instance Name	Zone	Compute Offering	Provision Time	Action
 p1-websvr-01	AU-HCSC-DC02-ZN01 (Brisbane)	Basic (2GB RAM, 1*vCPU)	2016-05-30 13:04:33	

## 6.1.2 VM Operations on Instance Listing page

VM **Reboot**, **Stop**, **Start** and **Terminate** can all be performed on this page by clicking the **Action** drop down menu:



**Action**





5:28 

-  View
-  Reboot
-  Stop
-  Terminate

## 6.2 VM Details page

Click **View** under **Action** button or **Instance Name** on **Instance Listing** page to view the **VM Details**.

Instance Name	Zone	Compute Offering	Provision Time	Action
 vm01	HK-DC03-ZN01	Standard (4GB RAM, 2*vCPU)	2016-07-04 07:11:46	

-  View
-  Reboot
-  Stop
-  Terminate

The **VM Details** page shows VM information and can perform actions on the VM. The information about VM includes: **VM names, size, OS, state, lifetime policy, network interfaces, VM password, created time, created by, tags, volume and VM snapshots.**

The **VM Details** page provides the following actions to manage the VM:

- Start, Stop, Reboot and Terminate VM.
- Access Remote Console of the VM.
- Reset VM password (if VM is launched from supported template).
- Show / Hide last known VM password.
- Edit VM display name.
- Change Compute Offering (resize VM).
- Attach and detach ISO.
- Change VM lifetime policy.

- Add / remove network interfaces.
- Set default network interface.
- Acquire public IP for the VM.
- Add / Remove tags of the VM.
- View, add new, attach existing and detach volume.
- View, create, delete and schedule volume snapshot.
- Create volume, create image and restore VM from volume snapshot.
- View, create and delete VM snapshot.
- Restore VM from VM snapshot.

**Notes :** Customers are highly recommended to change the VM password after resetting.

## 6.2.1 Overview Tab

The VM Overview Tab provides detailed configurations and access info. Users can modify server configurations by clicking the blue action buttons.

Home / Instance / vm01

### vm01

Overview Volumes VM Snapshot

#### Overview

Cloud / Location: HKBN, HKS03

OS: Windows 2008 R2 Datacenter SP1 (120GB Root Volume)

State: Running

Instance ID	88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Name	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Display Name	vm01
Description	N/A
Compute Offering	<a href="#">Resize</a> Standard (4GB RAM, 2*vCPU)
ISO Attachment	<a href="#">Attach</a>
Lifetime policy	<a href="#">Update</a> Never Expires

#### Login

[Reset Password](#) 1

User name	Administrator
Last known password	<a href="#">Show</a> .....

#### Journal

Created at	2016-07-04 07:11:46
Created by	admin_hkbn1955
Last Synchronized	2016-07-04 07:49:27 - 1 minute ago

#### Tags

[Manage](#) 5

Key	Value
Workload	My Workload 2016-07-04
Author	admin_hkbn1955
Account	hkbn1955

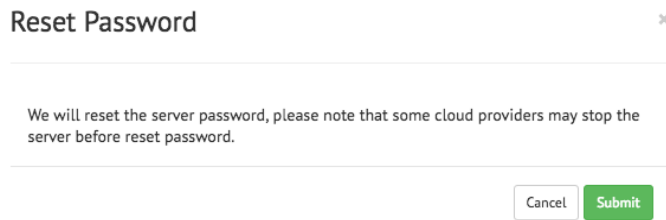
#### Network Interfaces

[Add Network Interface](#) 6

Nic 1 (default)	Network: <a href="#">HK4-HKBN05-VPC-Network</a>
	IP: 192.168.105.185
	Type: Isolated
	MAC Address: 02:00:15:25:00:0d
	Public IP: <a href="#">+ Acquire Public IP for Static NAT</a> 7

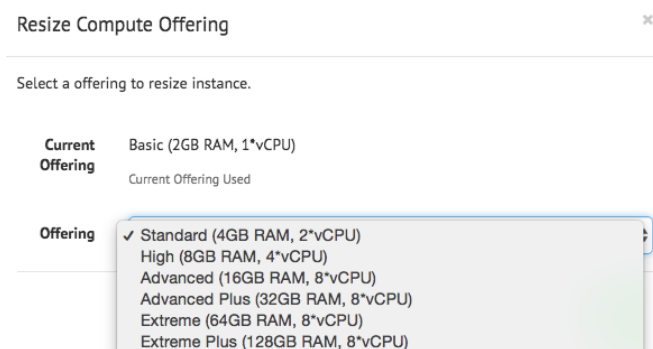
### 1. Reset Password

Click the **Reset Password** button to reset the VM password. Click **Submit** to confirm.



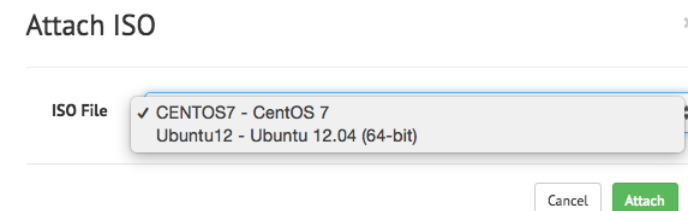
## 2. Compute Offering: Resize

Click the **Resize** button to change the server flavor. A dialog box will appear showing a list of Offering. Please note changing to a smaller server size is not advisable and certain cloud targets and operating systems may require server reboot to activate. Select a new Offering and click **Resize**.



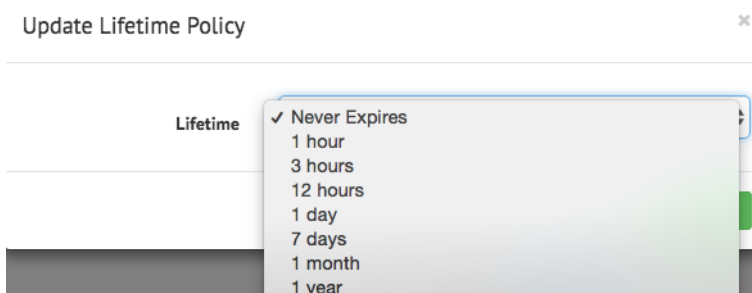
## 3. ISO Attachment: Attach

Click the **Attach** button to attach an ISO image. A dialog box will appear showing a list of available ISO images. These images have to be uploaded in advance. Select the ISO image and click **Attach** to confirm.



## 4. Lifetime Policy: Update

Click the **Update** button to change VM lifetime. A dialog box will appear showing lifetime choices. The VM will be automatically terminated once the lifetime expires. The system will automatically notify the VM owner once the lifetime reaches 50%.



## 5. Tags: Manage



Click the **Manage** button to modify server tags. A dialog box will appear with a range of keys available for changes. User can modify the Account, Author, Life Cycle and Workload tags.

Tags Editor ✕

**Info!** Tags are case-sensitive key-value pairs, to help identifying and grouping resources.  
Currently Editing: demovm01 (Server)

Key	Value	
Account	HSDemo01	✕
Author	admin	✕
LifeCycle	Development	✕
Workload	My Workload 2016-05-31	✕

+ Add Tag ✓ Update

## 6. Network Interfaces: Add Network Interface

Click **Add Network Interface** button to add additional network interfaces. A dialog box will appear with a choice of available networks. Click **Add Network** to confirm.

## 7. Network Interfaces: Acquire Public IP for Static NAT

VMs are launched with private IPs to conserve public IPs. For those requiring public IPs, click the **Acquire Public IP for Static NAT** button to assign a public IP on this network interface. A dialog box will appear showing Terms and Conditions. To confirm, check the box and click **Agree**.

I have read and agreed to the Terms and Conditions

Decline

Agree

### 6.2.2 Volumes Tab

The Volume tab allows users to manage server volumes including add, delete, attach, and detach, as well as snapshot management. The following diagram illustrates the volume and snapshot operation user interface.

Home / Instance / vm01

vm01

Overview Volumes VM Snapshot

Name	Size	Created at	Type	Status	Action
ROOT-876	120.0 GB	2016-07-04 07:11:46	root	active	<span>1 Refresh</span> <span>2 + Add Volume</span> <span>3</span> <span>4</span>
vm01_V1467775935	10.0 GB	2016-07-06 03:39:02	data	active	<span>3</span> <span>4</span>

### 1. Refresh

Click the **Refresh** button to refresh the status of volumes.

### 2. Add Volume

Click the **Add Volume** button to add additional volumes to the VM. A dialog box will appear for user to enter:

- Volume Name
- Disk Offerings
  - Users can choose from the storage tiers: SSD, T1, T2 or T3.
- Size (GB)

Overview Volumes VM Snapshot

Refresh + Add Volume

Add New Volume

Create New Volume Attach Existing Volume

Volume Name: vm01\_V1467775935

Disk Offering: T1

Size (GB): 100

Attach Volume

Add Cancel

### 3. View Snapshot

Click the **View Snapshot** button to view volume snapshot. A dialog box will appear to list the snapshots. Users can create volume, create image, restore VM or delete the snapshot.

Volume Snapshots

Created	Identifier	Name	Schedule	Action
2016-07-06T11:50:50+0800	494c02f4-fd1a-4ade-b2d9-ec755bbd334e	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db_ROOT-876_20160706035050	MANUAL	<input type="button" value="Create Volume"/> <input type="button" value="Create Image"/> <input type="button" value="Restore VM"/> <input type="button" value="Delete"/>

Cancel Refresh Create Snapshot

### 4. Schedule Snapshot

Click the **Schedule Snapshot** button to schedule snapshot. A dialog box will appear to enter the following info:

- Schedule Basis
- Time
- Time zone
- Keep # of snapshots

Snapshot schedule ×

---

Create new schedule

You can setup recurring snapshot schedules by selecting from the available options below and applying your policy preference

**Schedule Basis**  Hourly  Daily  Weekly  Monthly

**Time**  minute(s) Past the Hour

**Time zone**

**Keep**  Snapshot(s)

---

Current schedule

You haven't yet scheduled any snapshot.

Current snapshot schedules will also be listed. Click **Setup Policy** to confirm the schedule.

### 6.2.3 VM Snapshot Tab

Users can create snapshot of the entire VM including all attached disks. This is a convenient way to create VM backup for instant recovery (e.g. backup before applying software patch).

Home / Instance / vm01

vm01 🗨️ 📄 🗑️ 🏠

Overview Volumes VM Snapshot

1 Refresh
2 + Add VM Snapshot

Name	Created at	Status	Action
vm_snapshot_20160725	2016-07-25T14:57:15+0800	DiskAndMemory	true N/A active

3 Restore VM
4 🗑️

#### 1. Refresh

Click the **Refresh** button to refresh the list of snapshots.

#### 2. Add VM Snapshot

Click the **Add VM Snapshot** button to create a snapshot of the entire VM including attached disks. A dialog box will appear for users to enter:

- Name
- Description
- Snapshot Memory
- Quiesce VM

## Add New VM Snapshot

---

\* Name

Description

Snapshot Memory

Quiesce VM

---

**3. Restore VM**

Click the **Restore VM** button to restore the VM.

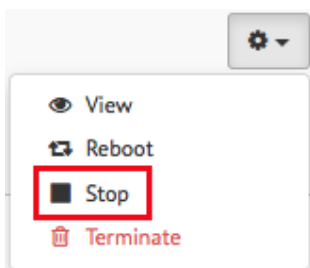
**4. Delete**

Click the **Delete** button to delete the VM Snapshot.

## 6.3 VM Operation

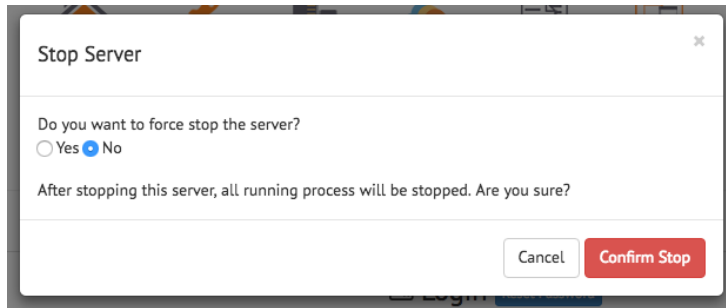
### 6.3.1 Stop VM

There are 2 ways to stop a VM: from the **Server Listing** page or the **VM Details** page. In the **Server Listing** page, click the **Action** drop down menu and select **Stop**.



On the **VM Details** page, click the **Stop** button on the top right of the page.

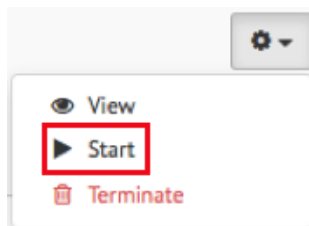




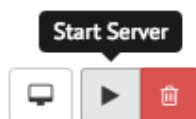
Then select **Yes** or **No** depending on whether you wish to **force stop** the VM. Click **Confirm Stop** to stop the VM.

### 6.3.2 Start VM

There are 2 ways to start a VM: from the **Server Listing** page or the **VM Details** page. In the **Server Listing** page, click the **Action** drop down menu and select **Start**.

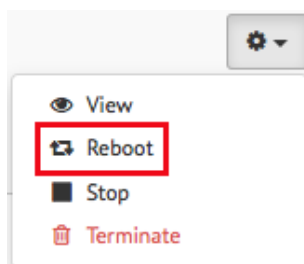


Or go to the **VM Details** page and click the **Start** button.



### 6.3.3 Reboot VM

There are 2 ways to reboot a VM: from the **Server Listing** page or the **VM Details** page. In the **Server Listing** page, click the **Action** drop down menu and select **Reboot**.

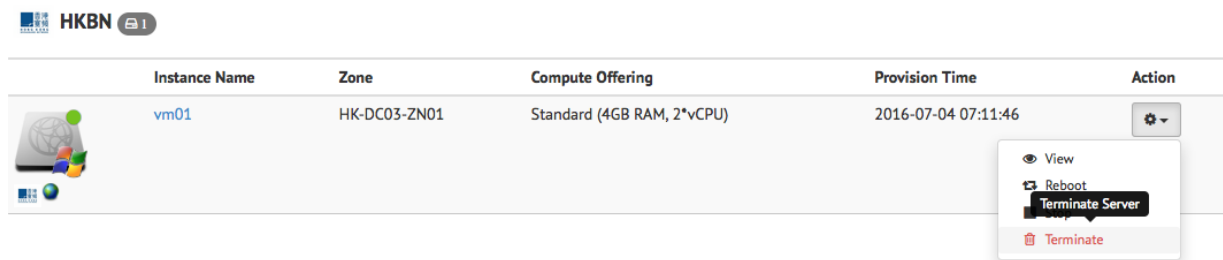


Or go to the **VM Details** page and click the **Reboot Server** button.

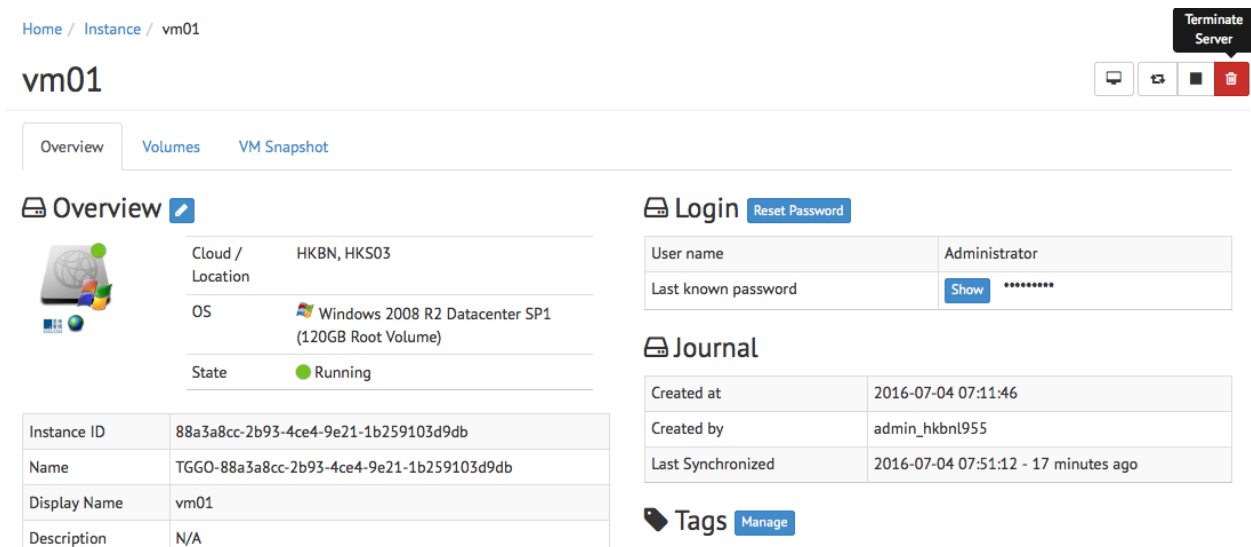


### 6.3.4 Terminate VM

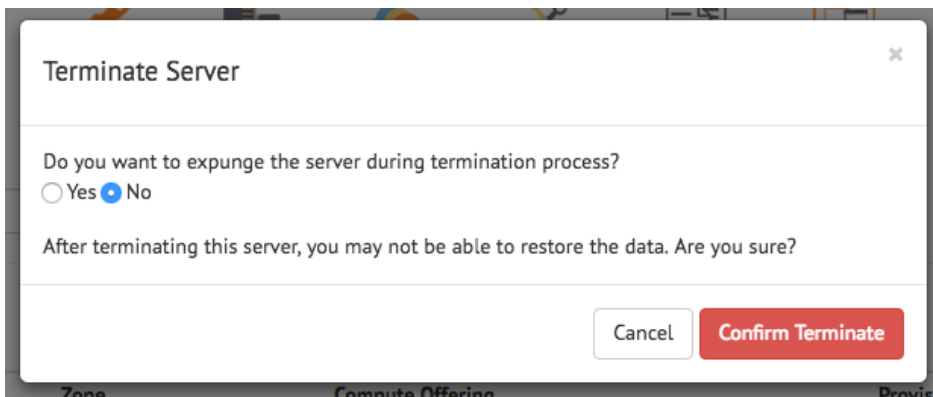
There are 2 ways to terminate a VM: from the **Server Listing** page or the **VM Details** page. In the **Server Listing** page, click the **Action** drop down menu and select **Terminate**:



In VM Details page, click the red **Trash** button:



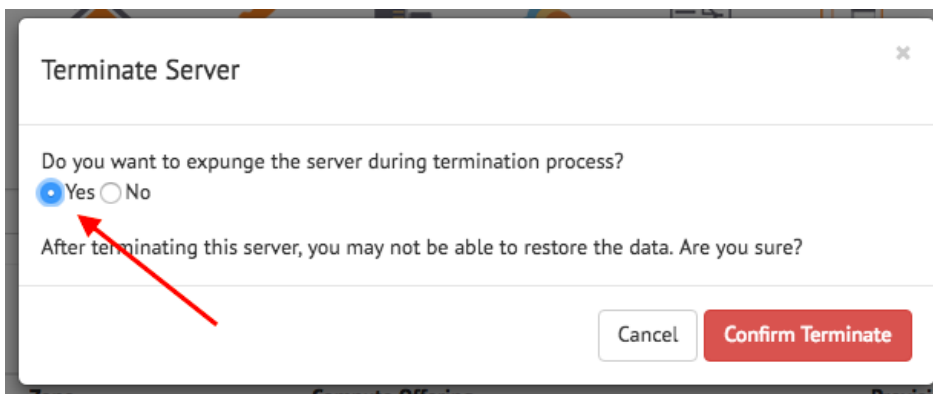
Either way will pop-up a Terminate Server dialog box:



By default, the server will not be expunged. Click the red **Confirm Terminate** button to terminate the VM.

### 6.3.4.1 Expunge

If Expunge is selected, the VM will be destroyed immediately and you will not be able to recover it. If Expunge is not selected, the VM will not be destroyed immediately and the VM can be recovered within 24 hours.



You can Expunge a terminated VM in either **Server Listing** or **VM Details** page.



### 6.3.4.2 Recover VM

Click the **Recover** button in **Server Listing** or **VM Details** page to recover a terminated VM.

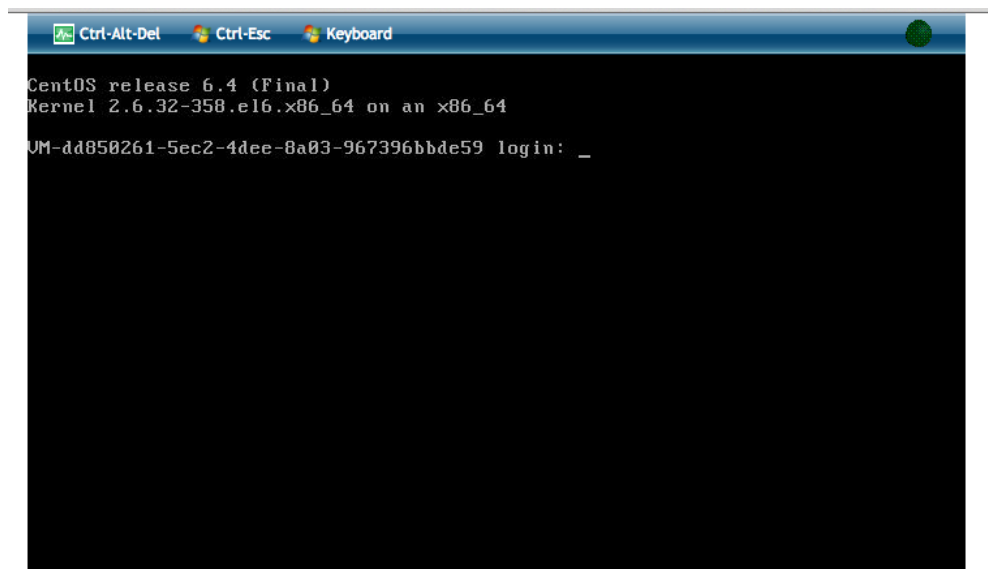


### 6.3.5 Remote Console

1. From the **Top Nav** menu, click the **Instance** icon.
2. In this **Server Listing** page, find your VM then click the **VM name** to go to the **VM Details** page.
3. Click the **Remote Console** button.

