iPECS vUCP
(Virtual Unified Communications Platform)

Installation Manual

Please read this manual carefully before operating System.
Retain it for future reference.

iPECS is an Ericsson-LG Brand

Revision History

ISSUE	DATE	DESCRIPTION OF CHANGES
1.0	Jan., 2018	S/W version 3.0.x. - Initial Release
1.1	Mar., 2018	S/W version 3.1.x. - Change the vUCP Default login value HTTPS and port number from 437 to 443
1.2	Apr., 2019	S/W version 3.5.x. - vMCIM is added and AWS platform is supported. - System Default License is changed to vUCP-CS2400S (SWL)
1.3	Dec.03, 2019	S/W version 4.0.x. - General Update (Style, Chart, Fonts)
	Dec.18, 2019	- Added the vVOIMT.
1.4	Sep., 2020	S/W version 4.1.x. - Applied S/W version 4.1.x
1.5	Mar., 2021	S/W version 5.0.x. - Applied S/W version 5.0.x

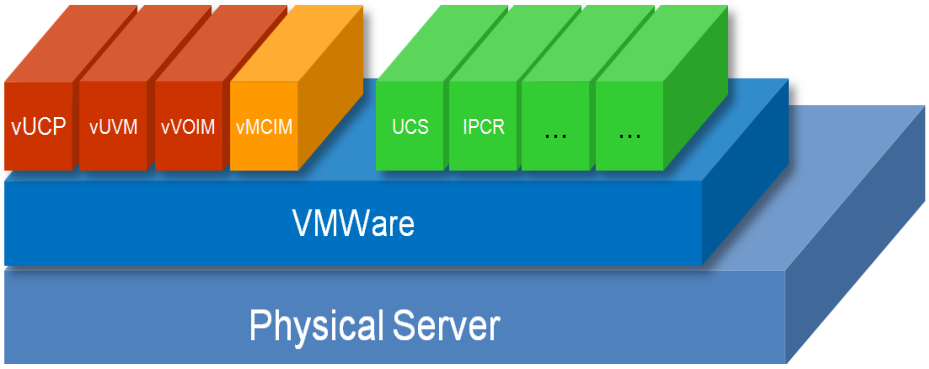
Table of Contents

1 Introduction

1.1 Overview of virtual UCP (vUCP)

The iPECS UCP is an award winning all-in-one IP-PBX and UC solution designed for SMB and mid-size enterprises providing great flexibility, scalability and reliability in delivering unified communications services and advanced communication features over dispersed and mobile environments.

The Virtual UCP (vUCP) is a software version of UCP, which can be run on virtual machine (VMware®). While supporting all the compelling advantage ofiPECS UCP, the vUCP allows more simple and flexible deployment and management with low total cost of ownership. Targeting at the midsize enterprise, vUCP supports from 200 ports at an affordable price to SMB businesses and can grow up to 2,400 ports with system port license.The vUCP can be installed on customers' existing virtual infrastructure or can be built ina new virtual server, together with other product and business applications like UCS premium, IPCR, Report Plus, etc.



1.2 Manual Application

This document provides detailed information covering the configuration of the vUCP.

The manual is written for the experienced installer who has knowledge of telephony terms and functions about the small and mid-sized business telecommunications systems.

1.3 Manual Organization

This manual is organized in four (4) major sections including:

- **Section 1 Introduction**: This section introduces the content and organization of the manual.
- **Section 2 Supported virtualized System**: This section introduces the supported virtualized system and requirements. Also, it explains about the specification of vUCP and explains the differences with embedded UCP systems.
- **Section 3 Virtual Machine Deployment**: This section introduces the deployment of virtual machine. It explains how to deploy the vUCP, vUVM, vMCIM and vVOIM/vVOIMT.
- **Section 4System Upgrade**: This section introduces how to upgrade the systems.

2 Supported virtualized System

2.1 Specification

The Virtual UCP system is virtualized into function base software operation as follows

- Virtual UCP(vUCP)– Voice and Standard UC features
- Virtual UVM(vUVM)– Voice mail
- Virtual VOIM(vVOIM)– G/711 base VOIP functions
- Virtual MCIM(vMCIM)– Voice Conference supported from Unified 3.5
- Virtual VOIMT(vVOIMT)– VOIP functions and transcoding functions from Unified 4.0

System Capacity of vUCP, vUVM, vMCIM and vVOIM/vVOIMT

The capacities associated with each software are given in the below table.

Table 2.1-1Virtual UCP System Capacities

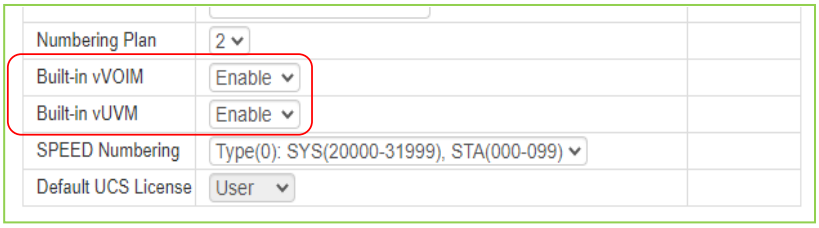
ITEM	Capacity	Remark
System Port • Default • Maximum	 50 2400	 vUCP-CS2400S(SWL) license vUCP-SPL licenses
Stations	2400	Total stations and Lines cannot exceed the available System port.
CO/IP Lines (external network channels incl. VoIP)	998	
UCS Standard Clients UCS Premium Clients	400 2400	
Server Redundancy	Yes	Geographical redundancy only
WTIM4/8 modules WTIM24	30 10	Max 3 WTIMs in a single sync. zone WTIM24 can't' be in same sync. zone w/ WTIM4/8
DECT phones	192 254	Mixed with WTIM4/8 Only WTIM24
VoIP Channels • System Maximum • Virtual VOIP • H/WVOIP	 998 998(Default: 6 vVOIM channels) 998	 Need Virtual VOIP license or H/W VOIP - Soft VOIP: G.711 only, no transcoding - DSP VOIP: G.711/729/722, transcoding
Per vVOIM (virtual VOIP) • Default channel • Maximum (Internal) • Maximum	 0 128 Channels 250 Channels	 w/License (8ch base increment)
vVOIM per system	4	
Per vVOIMT (virtual VOIP& Transcoding) • Default channel • Maximum	 32 32 Channels	 32 channel licenses
vVOIMT per system	31	Maximum 998 channels

ITEM	Capacity	Remark
Per vMCIM (virtual conference) • Default channel • Maximum	 64 64 Channels	 64 channel licenses
vMCIM per system	15	Maximum 998 channels
Per vUVM (virtual UVM) • Default (per system) • Maximum (Internal) • Maximum (per vUVM) • Maximum (per system)	 8 Channels 64 Channels 150 Channels 300 Channels	 w/License (8ch base increment)
VM Message Number • System Maximum • Per VM board