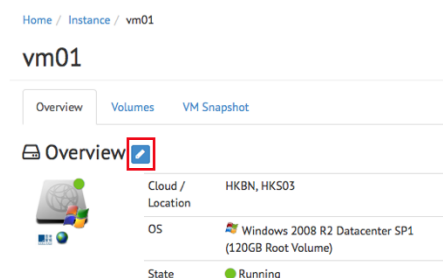


4. Then a new browser tab will open.



### 6.3.6 Change VM Display Name

1. From the **Top Nav** menu, click the **Instance** icon.
2. In this **Server Listing** page, find the VM you wish to edit, then click the **VM name** to go to the **VM Details** page.
3. Click the **pen** button in the **Overview** section.



4. Change the **Display Name** in the **Edit Server** dialog box then click the green **Save** button.





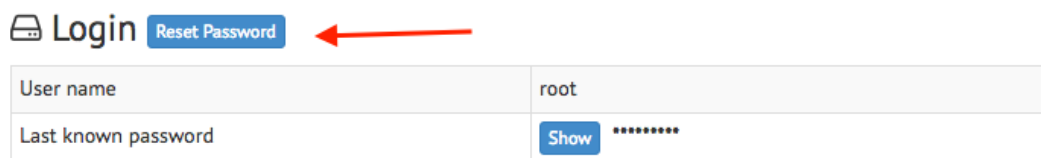
## 6.3.7 VM Password

### 6.3.7.1 Reset VM Password

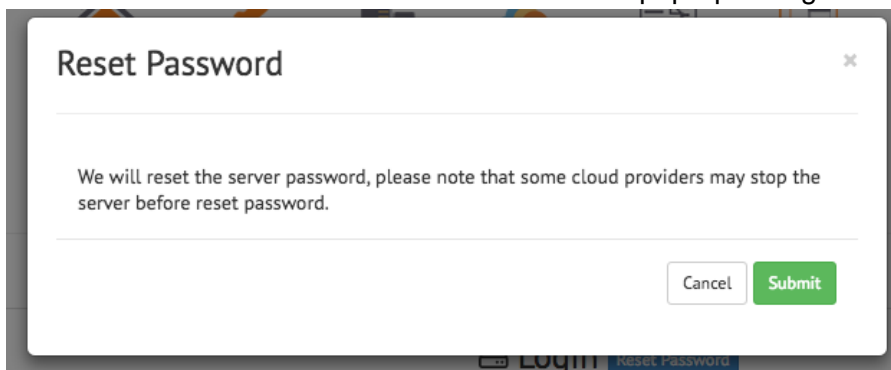
Some template supports password resetting after VM is launched. In some cases, you might need to stop the VM before you are allowed to reset the VM password.

To reset VM password:

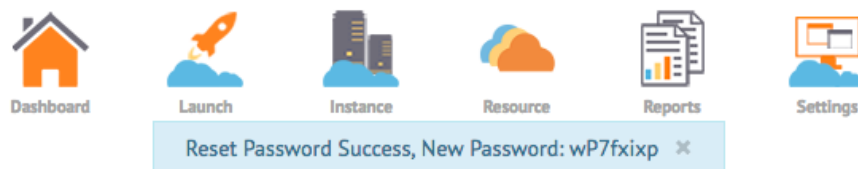
1. From the **Top Nav** menu, click the **Instance** icon.
2. In this **Server Listing** page, find the your VM then click the **VM name** to go to the **VM Details** page
3. Click the **Reset Password** button in the **Login** section.



4. Click the **Submit** button in the **Reset Password** pop-up dialog box.




5. After a while, user should see a pop-up message with your new VM password.



- User should also receive an email about this VM password.

### 6.3.7.2 Show / Hide Last Known VM Password

- From the **Top Nav** menu, click on the **Instance** icon.
- In this **Server Listing** page, find your VM then click the **VM name** to go to the **VM Details** page.
- Click the **Show / Hide** button under **Login** section to show or hide the VM password.

 Login [Reset Password](#)

User name	root
Last known password	<a href="#">Show</a> .....



**Notes :** To enhance security protection, customers are recommended to change the password after VM password is reset.


### 6.3.8 Resize VM (Compute Offering)

Users can resize the VM (change compute offering) by clicking the **Resize** button in the **VM Details** page. Please note that some OS's might require the VM to be stopped before resizing the VM.

- From the **Top Nav** menu, click the **Instance** icon.
- In this **Server Listing** page, find the VM that you want to edit, then click the **VM name** to go to the **VM Details** page.
- Click the **Resize** button under the **Overview** section.

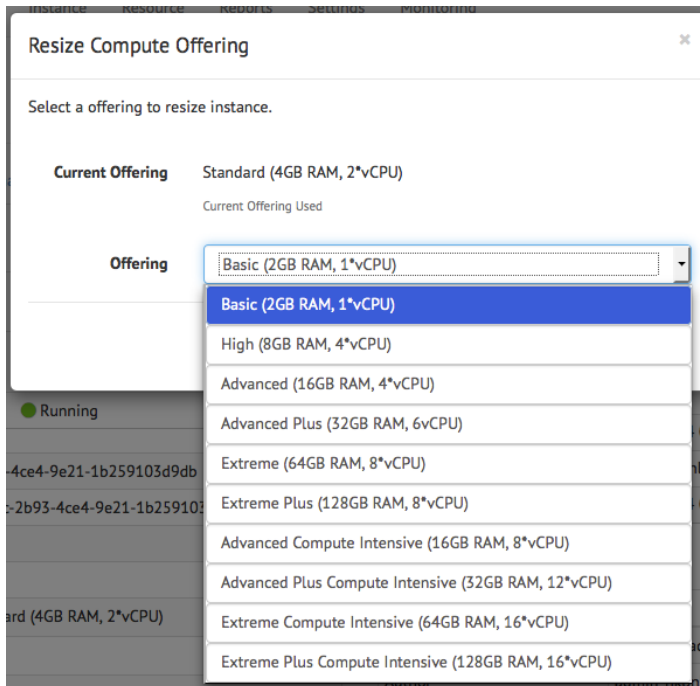
Overview [Volumes](#) [VM Snapshot](#)

 Overview 

	Cloud / Location	HKBN, HK503
	OS	Windows 2008 R2 Datacenter SP1 (120GB Root Volume)
	State	<span style="color: green;">●</span> Running

Instance ID	88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Name	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Display Name	vm01
Description	N/A
Compute Offering	<a href="#">Resize</a> Standard (4GB RAM, 2*vCPU)
ISO Attachment	<a href="#">Attach</a>
Lifetime policy	<a href="#">Update</a> Never Expires

4. Change the **Offering** in the **Resize Compute Offering** dialog box then click the **Save** button.



### 6.3.9 Manage VM Network Interface

There are a few network related operations that a user can perform in the **VM Details page**: attaching a new network interface, removing a network interface, setting the default network, acquiring a public IP, and releasing the public IP. For more Network Operations, you can click the network name in the Network Interfaces section of the VM Details page to access the network details.

**Network Interfaces** [Add Network Interface](#)

Nic 1 (default)	Network	<a href="#">HK4-HKBN05-VPC-Network</a>
	IP	192.168.105.185
	Type	Isolated
	MAC Address	02:00:15:25:00:0d
	Public IP	<a href="#">+ Acquire Public IP for Static NAT</a>

#### 6.3.9.1 Attach New Network Interface

1. In the VM Details page, click the **Add Network Interface** button.

**Network Interfaces** [Add Network Interface](#)

Nic 1 (default)	Network	<a href="#">HK4-HKBN05-VPC-Network</a>
	IP	192.168.105.185
	Type	Isolated
	MAC Address	02:00:15:25:00:0d
	Public IP	<a href="#">+ Acquire Public IP for Static NAT</a>

2. Select an available network from the **Network** drop down list in the **Add Network Interface** dialog box.

3. Click the green **Add Network** button.
4. After the 2nd network interface is added, you should see:

Network Interfaces [Add Network Interface](#)

Nic 1 (default)	Network	HK4-HKBN05-VPC-Network
	IP	10.7.1.4
	Type	Isolated
	MAC Address	02:00:6f:15:00:0f
	Public IP	<a href="#">+ Acquire Public IP for Static NAT</a>
Nic 2	Network	network-2
	IP	192.168.1.196
	Type	Isolated
	MAC Address	02:00:6a:25:00:02
	Public IP	<a href="#">+ Acquire Public IP for Static NAT</a>
	<a href="#">Set as Default</a> <a href="#">Remove</a>	

### 6.3.9.2 Remove Network Interface

When there are more than one network interfaces, you can remove the non-default network by clicking the red **Remove** button in Network Interface section of the **VM Details** page.

### Network Interfaces Add Network Interface

Nic 1 (default)	Network	HK4-HKBN05-VPC-Network
	IP	10.7.1.4
	Type	Isolated
	MAC Address	02:00:6f:15:00:0f
	Public IP	<span>+ Acquire Public IP for Static NAT</span>
Nic 2	Network	network-2
	IP	192.168.1.196
	Type	Isolated
	MAC Address	02:00:6a:25:00:02
	Public IP	<span>+ Acquire Public IP for Static NAT</span>
	<span>Set as Default</span> <span>Remove</span>	

#### 6.3.9.3 Set Default Network

When there are more than one network interfaces, you can select one to be the default interface. Go to the **VM Details** page and click **Set as Default** button under Network Interfaces section.

### Network Interfaces Add Network Interface

Nic 1 (default)	Network	HK4-HKBN05-VPC-Network
	IP	10.7.1.4
	Type	Isolated
	MAC Address	02:00:6f:15:00:0f
	Public IP	<span>+ Acquire Public IP for Static NAT</span>
Nic 2	Network	network-2
	IP	192.168.1.196
	Type	Isolated
	MAC Address	02:00:6a:25:00:02
	Public IP	<span>+ Acquire Public IP for Static NAT</span>
	<span>Set as Default</span> <span>Remove</span>	

#### 6.3.9.4 Acquire Public IP

1. In the VM Details page, click **Acquire Public IP for Static NAT** button.

### Network Interfaces Add Network Interface

Nic 1 (default)	Network	HK4-HKBN05-VPC-Network
	IP	10.7.1.4
	Type	Isolated
	MAC Address	02:00:6f:15:00:0f
	Public IP	<span>+ Acquire Public IP for Static NAT</span>

2. Agree the Terms and Conditions.
3. You should see the public IP after it acquired the IP

## Network Interfaces [Add Network Interface](#)

Nic 1 (default)	Network	<a href="#">HK4-HKBN05-VPC-Network</a>
	IP	192.168.105.185
	Type	Isolated
	MAC Address	02:00:15:25:00:0d
	Public IP	<a href="#">Release IP</a> <a href="#">103.63.135.110</a>

- Also, user should receive an email about this new acquired IP.

### 6.3.10 Manage Volume

User can manage VM volumes in the **Volumes tab** of the **VM Details page**.

The screenshot shows the 'VM Details' page with three tabs: 'Overview', 'Volumes', and 'VM Snapshot'. The 'Volumes' tab is highlighted with a red box. Below the tabs, there is an 'Overview' section with a server icon and a list of details:



Cloud / Location	HKBN, HKS03
OS	Windows 2008 R2 Datacenter SP1 (120GB Root Volume)
State	Running

In the Volumes tab, you can perform the following operations: add new data volume, attach existing data volume, detach and / or delete attached volume, take / delete / schedule volume snapshot, create volume from snapshot, create image form volume snapshot or restore VM from root volume snapshot.

#### 6.3.10.1 Add new Data Volume

1. Click the **Add Volume** button in Volumes tab.

The screenshot shows the 'Volumes' tab selected. At the top right, there are 'Refresh' and '+ Add Volume' buttons. Below is a table with the following data:

Name	Size	Created at	Type	Status	Action
ROOT-876	120.0 GB	2016-07-04 07:11:46	root	active	 

2. Click the **Create New Volume** button. User should see the following form:

The screenshot shows the 'Add New Volume' form. At the top right, there are 'Refresh' and '+ Add Volume' buttons. Below the form title, there are two buttons: 'Create New Volume' and 'Attach Existing Volume'. The form fields are:

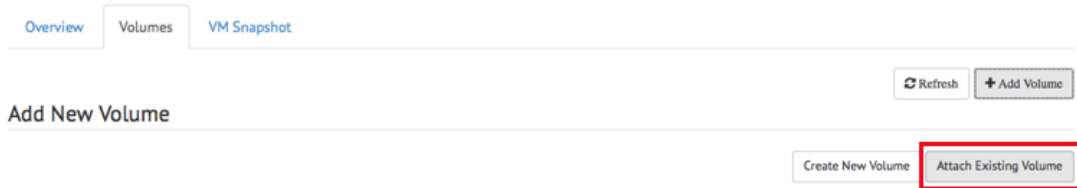
- Volume Name:
- Disk Offering:
- Size (GB):
- Attach Volume

At the bottom right, there are 'Add' and 'Cancel' buttons.

3. Enter **Volume Name**, select **Disk Offering**, enter the data volume **size**, click **Attach Volume** if user want to attach this volume to the current VM and click **Add** to create this data volume.
4. Agree the Terms and Conditions.
5. A new data volume is created and user should receive an email about this volume.

#### 6.3.10.2 Attach Existing Data Volume

1. Click the **Add Volume** button in Volumes tab.
2. Click the **Attach Existing Volume** button. User should see the following form.








3. Select **Available Volume** then click **Attach** button.

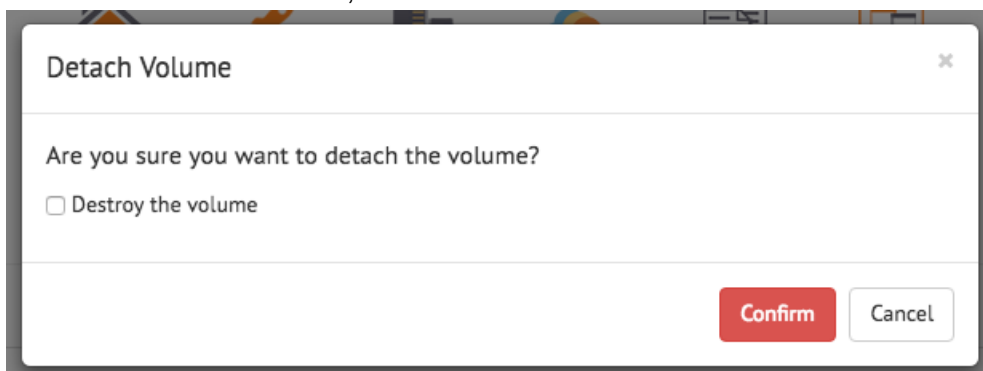
### 6.3.10.3 Detach Data Volume

1. Click the red **Detach** button.

The screenshot shows the 'Volumes' tab in the Cloud Portal. It displays a table with columns: Name, Size, Created at, Type, Status, and Action. There are two rows of data. The 'Action' column for the second row (vm01\_V1467775935) has a red 'Detach' button highlighted with a red box.

Name	Size	Created at	Type	Status	Action
ROOT-876	120.0 GB	2016-07-04 07:11:46	root	active	 
vm01_V1467775935	10.0 GB	2016-07-06 03:39:02	data	active	  

2. Check the **Destroy the volume checkbox** if user wants to destroy the data volume at the same time. Otherwise, leave it unchecked.

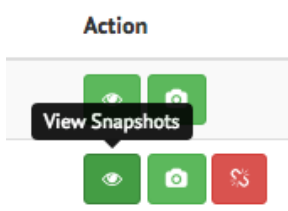


3. Click the red **Confirm** button.

### 6.3.10.4 Volume Snapshot

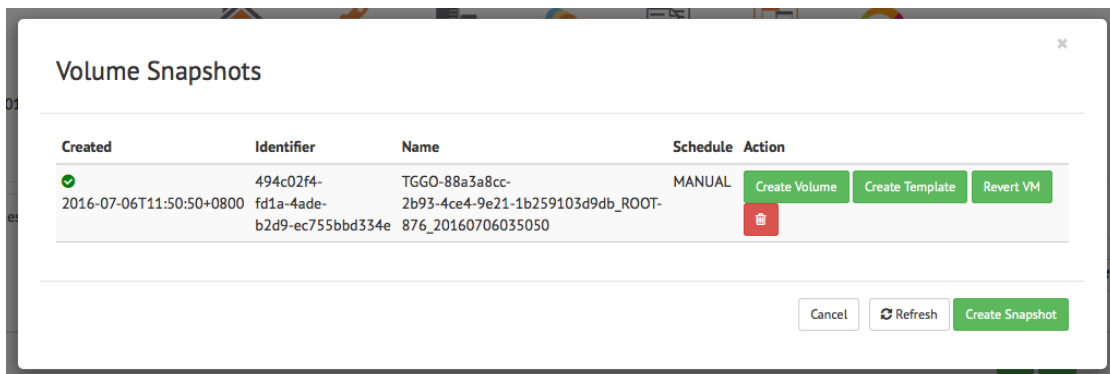
To view Volume snapshots.

1. Click the green **View Snapshots** button beside the Root or Data Volume in the Volume tab.



2. User should see this dialog:






### 6.3.10.5 Create Volume Snapshot

To create Root Volume or Data Volume Snapshot:

1. Click the green **View Snapshots** button beside the Root or Data Volume in the Volume tab.
2. Click the **Create Snapshot** button in Volume Snapshots dialog box.

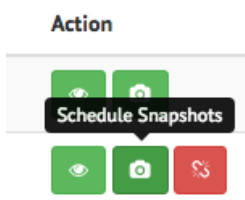
### 6.3.10.6 Delete Volume Snapshot

1. Click the green **View Snapshots** button next to the Root or Data Volume in the Volume tab.

2. Click the red **Trash** button  next to the snapshot that user wants to delete.

### 6.3.10.7 Schedule Volume Snapshot

1. Click the green **Schedule Snapshot** button beside the Root or Data Volume in the Volume tab.



2. User should see the Snapshot schedule dialog box.

This dialog box shows the current scheduled snapshot policy. It can be removed.

3. Fill in the details and click the green **Setup policy** button.
4. Agree the Terms and Conditions.

### 6.3.10.8 Create Volume from Snapshot

1. Click the **View Snapshots** button beside Root or Data Volume.

Created	Identifier	Name	Schedule	Action
2016-07-06T11:50:50+0800	494c02f4-fd1a-4ade-b2d9-ec755bbd334e	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db_ROOT-876_20160706035050	MANUAL	<input type="button" value="Create Volume"/> <input type="button" value="Create Template"/> <input type="button" value="Revert VM"/>

2. Click the **Create Volume** button from one of the snapshots.
3. Enter the **Volume Name** then click **Create** button.
4. Agree the Terms and Conditions.
5. Users should receive an email after the Volume is created.

### 6.3.10.9 Create Template from Root Volume Snapshot

Users can only create images from Root Volume snapshots, but not from data volume snapshots.

1. Click the **View Snapshots** button beside the Root Volume.
2. Click the green **Create Image** button.
3. Fill in the **Create Image From Snapshot** form.

4. Click the **Create** button.

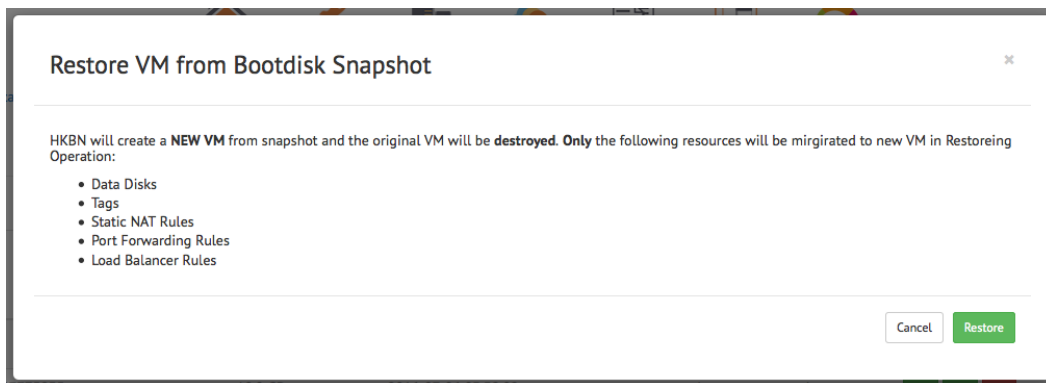
#### 6.3.10.10 Restore VM from Root Volume Snapshot

Cloud Portal supports restoring VM from a root volume snapshot if the VM still exists. In the restore VM operation, the system will create a **NEW VM** from snapshot and **the original VM will be destroyed**. The following resources will be migrated to new VM in this restore operation including Data Disks, VM Tags, Static NAT Rules, Port Forwarding Rules, Load Balancer Rules and Public IP address.

1. Go to the VM Details page under the Volumes tab.
2. Click the green View Snapshots button next to the root volume.
3. Click the green **Restore VM** button from one of the snapshots.

Created	Identifier	Name	Schedule	Action
2016-07-06T11:50:50+0800	494c02f4-fd1a-4ade-b2d9-ec755bbd334e	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db_ROOT-876_20160706035050	MANUAL	<a href="#">Create Volume</a> <a href="#">Create Image</a> <a href="#">Restore VM</a>

4. Click the green **Restore** button to confirm the restore.



### 6.3.11 Manage VM Snapshot

The VM Snapshots tab in the VM Details page can perform the following operations: create a VM snapshot, delete a VM snapshot, and restore from VM snapshot.


#### 6.3.11.1 Create new VM Snapshot

1. Go to the VM Snapshots tab in the VM Details page then click the **Add VM Snapshot** button.
2. Enter the name of the snapshot, description, and check available options, then click the **Create** button and agree the Terms and Conditions.

3. Check the **Snapshot Memory** checkbox if you want to take 'disk and memory' snapshot.
4. When the **Snapshot Memory** checkbox is unchecked, only a 'disk' snapshot is taken.
5. When the state of VM is:
  - Running – Both 'disk and memory' and 'disk' snapshots can be taken.
  - Stopped – Only 'disk' snapshots can be taken.
6. Check the **Quiesce VM** checkbox to allow application awareness on the snapshot to be created if OS level is supported.

#### 6.3.11.2 Restore from VM Snapshot

Click the **Restore VM** button in the VM Snapshots tab to restore the VM.


Overview Volumes VM Snapshot						
Name	Created at	Status	Action			
Snapshot-1	2016-06-02T20:43:32+0800	Disk	true	N/A	active	<a href="#">Restore VM</a> 


### 6.3.11.3 Delete VM Snapshot

Click the red **trash can**  in VM Snapshots tab to delete the VM snapshot.


### 6.3.12 Attach / Detach ISO

1. Click the blue **Attach** button in the VM Details page.

**Overview** 



Cloud / Location: HKBN, HK503

OS:  Windows 2008 R2 Datacenter SP1 (120GB Root Volume)

State: ● Running

Instance ID	88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Name	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Display Name	vm01
Description	N/A
Compute Offering	<a href="#">Resize</a> Standard (4GB RAM, 2*vCPU)
ISO Attachment	<a href="#">Attach</a>
Lifetime policy	<a href="#">Update</a> Never Expires

2. Select an **ISO File** then click the green **Attach** button.

**Attach ISO** ✕

---

ISO File:

---

3. Click the red **Detach** button to detach the ISO.

Instance ID	88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Name	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Display Name	vm01
Description	N/A
Compute Offering	<a href="#">Resize</a> Standard (4GB RAM, 2*vCPU)
ISO Attachment	<a href="#">Detach</a> CENTOS7 - CentOS 7 [0ffc67d9-eeec-4eea-b01d-eebfc
Lifetime policy	<a href="#">Update</a> Never Expires

## 7 Resource

The Resource Menu contains functions for managing integrated resource pools.



### 7.1 Resource Pools

Click the Resource icon in the top menu to show a list of integrated resource pools. In this example, there is one resource pool - named HKBNL955R. For each resource pool, users can manage the following functions:

- Regions
- Usage & Limit
- Networking
- Offering
- Images
- Snapshots
- Volumes
- ISOs

### 7.2 Regions

A resource pool can have multiple zones, one zone is defined by default and multiple zones are not supported.

[Home](#) / [Resource Pools](#) / [Edit HKBNL955R](#)

#### Resource Pool - HKBNL955R

[Regions](#) [Usage & Limit](#) [Networking](#) [Offering](#) [Images](#) [Snapshots](#) [Volumes](#) [ISOs](#)

Name	Icon	Version	Status	Action
HKS03		N/A		<a href="#">View Zones</a>

### 7.3 Usage & Limits

Resource limit is assigned on a per tenant basis. This is to prevent individual tenant from consuming too much platform resources and causing performance issues. The following chart shows assigned vs. consumed resources.

Home / Resource Pools / Edit HKBNL955R

## Resource Pool - HKBNL955R

Regions

Usage &amp; Limit

Networking

Offering

Images

Snapshots

Volumes

ISOs

ALL Locations

HKS03

## Domain Limit

Instances - 2 of 2  
100.0%vCPU - 3 of 4 (core)  
75.0%RAM - 6144 of 8192 (MB)  
75.0%Public IP - 1 of 2  
50.0%Primary Storage - 250 of  
270 (GB)  
92.6%Secondary Storage - 3 of  
250 (GB)  
1.2%Snapshots - 2 used  
2 usedTemplates - 0 used  
0 usedVolumes - 3 used  
3 used

## 7.4 Networking

The Networking tab allows users to manage networks in a resource pool.

Home / Resource Pools / Edit HKBNL955R

## Resource Pool - HKBNL955R

Regions

Usage &amp; Limit

Networking

Offering

Images

Snapshots

Volumes

ISOs

Networks 1

VPC 1

VPN Customer Gateways 0

Public IPs 1

+ Add Flat Network

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	2	0	HKS03	HK-DC03-ZN01	Edit Delete

User can perform the following network operations:

- create / delete / manage flat network
- create / delete / manage VPC
- create / delete VPN customer gateways
- acquire / release public IP etc.

### 7.4.1 VPC Network

The Virtual Private Cloud (VPC) is a private, isolated part of cloud platform. A VPC can have its own virtual network topology that resembles a traditional physical network. You can launch VMs in the virtual network that can have private addresses in the range of your choice. You can define network tiers within your VPC network range, which enables you to group similar kinds of instances based on IP address range.

Users can manage VPC networks by going to the **Networking tab > VPC tab** on the **Resource** page.

1. Click the **Resource** icon in the **Top Nav** menu.
2. Click the **Networking tab** then click the **VPC tab**.



Home / Resource Pools / Edit HKBNL955R

## Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks 1 **VPC 1** VPN Customer Gateways 0 Public IPs 2

+ Add VPC

Name	Cidr	Subnets	Associated VMs	Associated Public IPs	Status	Location	Zone	Actions
HK4-HKBN05-VPC	192.168.0.0/16	1	2	2	Enabled	HKS03	HK-DC03-ZN01	Edit Delete

Users can manage the following VPC functions:

- create / delete VPC
- update VPC name
- restart VPC
- add site-to-site VPN
- add / remove ACL lists
- create / delete subnet
- acquire new IP for the VPC subnet.

**Note: VPC is pre-provisioned by HKBN and customers are highly recommended NOT to delete and/or create VPC via cloud portal.**

Users can also see all subnets in the Networks tab:

Home / Resource Pools / Edit HKBNL955R

## Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks 1 VPC 1 VPN Customer Gateways 0 Public IPs 2

+ Add Flat Network

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	2	0	HKS03	HK-DC03-ZN01	Edit Delete

### 7.4.1.1 Edit and Restart VPC

To edit or restart a VPC:

1. Go to the **VPC** tab.
2. Click the **VPC name** or **Edit** button to view the details of the VPC.

Home / Resource Pools / Edit HKBNL955R

## Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks 1 VPC 1 VPN Customer Gateways 0 Public IPs 2

+ Add VPC

Name	Cidr	Subnets	Associated VMs	Associated Public IPs	Status	Location	Zone	Actions
HK4-HKBN05-VPC	192.168.0.0/16	1	2	2	Enabled	HKS03	HK-DC03-ZN01	<b>Edit</b> Delete

3. Click the **Overview** tab.
4. Change the **VPC Name** and/or **Display Name** then click the **Update Network** button to update the VPC.
5. To restart the VPC, follow the above step 1 and 2 then click the blue **Restart VPC** button.

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC

## VPC HK4-HKBN05-VPC

Overview

Site-to-site VPN

ACL Lists 3

Subnets 1

Public IPs 2

Update Network

Delete

Attribute	Value
Name	HK4-HKBN05-VPC
Display Name	HK4-HKBN05-VPC
Status	Enabled
Provider	cloudstack
Location Code	HKS03
ID	594c0c98-f3cf-44ce-9e62-99a6a59009f4
Zone Name	HK-DC03-ZN01
CIDR	192.168.0.0/16
VPC Offering ID	0bf4735f-343d-4408-a5fc-332b20c4e08a
Account	admin_hkbnl955
Domain	AA000422
Restart Required	false
Network Domain	cs2fcloud.internal
Distributed VPC Router	false
Region Level VPC	false
Associated VMs	Subnet <b>HK4-HKBN05-VPC-Network</b> : <ul style="list-style-type: none"> <li>vm01 (running)</li> <li>vm02 (stopped)</li> </ul>
Restart VPC	<a href="#">Restart VPC</a>

### 7.4.1.2 Subnet

#### 7.4.1.2.1 Create Subnet (Tier)

##### To create a VPC subnet:

1. Go to the **VPC** tab.
2. Click the **VPC name** or **Edit** button to view the details of the VPC.
3. Click the **Subnets** tab.
4. Click the **Add Subnet** button.

[+ Add Subnet](#)

5. Fill in the **Create New Subnet** form.

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC

## VPC HK4-HKBN05-VPC

Overview

Site-to-site VPN

ACL Lists 3

Subnets 1

Public IPs 2

## Create New Subnet

+ Add Subnet

* Name	<input type="text" value="HK4-HKBN05-VPC-web"/>
* Display Text	<input type="text" value="HK4-HKBN05-VPC Web Tier"/>
Network Offering	<input type="text" value="DefaultIsolatedNetworkOfferingForVpcNetworksNoLB"/>
Gateway	<input type="text" value="e.g. 10.12.0.1"/> <small>Cidr of VPC: 192.168.0.0/16</small>
Netmask	<input type="text" value="e.g. 255.255.255.0"/>
ACL List	<input type="text" value="- Create a new ACL list -"/>
<input type="button" value="Create Tier"/> <input type="button" value="Cancel"/>	

**Name** - name of this subnet.

**Display Text** - display name of this subnet.

**Network Offering** - select one of the offerings.

**Gateway** - must be within the CIDR of VPC.

**Netmask** - netmask of this subnet.

**ACL List** - select one of the existing ACL lists or select **Create a new ACL list for the system** to create a new one for you.

6. Click the red **Create** button.
7. Agree the Terms and Conditions.

The Notification Center will show the progress of the subnet creation. The page will be auto-refreshed after the new subnet is created.

#### 7.4.1.2.2 Edit Subnet

Users can edit the subnet in the subnet details page. There are 2 ways to go to the subnet details page:

1. Click the subnet **Name** or **Edit** button in **Networks** tab.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks 2 VPC 1 VPN Customer Gateways 0 Public IPs 2

+ Add Flat Network

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	2	0	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>
HK4-HKBN05-VPC Web Tier (HK4-HKBN05-VPC)	private	192.168.10.0/24	inactive	0	0	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>

2. Go to the **Subnet** tab in **VPC details** page and click the **Edit** button.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks 1 VPC 1 VPN Customer Gateways 0 Public IPs 2

+ Add VPC

Name	Cidr	Subnets	Associated VMs	Associated Public IPs	Status	Location	Zone	Actions
HK4-HKBN05-VPC	192.168.0.0/16	1	2	2	Enabled	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>

In the subnet details page, users can update the subnet's **Name** and/or **Display Name**. Once completed, click the **Update Network** button.

Home / Resource Pools / HKBNL955R / Network HK4-HKBN05-VPC-web

## Network HK4-HKBN05-VPC Web Tier (HK4-HKBN05-VPC)

Overview [ACL Rules](#)

[Update Network](#) [Delete](#)

Attribute	Value
Name	HK4-HKBN05-VPC-web
Display Name	HK4-HKBN05-VPC Web Tier
Type	private
Status	inactive
Zone Name	HK-DC03-ZN01
Provider	cloudstack
Location Code	HKS03
State	Allocated
Traffic Type	Guest
Gateway	192.168.10.1
Netmask	255.255.255.0
CIDR	192.168.10.0/24
DNS Server	8.8.8.8
Broadcast Domain Type	Vlan
Is System	false
ACL Type	Account
Domain ID	1b06c9cc-d677-4d7b-91d7-c50e4fdd7e94
Physical Network ID	9f6dfb29-5934-42bf-aad2-a6b3ec8f1afe
Network Offering ID	48585bc5-c132-4097-9c8b-637f2c24a1c
Associated VMs	No associated VMs found.

### 7.4.1.2.3 Subnet ACL Rules

To edit the ACL Rules of a subnet:

1. Go to the **VPC tab**.
2. Click the **VPC name** or **Edit** button to view the details of the VPC.
3. Click the **Subnets tab** and then click the **Edit** button of the subnet.
4. Click the **ACL Rules** tab.

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC

## VPC HK4-HKBN05-VPC

Overview Site-to-site VPN ACL Lists **3** Subnets **2** Public IPs **2**

Name	Description	
<input type="text"/>	<input type="text"/>	<a href="#">+ Add</a>
HK4-HKBN05-VPC-app-acl-list	Auto-created ACL list for HK4-HKBN05-VPC-app	<a href="#">Toggle Details</a> <a href="#">Delete ACL List</a>
HK4-HKBN05-VPC-web-acl-list	Auto-created ACL list for HK4-HKBN05-VPC-web	<a href="#">Toggle Details</a> <a href="#">Delete ACL List</a>

ACLs

Action	Traffic Type	Source CIDR	Protocol	Protocol No.	Start Port / ICMP Type	End Port / ICMP Code	
<input type="text" value="allow"/>	<input type="text" value="ingress"/>	<input type="text" value="0.0.0.0/0"/>	<input type="text" value="ALL"/>				<a href="#">+ Add</a>
Allow	Egress	0.0.0.0/0	ALL		All	All	<a href="#">Delete ACL</a>

You may drag and drop to reorder. [Update Order](#)

VPC_HK4-HKBN05-VPC_Tier_HK4-HKBN05-VPC-Network_ACL_7a2fe77d-198e-4189-a2e1-31cdae757e75	ACL for VPC_HK4-HKBN05-VPC_Tier_HK4-HKBN05-VPC-Network_ACL_7a2fe77d-198e-4189-a2e1-31cdae757e75	<a href="#">Toggle Details</a> <a href="#">Delete ACL List</a>
---	---	--

Users can add or delete ACL rules. Users can also reorder the ACL rules by dragging and dropping, and then click the **Update Order** button. By default, the “Egress allows all” rules was added during creation.

#### 7.4.1.2.4 Delete Subnet

1. Go to the **VPC tab**.
2. Click the **VPC name** or **Edit** button to view the details of the VPC.
3. Click the **Subnets tab**.
4. Click the red **Delete Subnet** button.

Please note that users cannot delete a subnet with any associated VM.

#### 7.4.1.3 Acquire IP

There are 2 ways to acquire New IP to a VM.

1. Go to the VM details page and click the **Acquire Public IP for Static NAT** button.

Home / Instance / vm01

## vm01



Overview Volumes VM Snapshot

## Overview



Cloud / Location	HKBN, HKS03
OS	Windows 2008 R2 Datacenter SP1 (120GB Root Volume)
State	Running

Instance ID	88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Name	TGGO-88a3a8cc-2b93-4ce4-9e21-1b259103d9db
Display Name	vm01
Description	N/A
Compute Details	<a href="#">Resize</a> Standard (4GB RAM, 2*vCPU)
ISO Attachment	<a href="#">Detach</a> vmware-tools.iso - CentOS 4.5 (32-bit) [3a99e3bf-4d34-459b-8ace-127cfe5eea57]
Lifetime policy	<a href="#">Update</a> Never Expires

Login [Reset Password](#)

User name	Administrator
Last known password	<a href="#">Show</a> *****

## Journal

Created at	2016-07-04 15:11:46
Created by	admin_hkbn1955
Last Synchronized	2016-07-25 10:21:07 - 9 minutes ago

Tags [Manage](#)

Key	Value
Workload	My Workload 2016-07-04
Author	admin_hkbn1955
Account	hkbn1955

Network Interfaces [Add Network Interface](#)

Nic 1 (default)	Network	HK4-HKBN05-VPC-Network
	IP	192.168.105.185
	Type	Isolated
	MAC Address	02:00:15:25:00:0d
	Public IP	<a href="#">+ Acquire Public IP for Static NAT</a>

2. Go to the **Network details page** by clicking the Network Name of **Edit** button in **Networks** tab.

Home / Resource Pools / Edit HKBN1955R

## Resource Pool - HKBN1955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks **2** VPC **1** VPN Customer Gateways **0** Public IPs **1**

[+ Add Flat Network](#)

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	<b>2</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>
My Network	private	192.168.1.0/24	inactive	<b>0</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>

1. Click the **Public IPs** tab in the **Network details page**.

Home / Resource Pools / HKBN1955R / Network mynetwork

## Network My Network

Overview Egress Rules **0** **Public IPs** **0**

Address	Zone	Associated VM	State	Actions
				<a href="#">Acquire New IP</a>

2. Click the **Acquire New IP** button.

[Acquire New IP](#)

3. Agree the Terms and Conditions.
4. The new IP should show up in the same page after it has been created. Click the **IP** or **Edit** button to go into the IP details page.

Home / Resource Pools / HKBNL955R / Network mynetwork

### Network My Network

Overview Egress Rules 0 Public IPs 1

Acquire New IP

Address	Zone	Associated VM	State	Actions
103.63.135.82 <span>Source Nat</span>	HK-DC03-ZN01	-	Allocated At 2016-07-25 10:37:54	<span>Edit</span>

5. Click the **Enable Static NAT** button in the **IP details page**.
6. Select one of the **VMs** from the drop down list then click the red **Enable Static NAT** button.

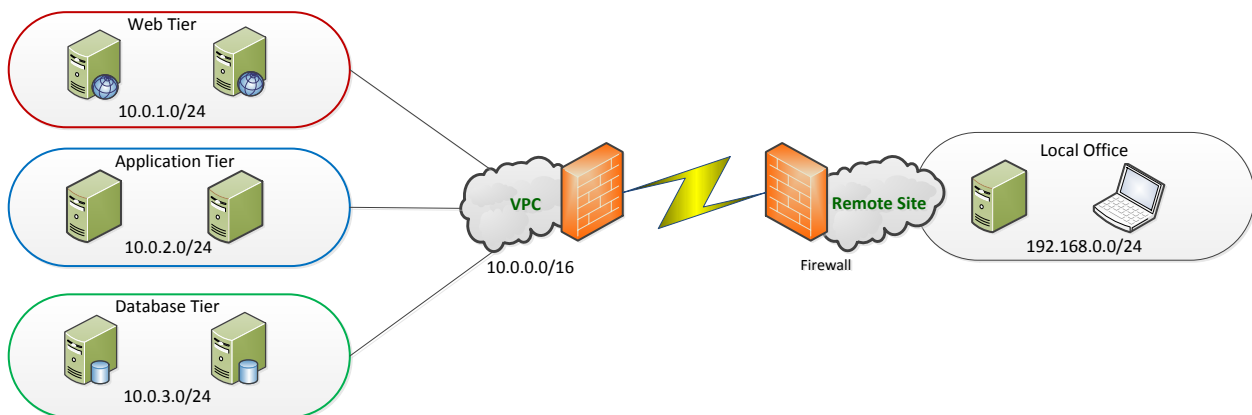
Please note that if the IP has any Port Forwarding or Load Balancer rules then this IP cannot enable Static NAT.

There are a few ways to release an IP.

1. Click the **Release IP** button in the VM details page.
2. Click the **Release IP** button in the Network > Public IPs tab.
3. Click the **Release IP** button in the Public IPs tab in Network details page.

Please note that the Source NAT IP cannot be released.

#### 7.4.1.4 VPC site-to-site VPN



Site-to-site VPN is supported by VPC, which enables VPN connection between VPCs and hardware-based VPN devices (e.g. firewall) at remote site such as your local office, datacenter or co-location facility network. A VPN customer gateway is needed for creating VPC site-to-site VPNs.

##### 7.4.1.4.1 VPC Customer Gateway

To view all of the VPN customer gateways, click the **VPN Customer Gateways** tab.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks 2 VPC 1 VPN Customer Gateways 0 Public IPs 2

+ Add VPN Customer Gateway

Name	Cidr	Using by VPC	Gateway
------	------	--------------	---------

Users can add, delete, or edit a VPN customer gateway.

To add a new VPN customer gateway:

1. Click the **Add VPN Customer Gateway** tab.
2. Fill in the following form.

Resource Pool - **HKBNL955R** Regions Usage & Limit **Networking** Offering Images Snapshots Volumes ISOs

Networks **2** VPC **1** VPN Customer Gateways **0** Public IPs **2**

[+ Add VPN Customer Gateway](#)

### Create VPN Customer Gateway

\* Name

\* Cidr

\* Gateway

\* IPsec Preshared-Key

ESP Policy

\* ESP Lifetime (Second)

IKE Policy

\* IKE Lifetime (Second)

Dead Peer Detection (DPD)

[✔ Create](#) [Cancel](#)

3. Click **Create** button.

To edit the VPN customer gateway:

1. Go to the **VPN Customer Gateways** tab.
2. Click the **Name** or **Edit** button.
3. Update the value and click the **Update Gateway** button.

To delete the VPN customer gateway:

1. Go to the **VPN Customer Gateways** tab.
2. Click the red **Delete** button.

#### 7.4.1.4.2 Setting up VPC site-to-site VPN

There must be at least one VPN customer gateway created in order to create a site-to-site VPN.

To add a new site-to-site VPN:

1. Go to the **VPC** tab.
2. Click the VPC **Name** or **Edit** button to the VPC details page.
3. Click the **Site-to-site VPN** tab.



Home / Resource Pools / Frank DA / VPC myvpc2

## VPC My VPC 2

Overview

Site-to-site VPN

ACL Lists 1

Subnets 1

Public IPs 1

### Connections

Customer Gateway	Passive	State
my-vpn-gateway	true	

[+ Add](#)

4. Select the **Customer Gateway** and click the **Add** button.
5. Then users should see the following:

Home / Resource Pools / Frank DA / VPC myvpc2

## VPC My VPC 2

Overview

Site-to-site VPN

ACL Lists 1

Subnets 1

Public IPs 1

Public IP: 59.100.125.153

ID: 012ecc82-a5b1-4502-aa64-f7f31bd1eaa3

### Connections

Customer Gateway	Passive	State
my-vpn-gateway	true	

[+ Add](#)

my-vpn-gateway	true	● Disconnected
----------------	------	----------------

[Toggle Details](#)  
[Delete VPN connection](#)

6. Click the **Toggle Details** button to **Reset** or **Refresh** the connection.

Home / Resource Pools / Frank DA / VPC myvpc2

## VPC My VPC 2

Overview

Site-to-site VPN

ACL Lists 1

Subnets 1

Public IPs 1

Public IP: 59.100.125.153

ID: 012ecc82-a5b1-4502-aa64-f7f31bd1eaa3

### Connections

Customer Gateway	Passive	State
my-vpn-gateway	true	

[+ Add](#)

my-vpn-gateway	true	● Disconnected
----------------	------	----------------

[Toggle Details](#)  
[Delete VPN connection](#)

[Reset Connection](#)
[Refresh](#)

7. Click the red **Delete VPN connection** button to delete it.

### 7.4.1.4.3 Example for configuring Site-to-Site VPN connection at customer's IT infrastructure

Cisco ASA, Juniper SRX and Juniper Netscreen are popular firewalls to terminate site-to-site VPN connection for enterprises. According to the parameter inside the captured screen in previous example, below are the suggested site-to-site VPN configuration of Cisco ASA, Juniper SRX and Juniper Netscreen at customer site.

**Note that if the equipment or configuration is different from below examples, greater effort and longer time may be needed for the planning and coordination of the setup.**

## 7.4.1.4.4 Cisco ASA Configuration

```
conf t
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 5
  lifetime 86400
crypto ikev1 enable outside
crypto ikev2 policy 1
  encryption aes-256
  prf sha
  lifetime seconds 3600
crypto ikev2 enable outside

crypto ipsec ikev1 transform-set V1-ESP-AES256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev2 ipsec-proposal V2-AES256-SHA1
protocol esp encryption aes-256
protocol esp integrity sha-1
exit
crypto ipsec security-association lifetime seconds 3600

object-group network CustomerLAN
network-object 192.168.100.0 255.255.255.0
object-group network VPC_Network
network-object 10.4.2.0 255.255.255.0
exit
access-list ACL_VPN_VPC extended permit ip object-group CustomerLAN object-group
VPC_Network

tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
ikev1 pre-shared-key SecretPassword
exit

crypto map map_outside 1 match address ACL_VPN_VPC
crypto map map_outside 1 set pfs group5
crypto map map_outside 1 set peer 1.1.1.1
crypto map map_outside 1 set ikev1 transform-set V1-ESP-AES256-SHA
crypto map map_outside 1 set ikev2 ipsec-proposal V2-AES256-SHA1
crypto map map_outside interface outside

nat (inside,outside) source static CustomerLAN CustomerLAN destination static
VPC_Network VPC_Network no-proxy-arp

end
write
```

#### 7.4.1.4.5 Juniper SRX Configuration

##### Phase-I (IKE VPN) configurations

```

set security ike proposal Pre-G5-AES256-SHA1 authentication-method pre-shared-keys
set security ike proposal Pre-G5-AES256-SHA1 dh-group group5
set security ike proposal Pre-G5-AES256-SHA1 authentication-algorithm sha1
set security ike proposal Pre-G5-AES256-SHA1 encryption-algorithm aes-256-cbc
set security ike proposal Pre-G5-AES256-SHA1 lifetime-seconds 86400
set security ike policy VPC-IKE-Policy mode main
set security ike policy VPC-IKE-Policy proposals Pre-G5-AES256-SHA1
set security ike policy VPC-IKE-Policy pre-shared-key ascii-text SecretPassword
set security ike gateway VPC-GW ike-policy VPC-IKE-Policy
set security ike gateway VPC-GW address 1.1.1.1
set security ike gateway VPC-GW external-interface reth0
set security ike gateway VPC-GW general-ikeid

```

Interface connected to Internet, depend on the customer device configuration.

##### Phase-II (IPSEC VPN) configurations

```

set security ipsec proposal ESP-G5-AES256-SHA1 protocol esp
set security ipsec proposal ESP-G5-AES256-SHA1 authentication-algorithm hmac-sha1-96
set security ipsec proposal ESP-G5-AES256-SHA1 encryption-algorithm aes-256-cbc
set security ipsec proposal ESP-G5-AES256-SHA1 lifetime-seconds 3600
set security ipsec policy VPC-IPSec-Policy perfect-forward-secrecy keys group5
set security ipsec policy VPC-IPSec-Policy proposals ESP-G5-AES256-SHA1
set security ipsec vpn VPC-VPN ike gateway VPC-GW
set security ipsec vpn VPC-VPN ike ipsec-policy VPC-IPSec-Policy
set security ipsec vpn VPC-VPN establish-tunnels immediately

```

Zone names depended on the customer device

To access protected resources, there should be traffic passing policy from untrust zone to trust zone where the protected resource is located, is configured as follows.

```

set security zones security-zone trust address-book address CustomerLAN 192.168.100.0/24
set security zones security-zone untrust address-book address VPC_Network 10.4.2.0/24

set security policies from-zone untrust to-zone trust policy VPC-CustomerSite match source-address VPC_Network
set security policies from-zone untrust to-zone trust policy VPC-CustomerSite match destination-address CustomerLAN
set security policies from-zone untrust to-zone trust policy VPC-CustomerSite match application any
set security policies from-zone untrust to-zone trust policy VPC-CustomerSite then permit tunnel ipsec-vpn VPC-VPN
set security policies from-zone untrust to-zone trust policy VPC-CustomerSite then permit tunnel pair-policy CustomerSite-VPC

```

```
set security policies from-zone untrust to-zone trust policy VPC-CustomerSite then log
session-init
```

```
set security policies from-zone trust to-zone untrust policy CustomerSite-VPC match source-
address CustomerLAN
```

```
set security policies from-zone trust to-zone untrust policy CustomerSite-VPC match
destination-address VPC_Network
```

```
set security policies from-zone trust to-zone untrust policy CustomerSite-VPC match
application any
```

```
set security policies from-zone trust to-zone untrust policy CustomerSite-VPC then permit
tunnel ipsec-vpn VPC-VPN
```

```
set security policies from-zone trust to-zone untrust policy CustomerSite-VPC then permit
tunnel pair-policy VPC-CustomerSite
```

```
set security policies from-zone trust to-zone untrust policy CustomerSite-VPC then log
session-init
```

```
insert security policies from-zone trust to-zone untrust policy CustomerSite-VPC before policy
AllowAllOutgoing
```

Depend on the customer device,  
it should be the last policy.

#### Configure NAT OFF for VPN traffic

```
set security nat source rule-set trust-to-untrust from zone trust
```

```
set security nat source rule-set trust-to-untrust to zone untrust
```

```
set security nat source rule-set trust-to-untrust rule VPC-NAT-OFF match source-address
192.168.100.0/24
```

```
set security nat source rule-set trust-to-untrust rule VPC-NAT-OFF match destination-address
10.4.2.0/24
```

```
set security nat source rule-set trust-to-untrust rule VPC-NAT-OFF then source-nat off
```

```
insert security nat source rule-set trust-to-untrust rule VPC-NAT-OFF before rule source-nat-
rule
```

Rule name depended on the  
customer device, it should be the last  
rule.

#### 7.4.1.4.6 Juniper Netscreen Configuration

```

set ike p1-proposal "Pre-G5-AES256-SHA1" preshare group5 esp aes256 sha-1 second 86400
set ike p2-proposal "ESP-G5-AES256-SHA1" group5 esp aes256 sha-1 second 3600
set ike gateway GW_VPC address 1.1.1.1 main outgoing-interface ethernet1 preshare
SecretPassword proposal Pre-G5-AES256-SHA1
set ike gateway GW_VPC nat-traversal
set vpn VPC gateway GW_VPC tunnel proposal ESP-G5-AES256-SHA1
set address Untrust VPC_Network 10.4.2.0/24
set address Trust CustomerLAN 192.168.100.0/24
set policy top name VPN_To_VPC from Trust to Untrust CustomerLAN VPC_Network any tunnel
vpn VPC
set policy top name VPN_From_VPC from Untrust to Trust VPC_Network CustomerLAN any
tunnel vpn VPC
save

```

Interface name  
depended on the  
customer device.

## 7.4.2 Flat Network

In case when client-to-server VPN is needed (L2TP/IPSEC), customer could create a Flat Network via the cloud portal.

### 7.4.2.1 Create / Delete Flat Network

To create a flat network:

1. Click the **Networks** tab.
2. Click the **Add Flat Network** button.

[+ Add Flat Network](#)

3. Fill in the **Create Flat Network** form:

Networks **1** VPC **1** VPN Customer Gateways **0** Public IPs **1**

[+ Add Flat Network](#)

### Create Flat Network

\* Name

\* Display Text

Zone

Network Offering

\* Gateway

\* Netmask

[✓ Create](#) [Cancel](#)

**Name** - flat network name.

**Display Text** - flat network display name.

**Zone** - the name of the zone this network applies to.

**Network Offering** - select one of the network offerings.

**Gateway** - this flat network gateway. E.g. 192.168.1.1  
**Netmask** - this flat network netmask. E.g. 255.255.255.0

4. Click **Create** button.
5. Agree the Terms and Conditions.

The Notification Center will show the progress of the network's creation. The page will be auto-refreshed after the new flat network is created.

#### To delete a flat network:

1. Click the **Resource** icon from the **Top Nav** menu.
2. Click the **Networking** tab in Resource Pool page.
3. Click the **Networks** tab.
4. Find the network that you want to delete, then click **Delete** button.

Please note that network cannot be deleted if the flat network is associated with any VM.

The **Networks** tab shows how many VMs are associated with this flat network. Mouse over **Associated VMs** to show the correspondent VM names.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks **2** VPC **1** VPN Customer Gateways **0** Public IPs **1** + Add Flat Network

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	<b>2</b> vm01 vm02	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>
My Network	private	192.168.1.0/24	inactive	<b>0</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>

#### 7.4.2.2 Add / Remote Egress Rule

To add Egress rule in a flat network:

1. Click the **Resource** icon from the **Top Nav** menu.
2. Click the **Networking** tab in Resource Pool page.
3. Click the **Networks** tab.
4. Find the flat network then click the **Edit** button or click on the **Name** of the network to edit the details of this flat network.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit Networking Offering Images Snapshots Volumes ISOs

Networks **2** VPC **1** VPN Customer Gateways **0** Public IPs **1** + Add Flat Network

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	<b>2</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>
My Network	private	192.168.1.0/24	inactive	<b>0</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>

5. Click the **Egress Rules** tab.

[Home](#) / [Resource Pools](#) / [HKBNL955R](#) / [Network mynetwork](#)

## Network My Network

[Overview](#)

Egress Rules **0**

Public IPs **0**

Source cidr	Protocol	Start Port / ICMP Type	End Port / Icmp Code	
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="TCP"/>	<input type="text" value="e.g. 22"/>	<input type="text" value="e.g. 22"/>	<input type="button" value="+ Add Rule"/>

6. Enter the source cidr, select protocol, start port / ICMP type and end port / ICMP code then click the **Add Rule** button.

To remove an Egress rule.

1. Go back to your flat network egress rules tab.
2. Find the egress that you want to remove.
3. Click the red **Delete Egress Rule** button.

[Home](#) / [Resource Pools](#) / [HKBNL955R](#) / [Network mynetwork](#)

## Network My Network

[Overview](#)

Egress Rules **1**

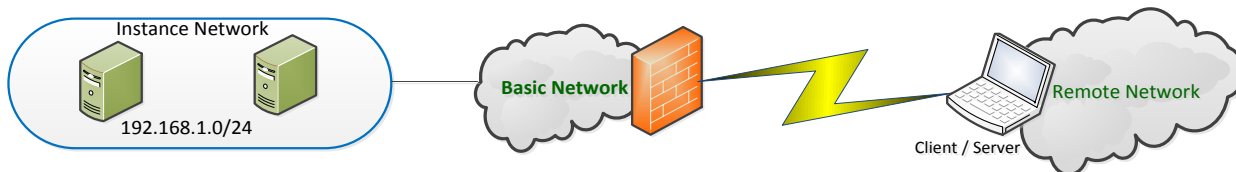
Public IPs **0**

Source cidr	Protocol	Start Port / ICMP Type	End Port / Icmp Code	
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="TCP"/>	<input type="text" value="e.g. 22"/>	<input type="text" value="e.g. 22"/>	<input type="button" value="+ Add Rule"/>
0.0.0.0/0	TCP	22	22	<input type="button" value="Delete Egress Rule"/>

### 7.4.2.3 Acquire New / Release IP

Users can acquire new IPs from the VM details page or you can go to the Public IP tab in the **Networks details** page and click the **Acquire New IP** button. Then click the **Enable Static NAT** button in the IP details page. The same steps can be applied to acquiring new IPs for a flat network. Please see the **Acquire New / Release IP** section under **VPC Network** for more details.

### 7.4.2.4 Configure remote access VPN using L2TP/IPsec Enabled Client



Available in Flat Network, enable external host access to cloud virtual servers securely using L2TP/IPsec client.

To add client to site VPN:

- Click the **Resource** icon in the **Top Nav** menu.
- Click **Networking** tab in the **Resource Pool** page.
- Click **Public IPs** tab.

Home / Resource Pools / Edit admin\_hdsdemo\_p

## Resource Pool - admin\_hdsdemo\_p

Regions Usage & Limit Networks Offering Templates Snapshots Volumes ISOs

Flat Network **2** VPC **1** VPN Customer Gateways **0** Public IPs **2**

Address	Network / VPC	Zone	Associated VM	State
202.77.40.252 <a href="#">Source Nat</a>	demo 910 VPC	HK-DC01-ZN01	-	Allocated At 2016-06-16 08:55:31 <a href="#">Edit</a>
202.77.40.245 <a href="#">Source Nat</a>	My Network	HK-DC01-ZN01	-	Allocated At 2016-06-24 04:02:00 <a href="#">Edit</a>

- Click and select the **Public IP** for the flat network to enable client to access site VPN
- Click **VPN** and **+ Enable Remote Access VPN**

Home / Resource Pools / admin\_hdsdemo\_p / Network myFlatnetwork / IP 202.77.40.245

## IP 202.77.40.245

Overview Firewall **0** Portforwarding **0** Load Balancer **0** VPN

Not Enabled

[+ Enable Remote Access VPN](#)

Home / Resource Pools / admin\_hdsdemo\_p / Network myFlatnetwork / IP 202.77.40.245

## IP 202.77.40.245

Overview Firewall **3** Portforwarding **0** Load Balancer **0** VPN

Your Remote Access VPN is currently enabled and can be accessed via the IP **202.77.40.245**.

Your IPsec pre-shared key is **DG2gRUgPKY82jecgZpWfkk3**

[Disable Remote Access VPN](#)

Username Password

admin  [+ Add](#)

- Input the Username and Password for remote access client.



#### 7.4.2.5 External Client setup for Remote Access VPN using L2TP/IPsec

- For the external host, set up a new connection for VPN client.

Change your networking settings



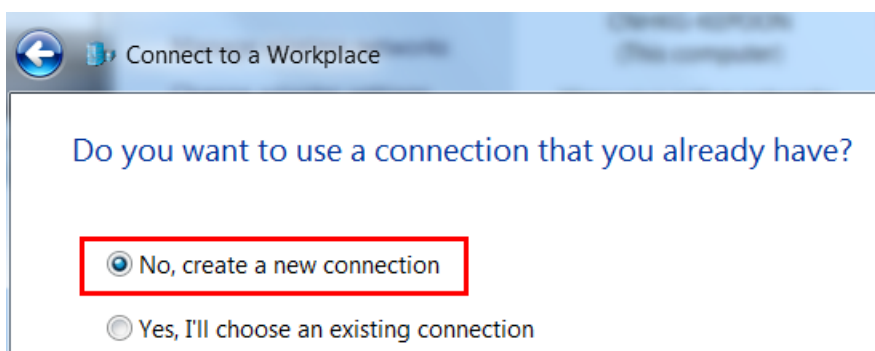
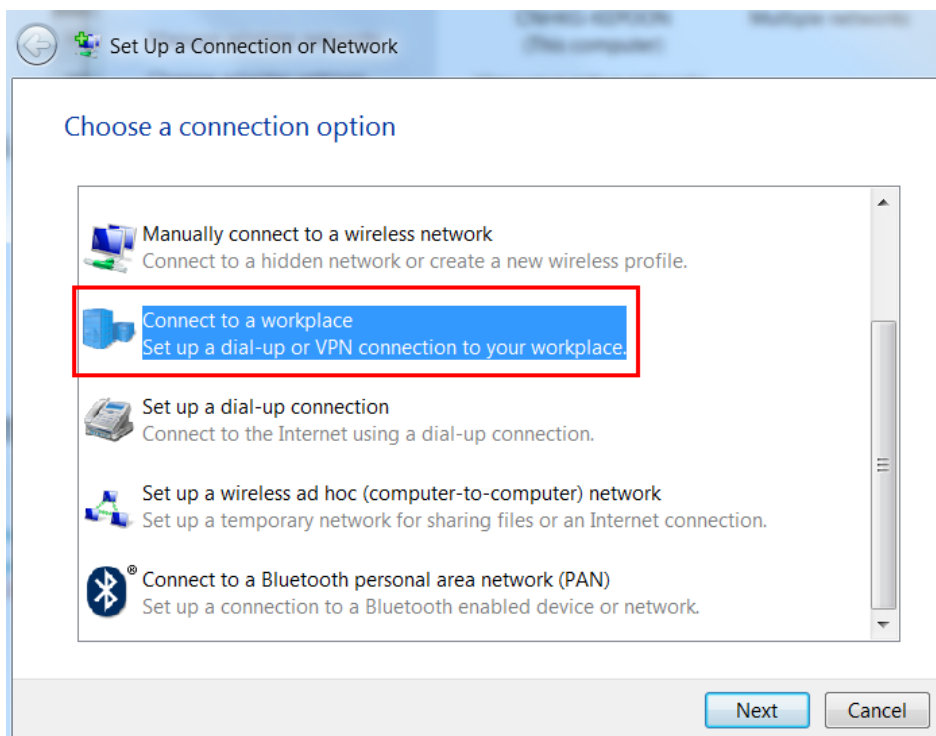
Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.



Connect to a network

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.



- For the Internet address, input your VPN Gateway IP address.

Connect to a Workplace

### Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

Don't connect now; just set it up so I can connect later

- Input your VPN user account login details. Click **Connect** to continue.

Connect to a Workplace

### Type your user name and password

User name:

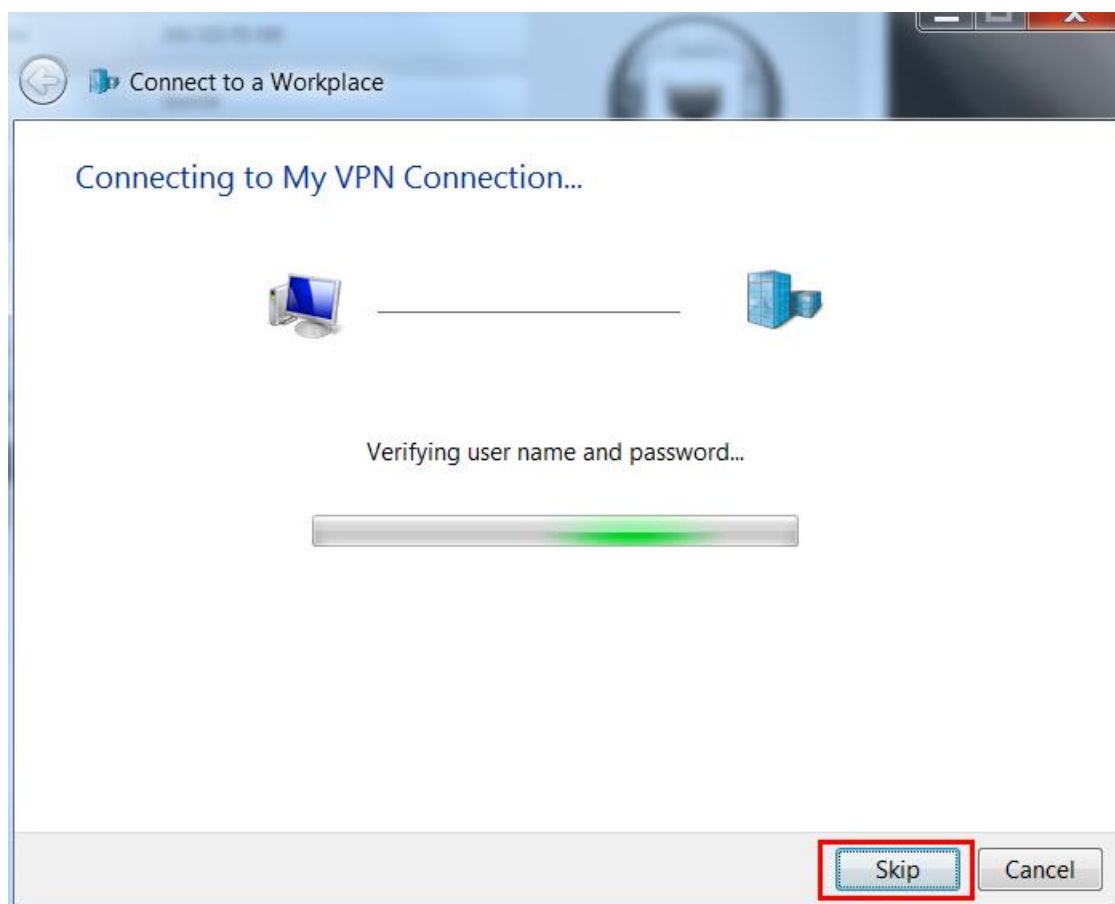
Password:

Show characters

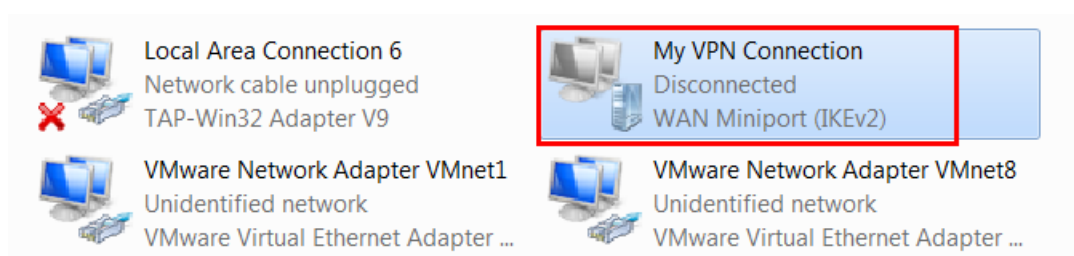
Remember this password

Domain (optional):

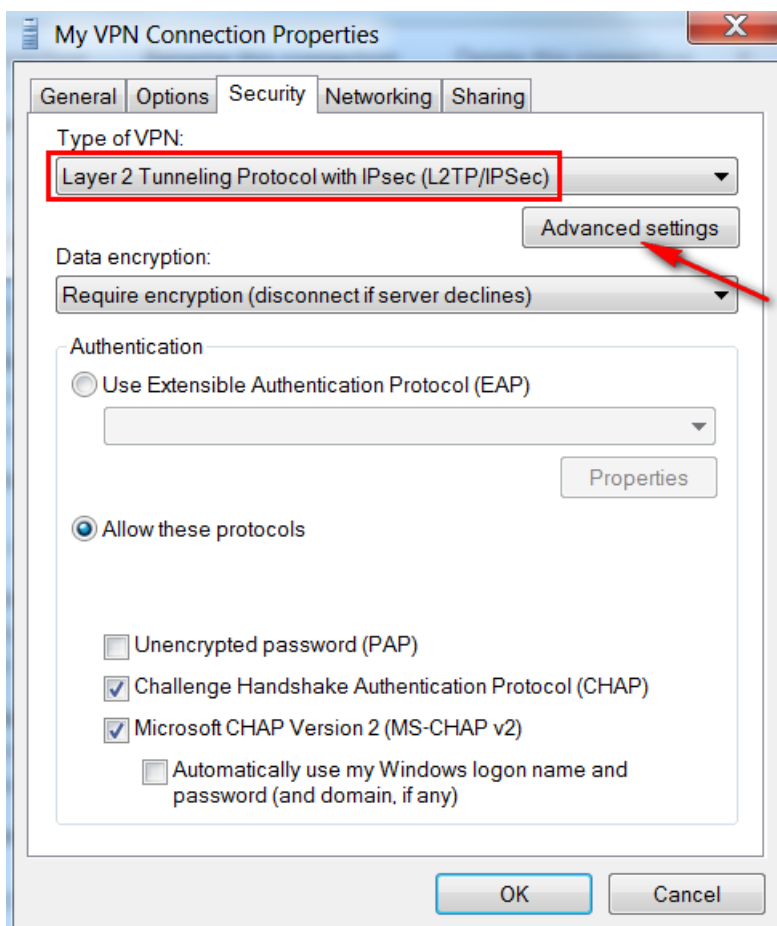
- Click **Skip** to continue.



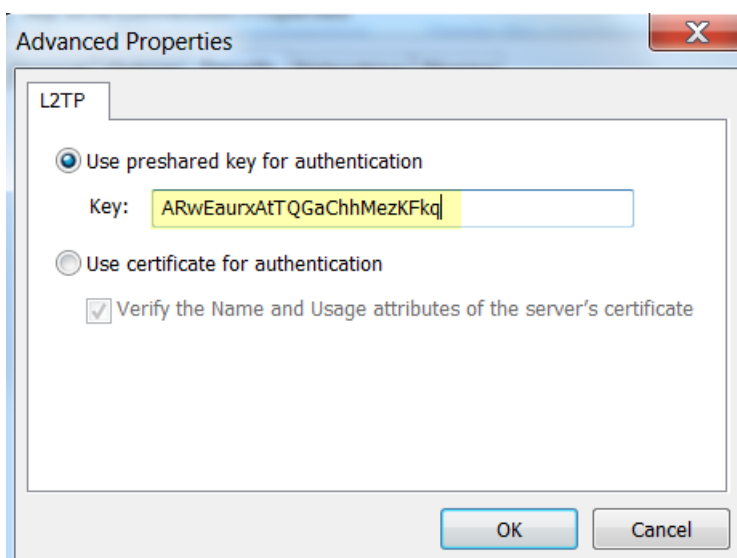
- Right click **My VPN Connection** icon.



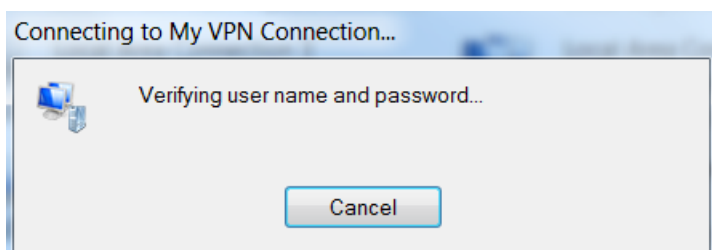
- Select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** as the Type of VPN. Click **Advanced setting** button to continue.



- Input the IPsec Preshared Key information to the below field. Click **OK** button to continue.



- Launch the VPN connection and input the user account login details.

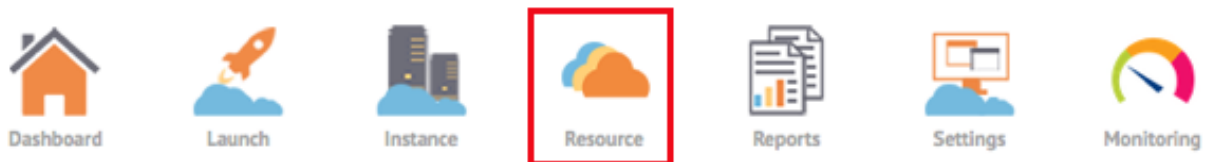


- Upon a successful login status, the external host should be able to access the virtual servers securely over IPsec encrypted connection.

## 7.4.3 Public IP

To view all Public IP addresses of all networks, VPCs and subnets:

- Click the **Resource** icon in the **Top Nav** menu.



- Click **Networking** tab in Resource Pool page.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit **Networking** Offering Images Snapshots Volumes ISOs

Networks **2** VPC **1** VPN Customer Gateways **0** Public IPs **2**

[+ Add Flat Network](#)

Name	Type	CIDR	Status	Associated VMs	Associated Public IPs	Location	Zone	Actions
HK4-HKBN05-VPC-Network (HK4-HKBN05-VPC)	private	192.168.105.0/24	active	<b>2</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>
HK4-HKBN05-VPC Web Tier (HK4-HKBN05-VPC)	private	192.168.10.0/24	inactive	<b>0</b>	<b>0</b>	HK503	HK-DC03-ZN01	<a href="#">Edit</a> <a href="#">Delete</a>

- Click **Public IPs** tab.

Home / Resource Pools / Edit HKBNL955R

### Resource Pool - HKBNL955R

Regions Usage & Limit **Networking** Offering Images Snapshots Volumes ISOs

Networks **2** VPC **1** VPN Customer Gateways **0** **Public IPs** **2**

Address	Network / VPC	Zone	Associated VM	State	Actions
103.63.135.225 <a href="#">Source Nat</a>	HK4-HKBN05-VPC	HK-DC03-ZN01	-	Allocated At 2015-10-29 17:31:13	<a href="#">Edit</a>
103.63.135.82	HK4-HKBN05-VPC	HK-DC03-ZN01	-	Allocated At 2016-07-25 11:02:34	<a href="#">Edit</a> <a href="#">Release IP</a>

It shows all public IPs in this page. Only Static NAT IP can be released. Click the IP or Edit button to go to the IP details page. Click the Network / VPC link to go to either the Network or VPC details page. Click the Associated VM to go to the VM details page.

### 7.4.3.1 Port Forwarding

To manage port forwarding of an IP:

- Go to the **IP details page**.
- Click the **Portforwarding tab**.

You can add a new port forwarding rule by entering the private start / end ports, public start / end ports, select protocol and VM.

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC / IP 103.63.135.82

## IP 103.63.135.82

Overview Portforwarding **1** Load Balancer **0**

Private Start	Private End	Public Start	Public End	Protocol	VM	State
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP	vm01	Active
80	80	80	80	TCP	vm01	Active

[+ Add](#) [Delete Portforwarding Rule](#)

Click the red **Delete Portforwarding Rule** button to remove any rule. Please note that the Port Forwarding is disabled when the IP is enabled Static NAT.

### 7.4.3.2 Load Balancer

To manage load balancer rules of an IP:

- Go to the **IP details page**.
- Click the **Load Balancer** tab.

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC / IP 103.63.135.82

## IP 103.63.135.82

Overview Portforwarding **0** Load Balancer **0**

Name	Public Port	Private Port	Algorithm	State	Network
<input type="text"/>	<input type="text"/>	<input type="text"/>	roundrobin		HK4-HKBN05-VPC-N

[+ Add](#)

- Enter the rule name, public / private port and select one of the algorithms then click **Add** button.
- After the rule is created, click the **Toggle Details** button to access the VM and Stickiness Policy.

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC / IP 103.63.135.82

## IP 103.63.135.82

Overview Portforwarding **0** Load Balancer **1**

Name	Public Port	Private Port	Algorithm	State
<input type="text"/>	<input type="text"/>	<input type="text"/>	roundrobin	
web	80	80	roundrobin	Add

[+ Add](#) [Toggle Details](#) [Delete Loadbalancer Rule](#)

**Instances assigned to this load balancer:**

Assign instances:

[Assign](#)

**Stickiness Policy:**

None [Edit](#)

Home / Resource Pools / HKBNL955R / VPC HK4-HKBN05-VPC / IP 103.63.135.82

IP 103.63.135.82

Overview

Portforwarding 0

Load Balancer 1

Name	Public Port	Private Port	Algorithm	State	
<input type="text"/>	<input type="text"/>	<input type="text"/>	roundrobin		<input type="button" value="+ Add"/>
web	80	80	roundrobin	Active	<input type="button" value="Toggle Details"/> <input type="button" value="Delete Loadbalancer Rule"/>

**Instances assigned to this load balancer:**

- vm01 TGG0-88a3a8cc-2b93-4ce4-9e21-1b259103d9db ()

**Assign instances:**

**Stickiness Policy:**

None

\* Method

- None
- SourceBased
- AppCookie
- LbCookie

### Stickiness Policy

**None:** Do not use stickiness policy

**SourceBased:** The source IP address is used to identify the user and locate user's stored data

**AppCookie:** Cookies are used. The cookie generated by the application is included in request and response URLs to create persistence

**LbCookie:** Cookies are used. The cookie generated by the Load Balancer is included in request and response URLs to create persistence

Click the red **Delete Loadbalancer Rule** button to remove any rule.

Please note that the Load Balancer is disabled when the IP is enabled with Static NAT.



### 7.4.3.3 VPN

To enable VPN:

- Go to the **IP details** page.
- Click the **VPN tab**.

[Home](#) / [Resource Pools](#) / [HKBNL955R](#) / [Network mynetwork](#) / IP 103.63.135.82

IP 103.63.135.82

Overview

Firewall 0

Portforwarding 0

Load Balancer 0

VPN

Not Enabled

[+ Enable Remote Access VPN](#)

- Click the **Enable Remote Access VPN** button.
- After the VPN remote access is enabled, you should see the following:

[Home](#) / [Resource Pools](#) / [HKBNL955R](#) / [Network mynetwork](#) / IP 103.63.135.82

IP 103.63.135.82

Overview

Firewall 3

Portforwarding 0

Load Balancer 0

VPN

Your Remote Access VPN is currently enabled and can be accessed via the IP **103.63.135.82**.

Your IPsec pre-shared key is **EhzXYxgYHQdrwf85r86Qr8YQ**

[Disable Remote Access VPN](#)

Username

Password

admin\_hkbnl955

\*\*\*\*\*

[+ Add](#)

- Add the username and password to access the VPN.

## 7.5 Templates

Users can create VM easily by using VM templates, or import a VM by uploading VM template in OVA format.

### 7.5.1 Upload Templates

To upload a template:

- Click the **Templates** tab in Resource Pool page.

[Home](#) / [Resource Pools](#) / [Edit Frank DA](#)

Resource Pool - Frank DA

Regions

Usage & Limit

Networking

Offering

Templates

Snapshots

Volumes

ISOs

ALL Locations

Name of Templates

[Upload](#)

[Refresh](#)

Name	OS Type	Status	Size	Zone	Location	Action
CentOS 6.4 (64-bit) Basic Server (120GB Root Volume)	centos 6.4		120.0 GB	DC01-ZN01	HDS AU	
CentOS 6.4 (64-bit) Basic Server (120GB Root Volume)	centos 6.4		120.0 GB	DC01-ZN02	HDS AU	
CentOS 6.4 (64-bit) Basic Server (180GB Root Volume)	centos 6.4		180.0 GB	DC01-ZN01	HDS AU	
CentOS 6.4 (64-bit) Basic Server (180GB Root Volume)	centos 6.4		180.0 GB	DC01-ZN02	HDS AU	
From Volume Snapshot CentOS 6_4 64-bit 2	centos 6.4		120.0 GB	DC01-ZN01	HDS AU	

- Click the Upload button.

Home / Resource Pools / Edit Frank DA

### Resource Pool - Frank DA

Regions Usage & Limit Networking Offering Templates Snapshots Volumes ISOs

ALL Locations Name of Templates

Name	OS Type	Status	Size	Zone	Location	Action
CentOS 6.4 (64-bit) Basic Server (120GB Root Volume)	centos 6.4		120.0 GB	DC01-ZN01	HDS AU	
CentOS 6.4 (64-bit) Basic Server (120GB Root Volume)	centos 6.4		120.0 GB	DC01-ZN02	HDS AU	
CentOS 6.4 (64-bit) Basic Server (180GB Root Volume)	centos 6.4		180.0 GB	DC01-ZN01	HDS AU	
CentOS 6.4 (64-bit) Basic Server (180GB Root Volume)	centos 6.4		180.0 GB	DC01-ZN02	HDS AU	
From Volume Snapshot CentOS 6_4 64-bit 2	centos 6.4		120.0 GB	DC01-ZN01	HDS AU	

- Please enter the following information in the Upload Your Own Cloud Template form:
  - Display Text and Name** - the name of this template.
  - URL** - the system will download the file from this URL. Eg. [http://www.mycompany.com/download/centos6\\_4-image.ova](http://www.mycompany.com/download/centos6_4-image.ova)
  - Zone** - choose one of the zones where you want the template to be available.
  - Hypervisor** - select one of the supported hypervisors. (Default: VMware)
  - Format** - the format of the template upload file. (Default: OVA)
  - Root disk controller** - this is an optional field for VMWare hypervisor. Specify the default disk controller for root volume. (Default: SCSI)
  - NIC adapter type** - this is an optional field for VMWare hypervisor. Specify the default network device type for system VMs. (Default: Vmxnet3)
  - Keyboard type** - this is an optional field for VMWare hypervisor. Select one of the keyboard device types. (Default: US Keyboard)
  - OS Type** - this helps CloudStack and the hypervisor perform certain operations and make assumptions that improve the performance of the guest.
  - Extractable** - check this if the template is available for extraction.
  - Password Enable** - check this if the template has the CloudStack password change script installed.
  - Dynamically Scalable** - check this if template contains XS/VMWare tools in order to support dynamic scaling of VM cpu/memory.
  - HVM** - check this if the template requires HVM.
- Click the Create button to create the template.
- Agree to the Terms and Conditions.
- You should see your uploaded template in the template list when the template is created successfully.

## 7.5.2 Download Templates

Users can download templates that have been updated to the system by the following steps:

- Click the **Templates tab** in the Resource Pool page.

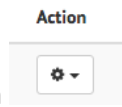
Action

- Select **Download** from the Action button .

### 7.5.3 Delete Templates

Users can delete templates that have been uploaded to the system by the following steps:

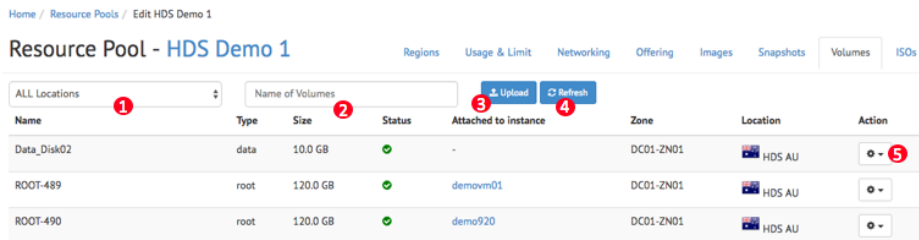
- Click the Templates tab in Resource Pool page.



- Select Delete from the Action button .

### 7.6 Volumes

Users can manage disk volumes by clicking on the **Volumes** tab. The following are key functions:



#### 1. Locations

Users can click on the **Locations** to select a location to display a list of volumes

#### 2. Name Search

Users can type a name to be searched

#### 3. Upload

Upload Volume ×

\* Name

\* URL

Zone

Format

Disk Offerings

Checksum

Users can upload a volume by providing the following info and click **Create**:

*Name:*

*URL:* location to download the disk volume

*Zone:* the zone to store the volume

*Format:* disk format

*Disk Offering:* for environment with more than one disk offering, specify the offering.

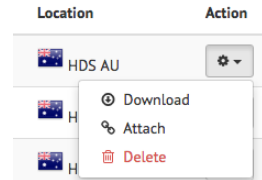
*Checksum:* check for consistency

#### 4. Refresh

Users can redisplay the list of volumes by clicking on the Refresh button

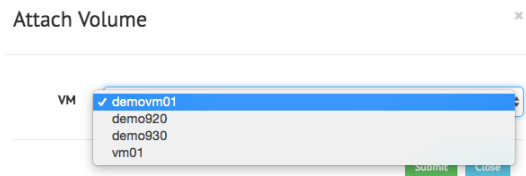
#### 5. Action

Users can download, attach or delete the volumes.



*Download: a new browser window will be opened to start downloading*

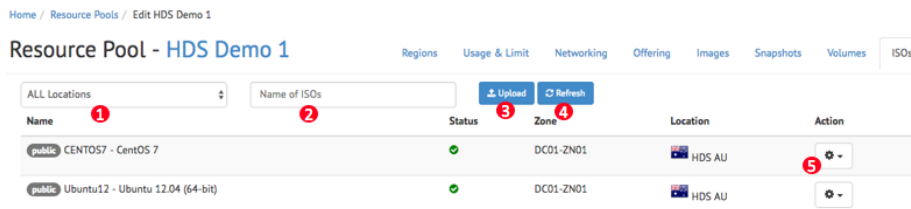
*Attach: select a VM from the dropdown list to attach the volume*



*Delete: delete the volume*

## 7.7 ISOs

Users can manage ISO images by clicking on the **ISO** tab. The following are key functions:



#### 1. Locations

Users can click on the **Locations** to select a location to display a list of volumes

#### 2. Name Search

Users can type a name to be searched

#### 3. Upload



Upload ISO ×

\* Name

\* Description

\* URL

OS Type

Zone

Bootable

Extractable

Users can upload an ISO image by providing the following info. and click **Create**:

*Name:*

*Description:*

*URL: location to download the ISO image*

*OS Type: select an OS format*

*Zone: the zone to store the ISO image*

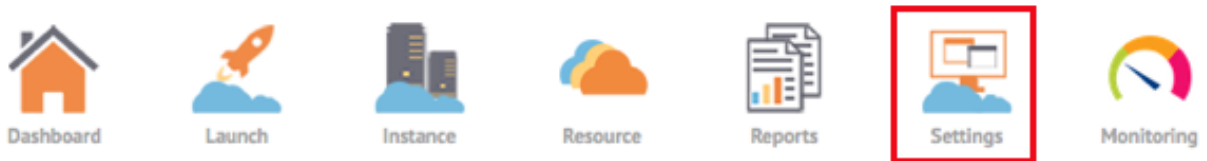
*Bootable: check if the ISO image is bootable*

*Extractable: check if the ISO image is extractable*

#### 4. Refresh

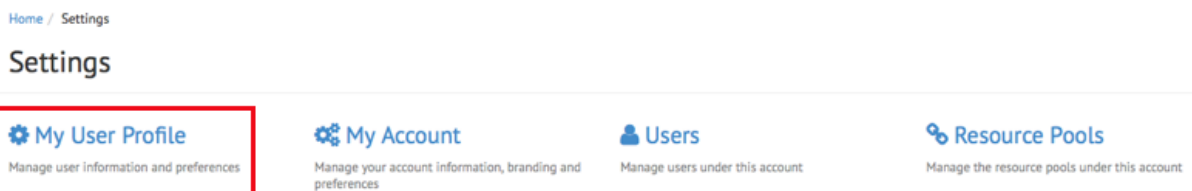
Users can redisplay the list of volumes by clicking on the **Refresh** button

## 8 Settings



The Settings Menu allows users to configure tenant and user level preferences.

### 8.1 My User Profile



The **My User Profile** section consists of 3 functions:

- General
  - Users can set and update contact information and change password.

Home / Users / My User Profile

### Edit My User Profile

General Preferences Access History

Login Name	admin_hkbn1955
* First Name	<input type="text" value="Trial V"/>
* Last Name	<input type="text" value="Admin"/>
* Email	<input type="text" value="hkbn_trial1955@togo.com.hk"/>
	<input type="button" value="Save"/>

---

Two-step verification	Enabled at 2016-07-21T02:31:15+00:00 (app).	<input type="button" value="Manage Settings"/>
Password	Password never changed	<input type="button" value="Change Password"/>

- Preferences
  - Users can set time zone preferences.

Home / Users / My User Profile

### Edit My User Profile

General Preferences Access History

Time Setting Preferences

Time Zone	<input type="text" value="(GMT+08:00) Hong Kong"/>
Time Format	<input type="text" value="%Y-%m-%d %H:%M:%S"/>
	<input type="button" value="Save"/>

- Access History
  - Detailed access records are kept.

Home / Users / My User Profile

### Edit My User Profile

General Preferences Access History

You are currently accessing from IP address 203.185.8.3.

Items/Page: 10 < 1 2 3 4 5 >

Date	IP Address	Estimated Location	Device	OS	Browser	Language	Status	Message
2016-07-25 09:44:31	203.185.8.3	HK, N/A, Central District	Other	Mac OS X 10.10	Firefox 47.0	en-US	success	Successfully logged in. OTP code verified.
2016-07-25 09:44:30	203.185.8.3	HK, N/A, Central District	Other	Mac OS X 10.10	Firefox 47.0	en-US	success	Password verified, asking for one time password.
2016-07-25 09:44:10	203.185.8.3	HK, N/A, Central District	Other	Mac OS X 10.10	Firefox 47.0	en-US	success	Password verified, asking for one time password.

## 8.2 My Account

Home / Settings

### Settings

**My User Profile**  
Manage user information and preferences

**My Account**  
Manage your account information, branding and preferences

**Users**  
Manage users under this account

**Resource Pools**  
Manage the resource pools under this account

The **My Account** section allows users to enter and update tenant level information. It consists of My Account, API Key and Branding.

### 8.2.1 My Account - General

Users can enter and update contact information.

Home / My Account

### My Account

General Preferences

\* **Company Name**

**Website**

**Address**

Street  City

State  Zip Code

United States

**Tel.**

**Fax**

**URL**

### 8.2.2 My Account - Preferences

The **Preferences** tab on the upper right side brings up the account **Preferences** page, with editable parameters for Monitoring and VM Lifetime policy.

[Home](#) / [My Account](#)

## My Account

[General](#)[Preferences](#)[Monitoring](#)[VM Lifetime Policy](#)[Save](#)[Back](#)

### 8.2.2.1 Monitoring

Enable / Disable email notification. Add email address(es) for this notification.

1. Go to the **My Account** page in **Settings** tab.
2. Click the **Preferences** tab.
3. Click the **Monitoring** text label.

[Home](#) / [My Account](#)

## My Account

[General](#)[Preferences](#)[Monitoring](#)**Email Notification**

Select if email notifications should be sent for events like user added, public IP attached or VM is terminated.

**Email Addresses**

Comma-separated email addresses that to receive notifications.

[VM Lifetime Policy](#)[Save](#)[Back](#)

4. Click the **Email Notification** check box if you want to receive email notifications.
5. Enter **Email Addresses** for those who will receive notification emails.
6. Click the **Save** button.

### 8.2.2.2 VM Lifetime Policy

Set the default value for the lifetime of the VM.

1. Go to the **My Account** page in Customer Portal.
2. Click the **Preferences** tab.
3. Click the **VM Lifetime Policy** text label.
4. Select the **Default value of VM lifetime** in the drop down menu.

[Home](#) / [My Account](#)

## My Account

[General](#)[Preferences](#)[Monitoring](#)[VM Lifetime Policy](#)**Default value of VM lifetime**

Refer to site preference setting

Refer to site preference setting

Never Expires

1h

3h

1d

7d

1m

1y

5. Click the **Save** button.

This will be the default value populated in **Lifetime** field in the **Launch VM** page.



Home / Resource Order

## + Launch VM

Workload  Life Cycle

Instance Name

Host Name

Lifetime

## 8.3 Users

HKBN Cloud platform is a multi-tenant and multi-user system with granular security controls. Administrators can add, modify and delete users from the tenant account. Each user will have his/her own login/password for accessing the HKBN Cloud Portal.

Home / Settings

### Settings

My User Profile

Manage user information and preferences

My Account

Manage your account information, branding and preferences

Users

Manage users under this account

Resource Pools

Manage the resource pools under this account

### 8.3.1 Add New User

Users with Admin roles can add user accounts on a tenant:

1. On the **Users Management** interface, click the **Add User** button.
2. Fill in the New User form by entering the **Login Name, First Name, Last Name, Email** and **Password**

Home / Users

## Users Management

Search Users

Cancel

## Add user to hkbnl955

\* Login Name   
Please enter alphanumeric and dot.

\* First Name

\* Last Name

\* Email

Active Status

\* Password

\* Password Confirmation

Roles  admin  poweruser  guest

3. Select the user's **Role**.

**Guest** – This group allows a user to view server, to access remote console and different types of resources including VM, disks, network, etc.

**Power Users** – This group allows to access most administration functions. A power user is able to view, create, delete, and manage all types of resources within the tenant.

**Admin** – This group allows to access most administration functions. In addition, an Admin account can also access to user management page to add, delete or modify user.

4. Click the **Save** button.
5. The newly added users will appear in the **Users Management** interface.

### 8.3.1.1 Modify User Properties

Users with Admin roles can edit user properties:

1. In the **Users Management** interface, click the **Edit** button in the **Actions** column of the user's name.
2. You will be redirected to the **Edit User** page. Modify the necessary fields.
3. Click the **Save** button.

### 8.3.1.2 Delete User

Users with Admin roles can delete user accounts on a tenant:

1. In the **Users Management** interface, mouse over to the **Actions** column of the user's name.
2. Click the **Drop User** button.
3. A dialog box will prompt the administrator to delete the user.
4. Click the **OK** button.

**Note: This action will permanently remove user records and settings in the system.**

### 8.3.1.3 Add User to Approval\_flow

Users with Admin roles can assign users to approval chains:

1. In the **Users Management** interface, click the **Edit** button in the **Actions** column of the user's name.
2. You will be redirected to the **Edit User** page. Scroll down to Approval section.

[Home](#) / [Users](#) / [Edit User](#)

## Edit User

General

Access History

* Login Name	<input type="text" value="admin_hkbnl955"/>
	<small>Please enter alphanumeric and dot.</small>
* First Name	<input type="text" value="Trial V"/>
* Last Name	<input type="text" value="Admin"/>
* Email	<input type="text" value="hkbn_trial955@tggo.com.hk"/>
Active Status	<input type="text" value="True"/>
Password	<input type="text"/>
	<small>Leave Blank if you don't want to change password.</small>
Password Confirmation	<input type="text"/>
	<small>Leave Blank if you don't want to change password.</small>
Roles	<input checked="" type="checkbox"/> admin <input type="checkbox"/> poweruser <input type="checkbox"/> guest
	<input type="button" value="Save"/> <input type="button" value="Preview Permissions"/>

## Approval

Chain	<input type="text" value="HKBNL955_Default_Approval_Chain"/>
	<input type="button" value="Submit"/> <input type="button" value="Back"/>

3. Select the **Default\_Approval\_Chain** and click the **Save** button.

Note: A simple Default Approval Chain is pre-configured and available for selection, which request approval by Admin account for every work order (e.g. VM provisioning / termination). Approval chain can be fine-tuned by HKBN to meet customer's need, please contact your account manager for details.

## 9 Monitoring

The Monitoring Menu contains functions for managing integrated cloud monitoring.



### 9.1 Login the Monitoring tool

1. Enter **Login Name** and **Password (Same as portal)**, then click Login.

PRTG NETWORK MONITOR (HKDC01-PR...

Login Name

Password

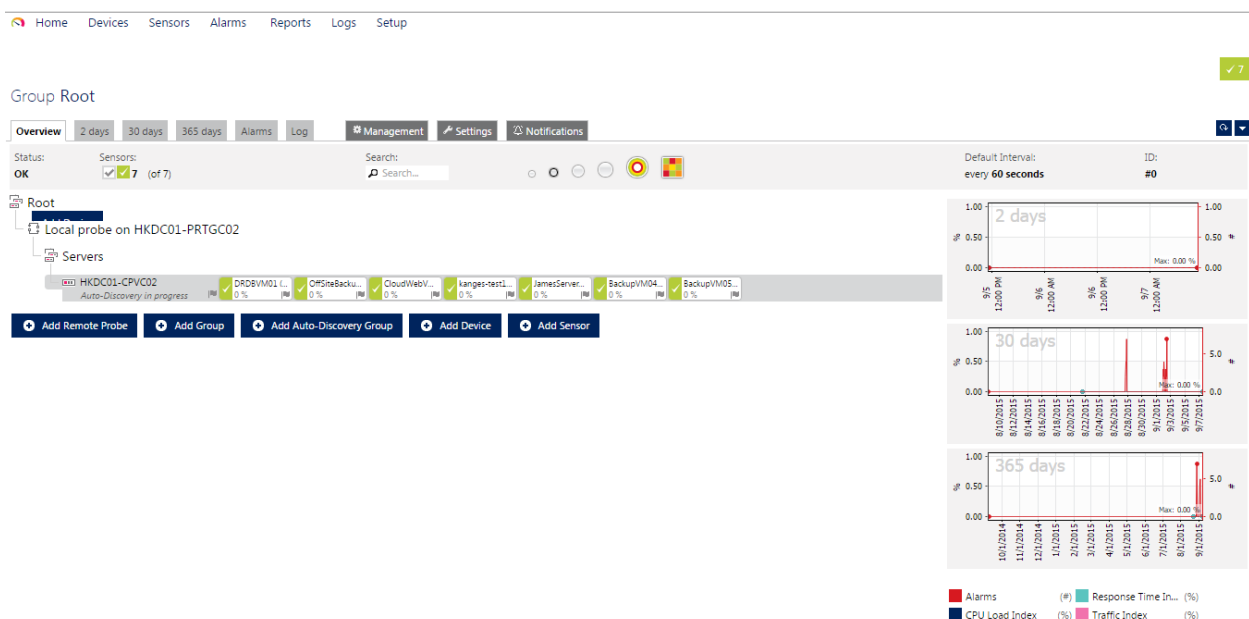
- Use AJAX Web GUI (All features, optimized for desktop access)
- Use Mobile Web GUI (Limited functionality, optimized for mobile access)
- Download Client Software (for Windows, iOS, Android)

**Login**

[Forgot password? Need Help?](#)

2. After a successful login, you can view information in dashboard including the followings:-

- Overview your managing devices
- Devices current status



## 9.2 View your device information & detail

### 9.2.1 Launch more status & resource usage

1. Click device you want to check



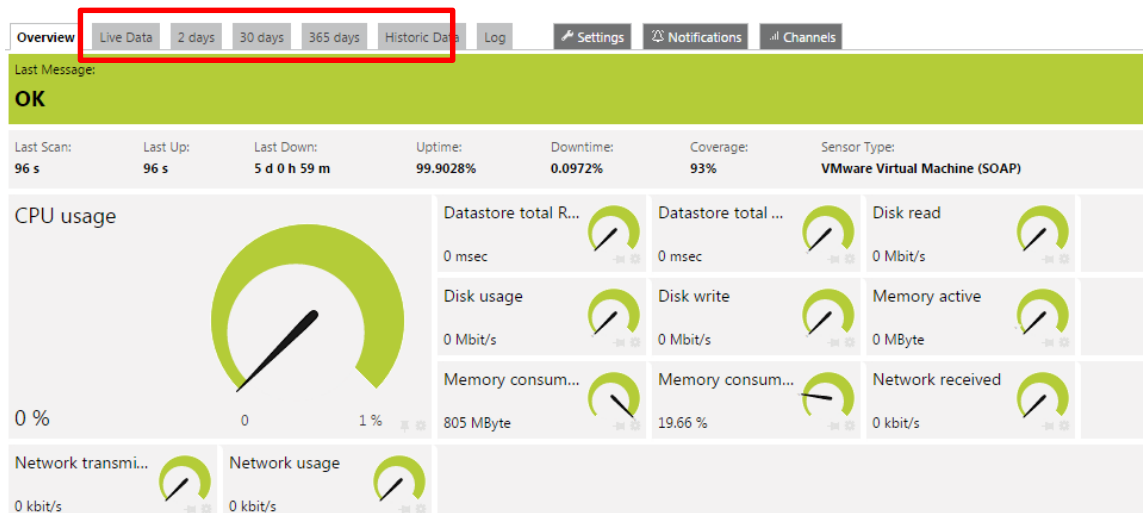
2. Device Dashboard



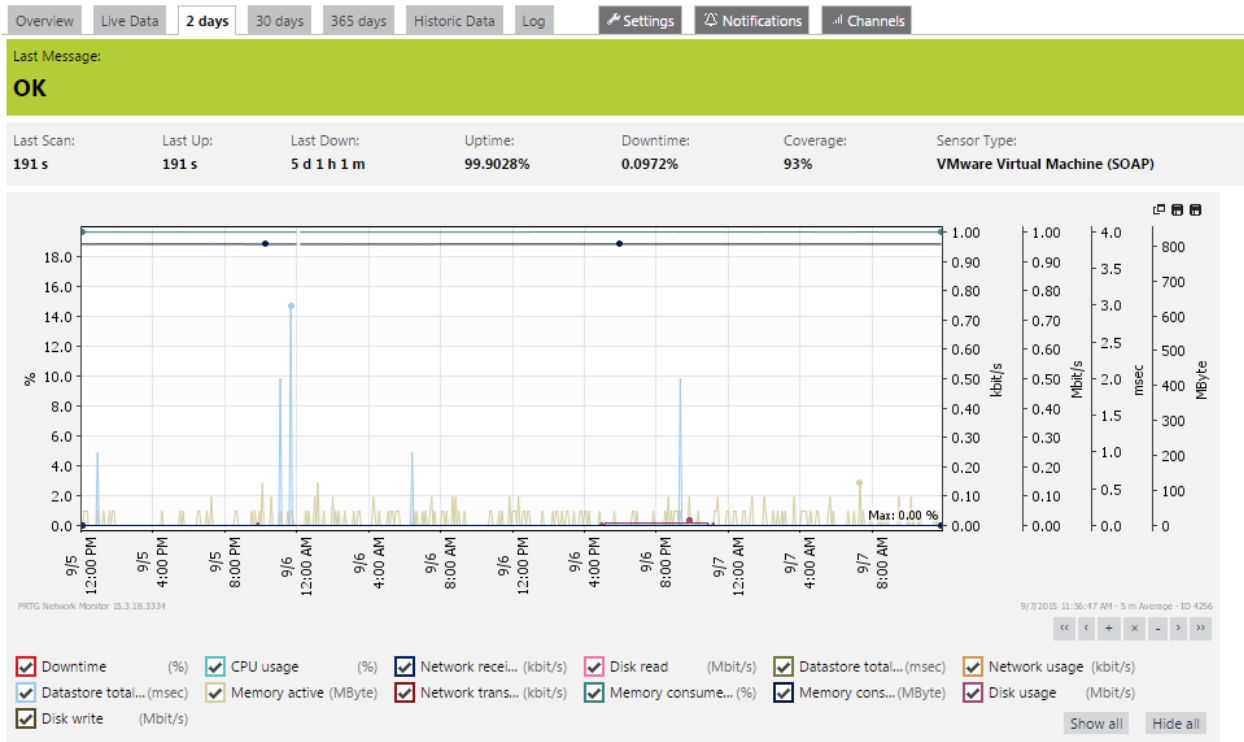
Shown device current status (Last up time, Last down time, Uptime percent, Downtime percent & Coverage) & resource usage (CPU, Memory, Disk & network etc).

### 9.2.2 View the performance data by chart

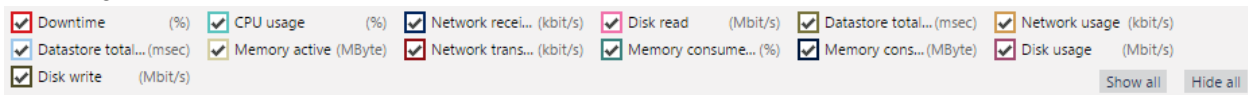
1. Select the time period in device dashboard



2. Show the resource usage in the format of chart and table



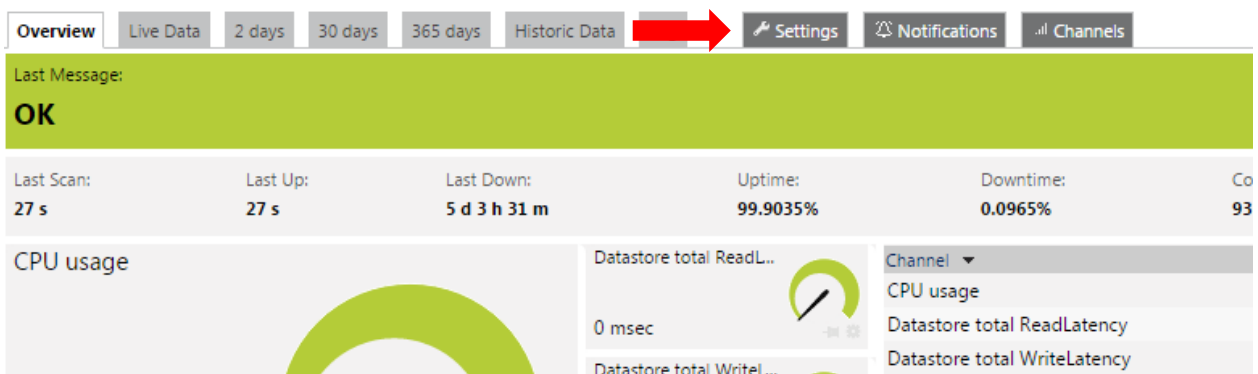
3. Select the checkbox to show or hide the graph. Also you can select “show all” & “hide all”.



9.3 Manage your device monitoring setting

9.3.1 Edit the Device setting

1. Select the settings in device dashboard.



2. Fill in and select your options in the Setting page for device

**BASIC SENSOR SETTINGS**

Sensor Name: DRDBVM01 (i-49-237-VM)

Parent Tags: guru

Tags: esxservvmsensor

Priority: ★★★★★

**VMWARE VIRTUAL MACHINE SETTINGS**

MoID: vm-860

Handling of "Powered Off" VM:
 

- Ignore "powered off" state (default)
- Alarm when VM is "powered off"

**SENSOR DISPLAY**

Primary Channel: CPU usage (%)

Chart Type:
 

- Show channels independently (default)
- Stack channels on top of each other

**SCANNING INTERVAL**

inherit from HKDC01-CPVC02 (Scanning Interval: 60 seconds, Set sensor to ...)

Scanning Interval: 30 seconds

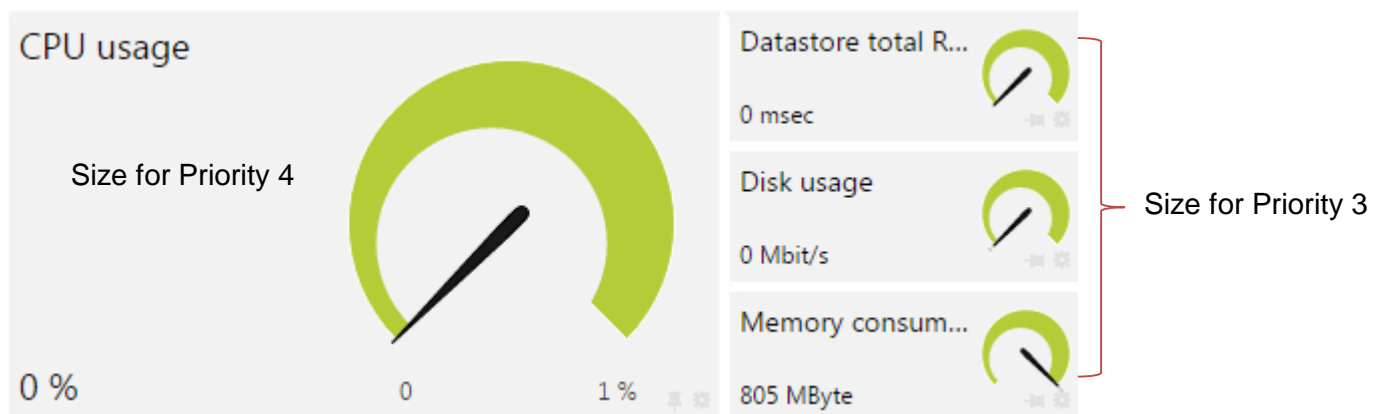
When a Sensor Reports an Error: Set sensor to warning for 1 interval, then set to "down" (recommended)

**SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW**

inherit from HKDC01-CPVC02

**BASIC SENSOR SETTINGS**

- Sensor Name : Enter a meaningful name to identify the sensor. By default, system shows this name in the device tree, in alarms, logs, notifications, reports, maps, libraries, and tickets. **(No recommend change it)**
- Parent Tag : **Don't change**
- Tag : **Don't change**
- Priority : Define the priority status of this object. System sorts this object in lists according to its priority, and the resource will be resized by priority. Below is an example for priority 3 & 4.



**VMWARE VIRTUAL MACHINE SETTINGS**

- Handling of "Powered Off" VM : **Ignore "powered off" state (default)** - In default setting, the sensor will not report a 'down' status when a virtual machine is powered off. If the powered off status is ignored, the sensor will report 0 value instead.  
**Alarm when VM is "powered off"** – The system will show the error when VM is powered off, even the manual is power off.

## SENSOR DISPLAY

- Primary Channel : Choose the resource you want to classify as primary. The newest value of the primary resource will always be displayed for this sensor. The primary resource can also be used to trigger notifications.
- Chart Type : Select how to display the graph. If you choose 'Show resources independently', every resource is displayed in a individual graph. Choose "Stack resources on top of each other" to create a multi- resource graph.  
**Recommend to use "Show channels independently (default)"**

## SCANNING INTERVAL

- Scanning Interval : Time between 2 scans of resource data
- When a Sensor Reports an Error : When a sensor reports an error, system can try reaching the corresponding device again with the next scanning interval before the sensor is shown as 'down'. This can avoid false alarms if your device has temporary issues only.

### 9.3.2 Suspend device monitoring

1. Unclick the checkbox under "Schedules, Dependencies, and Maintenance Window"

**SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW**

Inherit from ■ HKDC01-CPVC02

Dependencies, schedules and maintenance windows always pause all sensors inside a group/device. This pausing is always inherited to all sub-objects and the inheritance can not be disabled. Below you can set additional schedules, maintenance windows or dependencies that will be used on top of any inherited setting.

Schedule	None <span style="float: right;">▼</span>
Maintenance Window	<input checked="" type="radio"/> <b>Not set (monitor continuously)</b> <input type="radio"/> Set up a one-time maintenance window
Dependency Type	<input checked="" type="radio"/> <b>Use parent</b> <input type="radio"/> Select object <input type="radio"/> Master object for parent
Delay (Seconds)	0

- Schedule : **Set "None"**
- Maintenance Window : **Not set (monitor continuously)** – No set to Maintenance mode.  
**SET UP A ONE-TIME MAINTENANCE WINDOW** – Select this option will show the fields "Maintenance Begins At" & "Maintenance Ends At". Enter the time period you want to ignore.

Maintenance Begins At	2015-09-07 12:16	
Maintenance Ends At	2015-09-07 12:16	

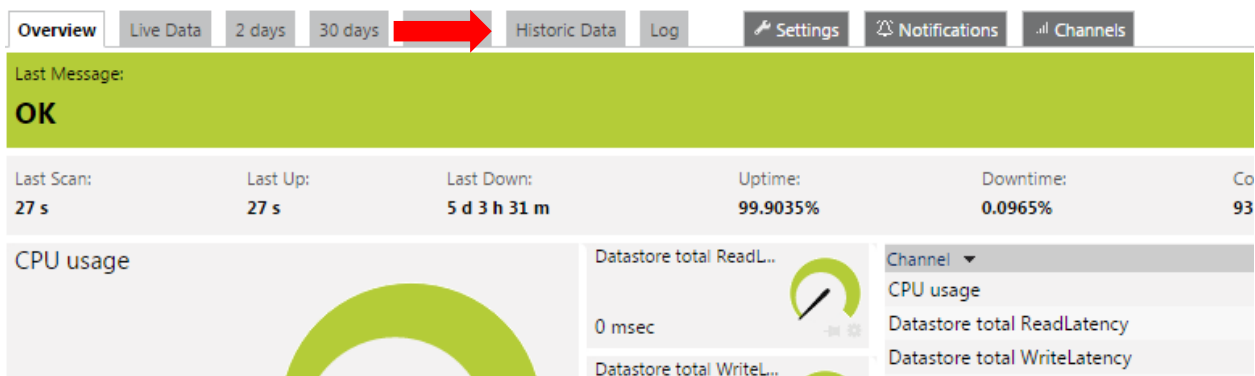
- Dependency Type : **Use default setting, no need to set.**
- Delay (Seconds) : Enter a value (in seconds). Resuming of monitoring for this object will be additionally delayed after the master object for this dependency is 'Up' again. This is helpful for



devices with sensors that need some time to resume after the restart of a device, while usually the dependency sensor (e.g. Ping) is already 'Up'. A delay can avoid false alarms.

## 9.4 Review or download historic data

1. Select the "Historic Data" in device dashboard.



The screenshot shows the device dashboard interface. At the top, there is a navigation bar with tabs: Overview, Live Data, 2 days, 30 days, Historic Data (highlighted with a red arrow), and Log. To the right of the tabs are buttons for Settings, Notifications, and Channels. Below the navigation bar, the status is shown as 'Last Message: OK'. A summary row displays: Last Scan: 27 s, Last Up: 27 s, Last Down: 5 d 3 h 31 m, Uptime: 99.9035%, Downtime: 0.0965%, and Co: 93. Below this, there are three panels: 'CPU usage' with a green gauge, 'Datstore total ReadL...' with a gauge showing 0 msec, and 'Datstore total WriteL...' with a gauge. A dropdown menu is open on the right, showing options: Channel, CPU usage, Datstore total ReadLatency, and Datstore total WriteLatency.

## 2. Review or download historic data setting option

Overview Live Data 2 days 30 days 365 days **Historic Data** Log Settings Notifications Channels

### REVIEW OR DOWNLOAD HISTORIC SENSOR DATA

Start **2015-08-01 00:00**

End **2015-09-01 00:00**

Quick Range

1 Day	2 Days	7 Days	14 Days
Today	Yesterday	Last Week (Mo-Su)	Last Week (Su-Sa)
Last Month	2 Months	6 Months	12 Months

Average Interval **30 Seconds**

Channels

<input checked="" type="checkbox"/> Downtime (%)	<input checked="" type="checkbox"/> CPU usage (%)	<input checked="" type="checkbox"/> Network recei... (kbit/s)
<input checked="" type="checkbox"/> Disk read (Mbit/s)	<input checked="" type="checkbox"/> Datastore total... (msec)	<input checked="" type="checkbox"/> Network usage (kbit/s)
<input checked="" type="checkbox"/> Datastore total... (msec)	<input checked="" type="checkbox"/> Memory active (MByte)	<input checked="" type="checkbox"/> Network trans... (kbit/s)
<input checked="" type="checkbox"/> Memory consume... (%)	<input checked="" type="checkbox"/> Memory cons... (MByte)	<input checked="" type="checkbox"/> Disk usage (Mbit/s)
<input checked="" type="checkbox"/> Disk write (Mbit/s)		

Show all Hide all

File Format

- HTML web page
- XML file
- CSV file

Percentile Results

- Do not show percentiles
- Show percentiles

**Start** Cancel

- Start : Enter your preferred start time.
- End : Enter your preferred end time.
- Quick Range : You can select the range by "quick range" and will auto fill in "Start" & "End".
- Average Interval : Select an interval for averaging. For time spans more than 40 days, the minimum interval is 60 minutes. If set below, it will be increased automatically. If you set a value less than the minimum Scanning Interval (This setting set in "4.1 Edit the Device setting"). Some data may be lost in the report.
- Channels : Select the resources you want to include.
- File Format : HTML web page for viewing only. And XML & CSV files for downloading only
- Percentile Results : 'On' displays a percentile calculation for each resource in an overview table with averages/sums for each resource.

3. If you select File Format to HTML web page, the system will take a time to generate the data

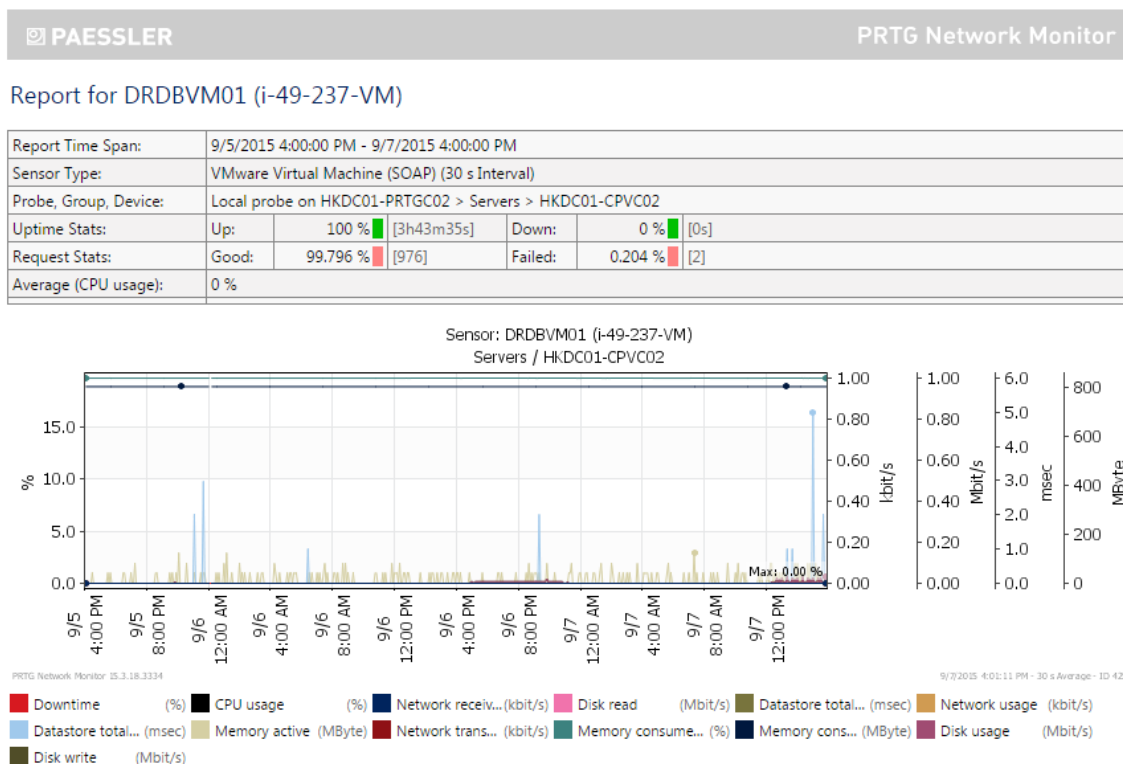
PRTG is now generating your historic data for:

**4256 DRDBVM01 (i-49-237-VM)**

The historic data will be shown here as soon as it's ready.



4. Sample for the HTML web page format report (Chart)



5. Sample for the HTML web page format report (Table)

Date Time	CPU usage	Network received	Disk read	Datastore total	ReadLatency	Network usage	Datastore total	WriteLatency	Memory active	Network transmitted	Memory consumed (Percent)	Memory consumed	Disk usage	Disk write
<b>Averages (of 120 values)</b>	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0.016666666666667 msec		11 MByte	0 kbit/s	19.65133333333334 %	805 MByte	< 0.01 Mbit/s	< 0.01 Mbit/s
9/7/2015 3:04:00 PM - 3:04:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0.02 Mbit/s	0.02 Mbit/s
9/7/2015 3:04:30 PM - 3:05:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		41 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:05:00 PM - 3:05:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		82 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:05:30 PM - 3:06:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		82 MByte	0 kbit/s	19.65 %	805 MByte	< 0.01 Mbit/s	< 0.01 Mbit/s
9/7/2015 3:06:00 PM - 3:06:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:06:30 PM - 3:07:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:07:00 PM - 3:07:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:07:30 PM - 3:08:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:08:00 PM - 3:08:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:08:30 PM - 3:09:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		82 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:09:00 PM - 3:09:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:09:30 PM - 3:10:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:10:00 PM - 3:10:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:10:30 PM - 3:11:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:11:00 PM - 3:11:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:11:30 PM - 3:12:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:12:00 PM - 3:12:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:12:30 PM - 3:13:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:13:00 PM - 3:13:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:13:30 PM - 3:14:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	0 Mbit/s	0 Mbit/s
9/7/2015 3:14:00 PM - 3:14:30 PM	0 %	0 kbit/s	0 Mbit/s	0 msec		0 kbit/s	0 msec		0 MByte	0 kbit/s	19.65 %	805 MByte	< 0.01 Mbit/s	< 0.01 Mbit/s

## 9.5 Add report (Support html format only)

### 9.5.1 Create the report

1. Select "Reports" > "Add report" in toolbar

The screenshot shows the Cloud Portal navigation bar with tabs for Home, Devices, Sensors, Alarms, Reports, Logs, and Setup. The 'Reports' tab is selected, and a dropdown menu is open, showing 'All' and 'Add Report'. A red arrow points to the 'Add Report' option. Below the navigation bar, the 'Group Root' section is visible, showing a tree view with 'Local probe on HKDC01-PRTGC02' and 'Servers'. The 'Servers' section lists several servers with their status (OK) and sensor health (0% green).

2. Add report setting option. please fill & select your option

#### BASIC REPORT SETTINGS

Report Name	<input type="text" value="Report"/>
Tags	<input type="text"/>
Template	<input type="text" value="&lt;please select a file&gt;"/> <span style="color: red;">This field is required.</span>
Security Context	<input type="text" value="2fa_hkbn"/>
Timezone	<input type="text" value="(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi"/>
Paper Size	<input type="radio"/> A4 <input type="radio"/> Legal <input checked="" type="radio"/> Letter

- Report Name : Enter a report name.
- Tags : Enter a list of tags (not case sensitive) for filtering purposes.
- Template : Choose a report template from the list of available templates. There are templates that offer optional data tables besides the graphs. You can also specify the graph/calculation intervals by selecting a template.
- Timezone : Timezone setting for all dates regarding this report. This includes schedule dates, report time span, and dates in tables/graphs.
- Paper Size : Specify the paper size for which the report will be formatted. Choose between the DIN A4, the US legal paper and the US letter paper format.

## SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

Add Sensors by Tag

Filter Sensors by Tag

- Add Sensors by Tag : Add "exxservvmsensor" if you want all device include in report. For the setup specify device, don't select any tag and will show you in step 6.1.1.
- Filter Sensors by Tag : **No need to set**

## SCHEDULE ("WHEN WILL THIS REPORT BE RUN?")

Report Schedule

- Every specific day of a week
- Every specific day of a month
- The day after a quarter is finished (i.e. at 1. April for the 1. January - 31. March Quarter)
- Every specific date

- Report Schedule : **Don't select any option**

## PERIOD ("WHAT TIME SPAN WILL THE REPORT COVER?")

Reported Period

- Current
- Previous

Report Period Type

- Day
- Week
- Month
- Quarter (January-March, April-June, etc.)
- Year

Week Period

Monday-Sunday

Report Only for Specific Hours-of-Day (Schedule)

None

- Reported Period : Specify which period is to be reported. Please choose between daily, weekly, monthly, quarterly or yearly reports. Examples: Current is 'today' for daily reports, 'current month' for monthly reports. Previous means 'yesterday' for daily reports, 'last month' for monthly reports.
- Report Period Type : Specify which period is to be reported. Please choose between daily, weekly, monthly, quarterly or yearly reports. Examples: Current is 'today' for daily reports, 'current month' for monthly reports. Previous means 'yesterday' for daily reports, 'last month' for monthly reports.
- Week Period : Define when the week will start and end.
- Report Only for Specific Hours-of-Day (Schedule) : **None (no need to set)**

## INCLUDE PERCENTILES

Percentile Results

- Do not show percentiles
- Show percentiles

- Percentile Results : 'Show percentiles' displays a percentile calculation for each resource in an overview table with averages/sums for each resource.

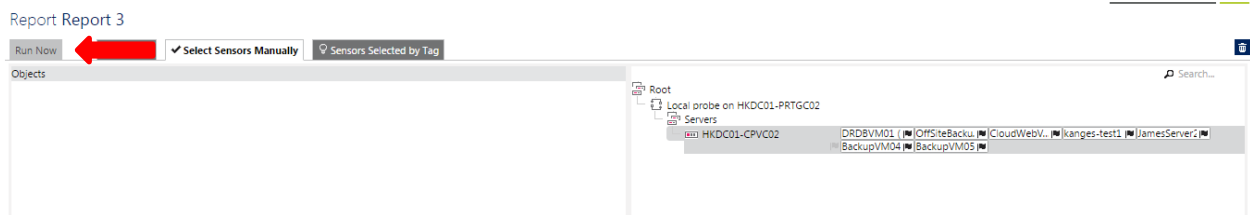
## REPORT COMMENTS

Introduction

Footer Comments

- Introduction : This introductory text will be shown on the report's first page.
- Footer Comments : These comments will be shown at the end of a report.

3. Complete the above setting, click the **Continue** button
4. The **Select Sensors Manually** page is shown. This page is manual setup and device data is included in the report. If you don't want to set it, select the **Run Now** tag and click the **Run Report** button. If you want to set it, go to [“6.1.1 select sensors manually”](#)



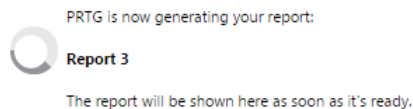
## PROCESSING OPTIONS

File Format and Delivery

View Report as HTML

Run Report

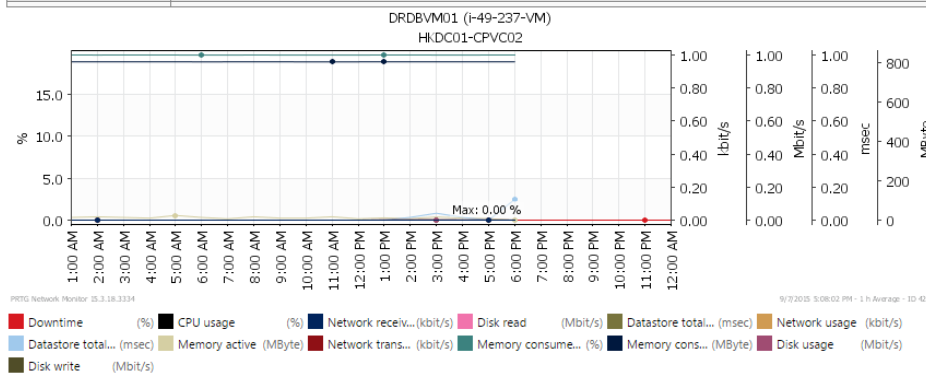
5. The system will take a time to generate the report



## 6. Sample for the report (HTML format)

### Report 3: DRDBVM01 (i-49-237-VM)

Report Time Span:	9/7/2015 12:00:00 AM - 9/8/2015 12:00:00 AM			
Report Hours:	24 / 7			
Sensor Type:	VMware Virtual Machine (SOAP) (30 s Interval)			
Probe, Group, Device:	Local probe on HKDC01-PRTGC02 > Servers > HKDC01-CPVC02			
Uptime Stats:	Up:	100 % [4h51m1s]	Down:	0 % [0s]
Request Stats:	Good:	100 % [729]	Failed:	0 % [0]
Average (CPU usage):	0 %			



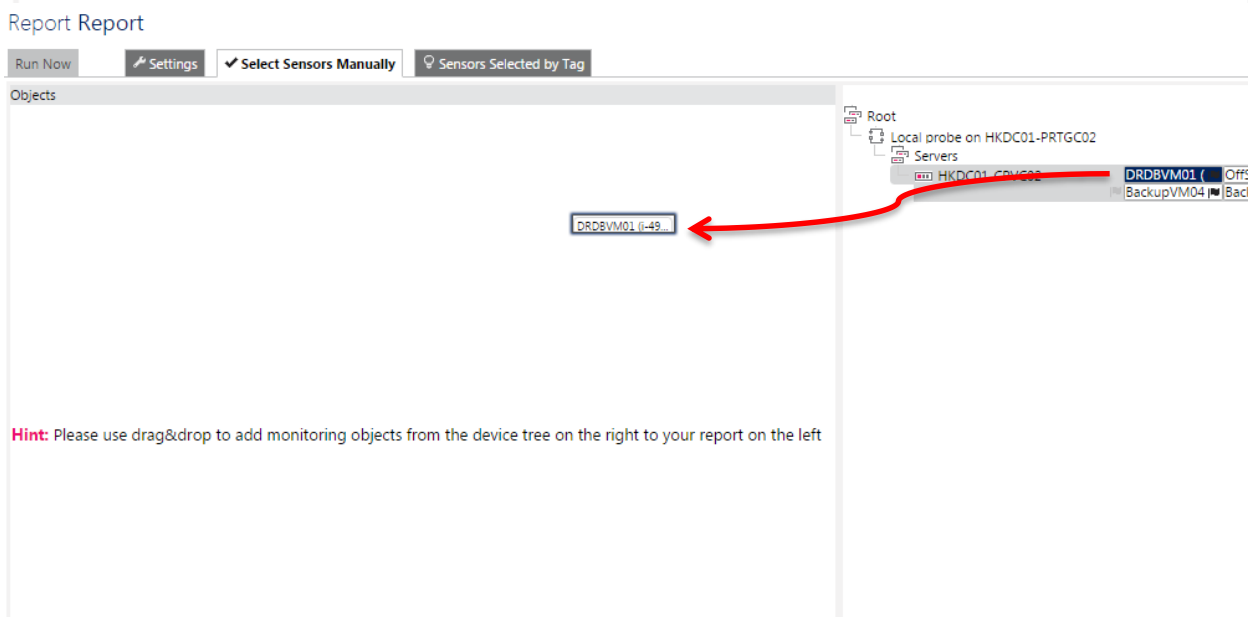
Channel	Average
CPU usage	0 %
Network received	0 kbit/s
Disk read	0 Mbit/s
Datstore total ReadLatency	0 msec
Network usage	0 kbit/s
Datstore total WriteLatency	0.0150891632373114 msec
Memory active	11 MByte
Network transmitted	0 kbit/s
Memory consumed (Percent)	19.6563648834019 %
Memory consumed	805 MByte
Disk usage	< 0.01 Mbit/s
Disk write	< 0.01 Mbit/s

Date Time	CPU usage	Network received	Disk read	Datstore total ReadLatency	Network usage	Datstore total WriteLatency	Memory active	Network transmitted	Memory consumed (Percent)	Memory consumed
<b>Averages (of 18 values)</b>	0 %	0 kbit/s	0 Mbit/s	0 msec	0 kbit/s	0.0150891632373114 msec	11 MByte	0 kbit/s	19.6563648834019 %	805 MByte
9/7/2015 11:00:00 PM - 12:00:00 AM										
9/7/2015 10:00:00 PM - 11:00:00 PM										
9/7/2015 9:00:00 PM - 10:00:00 PM										
9/7/2015 8:00:00 PM - 9:00:00 PM										
9/7/2015 7:00:00 PM - 8:00:00 PM										
9/7/2015 6:00:00 PM - 7:00:00 PM										
9/7/2015 5:00:00 PM - 6:00:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec	0 kbit/s	0.125 msec	0 MByte	0 kbit/s	19.66 %	805 MByte
9/7/2015 4:00:00 PM - 5:00:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec	0 kbit/s	0 msec	8 MByte	0 kbit/s	19.658 %	805 MByte
9/7/2015 3:00:00 PM - 4:00:00 PM	0 %	0 kbit/s	0 Mbit/s	0 msec	0 kbit/s	0.0166666666666667 msec	11 MByte	0 kbit/s	19.65133333333334 %	805 MByte

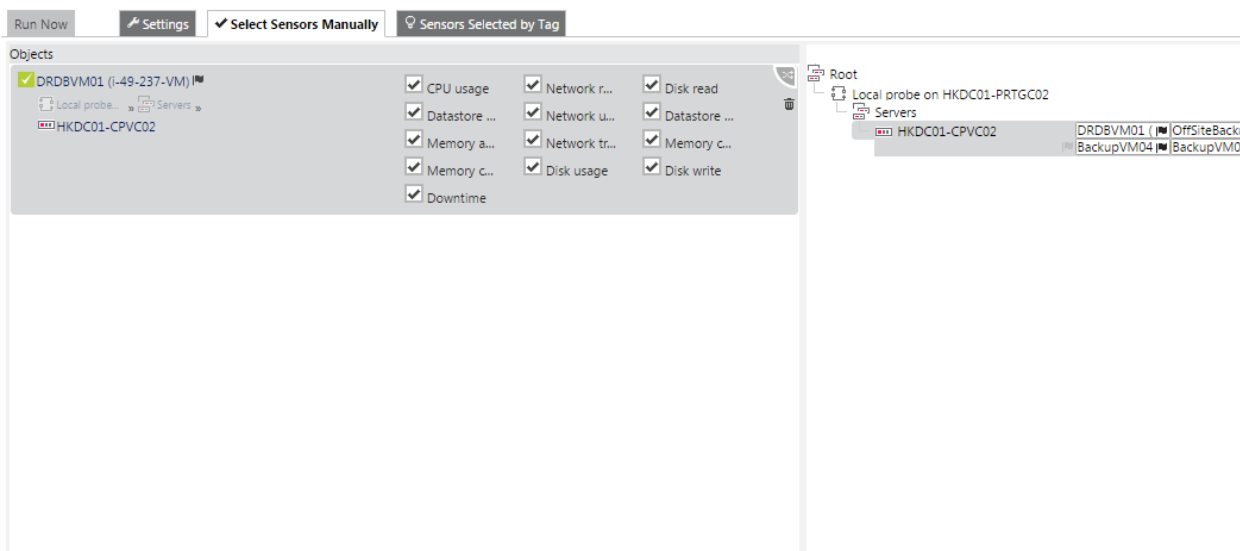
### 9.5.2 Select Sensors Manually

1. If you want to specify the device, you can select the device and drag & drop to the **Objects** tag. (Hints are shown in the system)

**Hint:** Please use drag&drop to add monitoring objects from the device tree on the right to your report on the left



2. After the device is added, you can select the checkboxes to include the related resource information in the report.

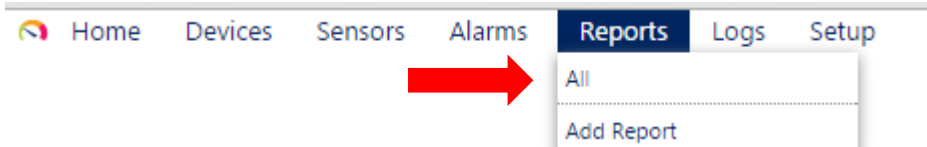




## 9.6 Manage your saved report

### 9.6.1 View and run your saved report

1. When the report is generated, system will save your report setting. You can find the saved report in toolbar “report” > “All”



2. You can find what report created.

Reports

Show reports tagged with

1 to 3 of 3

Object	Template	Security Context	Period	Schedule	Email	Status	Next Run	Last Run	Number of Sensors in last Run	Links
Report	Graph 1h interval, Table 24h interval	2fa_hkbn	Week	None		Idle	-	-	0	Edit Clone Delete
Report	Graph 30 min interval, Table 30 min interval	2fa_hkbn	Week	None		Idle	-	-	0	Edit Clone Delete
Report 3	Graph 1h interval, Table 1h interval	2fa_hkbn	Week	Yearly	cloud.monitoring@hds.com	Idle	1/1/2016 12:00:00 AM	-	0	Edit Clone Delete

[Add Report](#)

3. If you want to view the report again, click the report name.

Reports

Show reports tagged with

1 to 3 of 3

Object	Template
Report	Graph 1h interval, Table 24h interval
Report	Graph 30 min interval, Table 30 min interval
Report 3	Graph 1h interval, Table 1h interval

4. Click the **Run Report** button

Report Report

[Run Now](#) [Settings](#)  Select Sensors Manually  Sensors Selected by Tag

RUN REPORT "REPORT"

Report for

- Current Period: This week (9/7/2015 - 9/14/2015)
- Previous Period: Last week (8/31/2015 - 9/7/2015)
- Select A Period
- Select Date Range Manually

Start Date: 2015-09-08

End Date: 2015-09-09

Quick Range

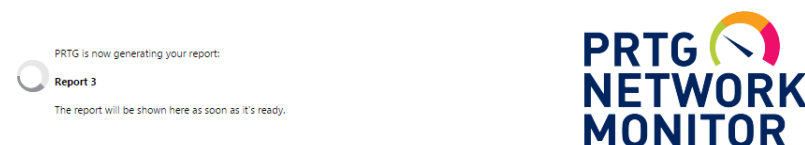
Today	Yesterday	Last Week (Mo-Su)	Last Week (Su-Sa)
Last Month	2 Months	6 Months	12 Months

PROCESSING OPTIONS

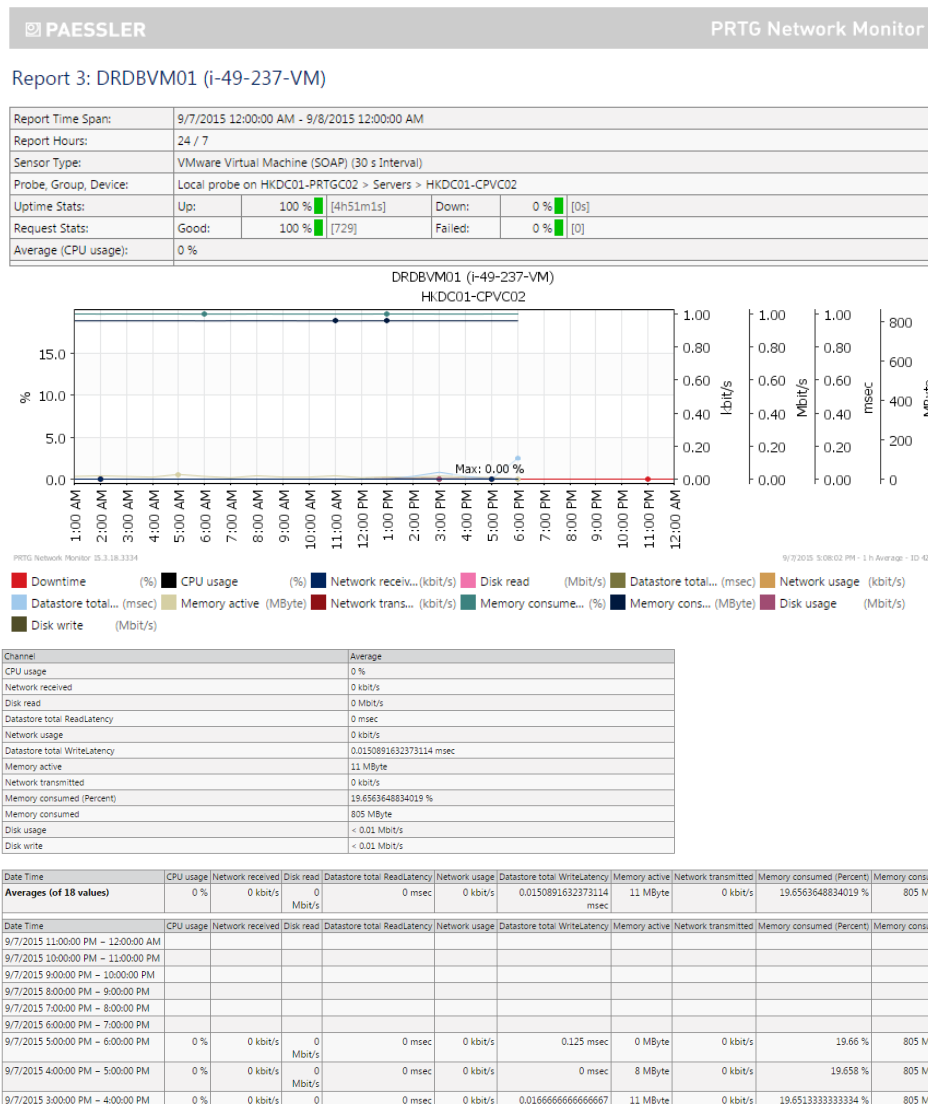
File Format and Delivery  View Report as HTML

[Run Report](#)

5. The system will take time to generate the report

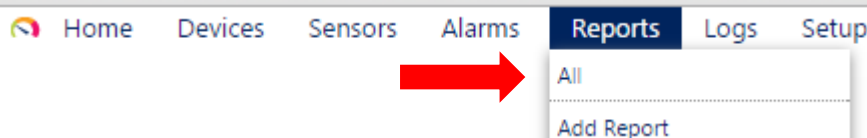


## 6. Sample for the report (HTML format)



### 9.6.2 Delete your report

- Go to report baseboard, click "Reports" > "All" in toolbar.



- You can find all the reports generated.

Reports

Show reports tagged with

← 1 to 3 of 3 →

Object	Template	Security Context	Period	Schedule	Email	Status	Next Run	Last Run	Number of Sensors in last Run	Links
Report	Graph 1h interval, Table 24h interval	2fa_hkbn	Week	None		Idle	-	-	0	<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a>
Report	Graph 30 min interval, Table 30 min interval	2fa_hkbn	Week	None		Idle	-	-	0	<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a>
Report 3	Graph 1h interval, Table 1h interval	2fa_hkbn	Week	Yearly	cloud.monitoring@hds.com	Idle	1/1/2016 12:00:00 AM	-	0	<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a>

← 1 to 3 of 3 →

[Add Report](#)

3. Click the **Delete** button

	Last Run	Number of Sensors in last Run	Links
	-	0	Edit  Delete
	-	0	Edit  Clone  Delete
AM	-	0	Edit  Clone  Delete

4. Note the warning message & click the **Delete Object** button.

Delete Object Report

DELETE AN OBJECT

You have decided to delete an object from the database. On this page PRTG will always show you all other object(s) from the database that may be connected to the object that you want to delete. You should review this list to make sure no other monitoring objects are unintentionally affected.

PLEASE APPROVE

Are you sure you want to delete the object Report ?

No, I do not want to delete this object

### 9.6.3 Edit your report

1. Go to report baseboard, click “Reports” > “All” in toolbar.

Home
 Devices
 Sensors
 Alarms
Reports
 Logs
 Setup

All


---

Add Report

2. You can find all the reports generated.

Reports

Show reports tagged with

← 1 to 3 of 3 →

Object	Template	Security Context	Period	Schedule	Email	Status	Next Run	Last Run	Number of Sensors in last Run	Links
Report	Graph 1h interval, Table 24h interval		Week	None		Idle	-	-	0	Edit  Clone  Delete
Report	Graph 30 min interval, Table 30 min interval		Week	None		Idle	-	-	0	Edit  Clone  Delete
Report 3	Graph 1h interval, Table 1h interval		Week	Yearly	cloud.monitoring@hds.com	Idle	1/1/2016 12:00:00 AM	-	0	Edit  Clone  Delete

← 1 to 3 of 3 →

Add Report

3. Click the **Edit** button

	Last Run	Number of Sensors in last Run	Links
	-	0	Edit  Clone  Delete
	-	0	Edit  Clone  Delete
AM	-	0	Edit  Clone  Delete

4. The report setting is shown and you can refer the setup in “9.5.1 Create the report”

## Report Report

Run Now Settings Select Sensors Manually Sensors Selected by Tag

### BASIC REPORT SETTINGS

Report Name: Report

Tags:

Template: Graph 30 min interval, Table 30 min interval

Security Context: 2fa\_hkbn

Timezone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Paper Size:
 

- A4
- Legal
- Letter

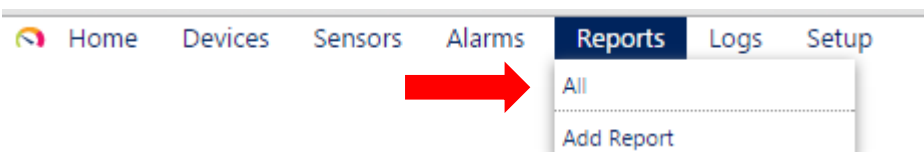
### SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

Add Sensors by Tag:

Filter Sensors by Tag:

### 9.6.4 Clone your report

1. Go to report baseboard, click "Reports" > "All" in toolbar.



2. You can find all the reports generated.

Reports

Show reports tagged with:

Object	Template	Security Context	Period	Schedule	Email	Status	Next Run	Last Run	Number of Sensors in last Run	Links
Report	Graph 1h interval, Table 24h interval	2fa_hkbn	Week	None		Idle	-	-	0	Edit Clone Delete
Report	Graph 30 min interval, Table 30 min interval	2fa_hkbn	Week	None		Idle	-	-	0	Edit Clone Delete
Report 3	Graph 1h interval, Table 1h interval	2fa_hkbn	Week	Yearly	cloud.monitoring@hds.com	Idle	1/1/2016 12:00:00 AM	-	0	Edit Clone Delete







Add Report

3. Click the Clone button

	Last Run	Number of Sensors in last Run	Links
	-	0	Edit Clone Delete
	-	0	Edit Clone Delete
AM	-	0	Edit Clone Delete

- The report has been cloned and named as “Clone of (source report name)”. You can edit the report by clicking the **Edit** button.

## Reports

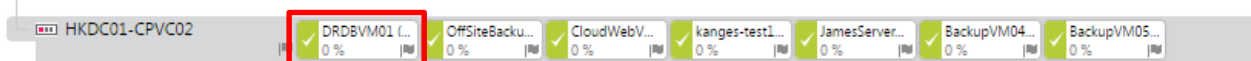
Show reports tagged with <input type="text"/>		
< ← 1 to 3 of 3 → >		
Object ▾	Template	Security
 Clone of Report	Graph 30 min interval, Table 30 min interval	 2fa
 Report	Graph 30 min interval, Table 30 min interval	 2fa
 Report 3	Graph 1h interval, Table 1h interval	 2fa
< ← 1 to 3 of 3 → >		

## 9.7 VM resource warning /error status & email notification

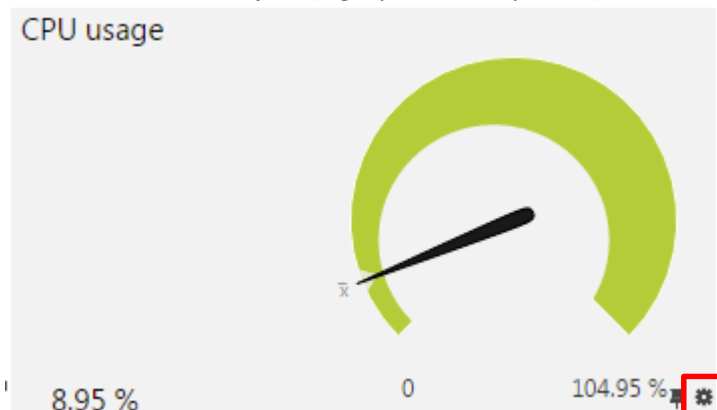
### 9.7.1 Setup the warning /error status

You can set the resource usage alert level (For example, when CPU usage is over 70%, you can define it as warning status). You can coordinate the email notification (please go to “9.8”) to alert your VM resource utilization.

- Click device you want to setup.



- Select the object (e.g. cpu, memory, disk.) and click the **Edit channel setting** button.

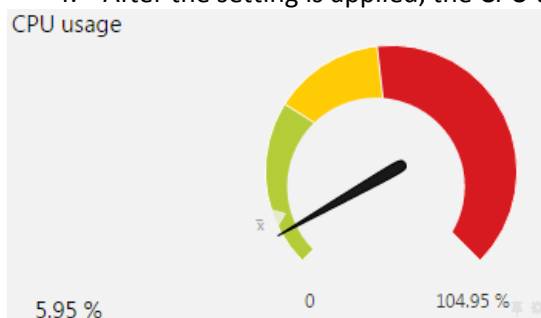


### 3. Select **Enable limits**.

Edit Channel	
Name	CPU usage
ID	2
Chart Rendering	<input checked="" type="radio"/> Show in Charts <input type="radio"/> Hide from Charts
Table Rendering	<input checked="" type="radio"/> Show in Tables <input type="radio"/> Hide from Tables
Line Color	<input checked="" type="radio"/> Automatic <input type="radio"/> Manual
Line Width	1
Data	<input checked="" type="radio"/> Display actual values in % <input type="radio"/> Display in percent of maximum
Value Mode	<input checked="" type="radio"/> Average <input type="radio"/> Minimum <input type="radio"/> Maximum
Decimal Places	<input type="radio"/> Automatic <input checked="" type="radio"/> All <input type="radio"/> Custom
Spike Filter	<input checked="" type="radio"/> Disable Filtering <input type="radio"/> Enable Filtering
Vertical Axis Scaling	<input checked="" type="radio"/> Automatic Scaling <input type="radio"/> Manual Scaling
Limits	<input type="radio"/> Disable Limits <input checked="" type="radio"/> <b>Enable Limits</b>
Upper Error Limit (%)	
Upper Warning Limit (%)	
Lower Warning Limit (%)	
Lower Error Limit (%)	
Error Limit Message	
Warning Limit Message	

- Upper Error Limit (%) : Values above this value will set the sensor state to 'Down'.
- Upper Warning Limit (%) : Values above this value will set the sensor state to 'Warning'.
- Lower Warning Limit (%) : Values below this value will set the sensor state to 'Warning'.
- Lower Error Limit (%) : Values below this value will set the sensor state to 'Down'.
- Error Limit Message : This message is added to the error status.
- Warning Limit Message : This message is added to the warning status.

### 4. After the setting is applied, the CPU usage status is updated. (Yellow for warning, Red for Error)



### 9.7.2 Setup email notification

1. Go to the below URL to set up email address  
<https://monitoring.hds-cloudconnect.com/myaccount.htm?tabid=2>

#### Account Settings

My Account | **Notifications** | Notification Contacts | Schedules

#### NOTIFICATIONS

Show notifications tagged with

← 1 to 1 of 1 →

Object	Active/Paused	Links
Email to all members of group 2FA TGGGo (Trial)	Active	<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a> <a href="#">Test</a> <a href="#">Pause</a>

← 1 to 1 of 1 →

[Add new notification](#)

2. Input your email address in the **Notification Name** field and click the **SEND EMAIL** button

#### BASIC NOTIFICATION SETTINGS

<b>Notification Name</b>	<b>Notification</b>
Tags	
Status	<input checked="" type="radio"/> Started <input type="radio"/> Paused
Schedule	None
Postpone	<input type="radio"/> Discard notifications during paused status <input checked="" type="radio"/> Collect notifications and send them when reactivated

#### NOTIFICATION SUMMARIZATION

Method	<input type="radio"/> Always notify ASAP <input type="radio"/> Send first DOWN message ASAP, summarize others <input checked="" type="radio"/> Send first DOWN and UP message ASAP, summarize others <input type="radio"/> Send all DOWN messages ASAP, summarize others <input type="radio"/> Send all DOWN and UP messages ASAP, summarize others <input type="radio"/> Always summarize notifications
Subject for Summarized Messages	[%sitename] %summarycount Summarized Notifications
Gather Notification For (Minutes)	1

**SEND EMAIL**

3. Input your email address to highlighted field

SEND EMAIL

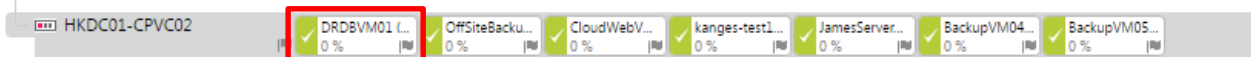
The three recipient settings below (user, user group, email address) work independently. So every contact/address selected by any of these settings will receive the notification

Send to User None ▼

Send to User Group None ▼

Send to Email Address

4. Go to device dashboard and select device you want to set up.



5. Click the **Notifications** tag



Sensor pocvm01-shing (i-23-907-TGGO) ★★★★★

Overview | Live Data | 2 days | 30 days | 365 days | Historic Data | Log | Settings | Notifications | Channels

Last Message: **OK**

Last Scan: 4 m 55 s	Last Up: 4 m 55 s	Last Down:	Uptime: 100.0000%	Downtime: 0.0000%
---------------------	-------------------	------------	-------------------	-------------------

CPU usage

CPU ready (Percent)  
0.06 %

Channel ▼

- CPU ready (Percent)
- CPU usage
- Datastore total ReadLatency
- Datastore total WriteLatency
- Disk read



6. Click the **Add State Trigger** button

TRIGGERS THAT CAN BE INHERITED FROM PARENT OBJECT(S)

Type	Notifications	Inherited from
State Trigger	When sensor state is <b>Down</b> for at least <b>1000</b> seconds perform <b>Email and push notification to admin</b> When sensor state is <b>Down</b> for at least <b>300</b> seconds perform <b>no notification</b> and repeat every <b>0</b> minutes When condition clears after a notification was triggered perform <b>no notification</b>	HKDC03CVC001PRD

Trigger Inheritance

- Inherit all triggers from parent objects and use the triggers defined below
- Only use the triggers defined below

TRIGGERS THAT ARE DEFINED IN LIBRARY OBJECT(S)

Type	Notifications	Inherited from
(no triggers defined)		

OBJECT TRIGGERS

Type	Notifications	Actions
(no triggers defined)		

7. Change the settings & email address.

OBJECT TRIGGERS

Type	Notifications	Actions
State Trigger	When sensor state is <b>Warning</b> for at least <b>60</b> seconds perform <b>alert@hkbn.com</b> When sensor state is <b>Warning</b> for at least <b>300</b> seconds perform <b>alert@hkbn.com</b> and repeat every <b>0</b> minutes When condition clears after a notification was triggered perform <b>alert@hkbn.com</b>	<input checked="" type="button" value="Save"/> <input type="button" value="Cancel"/>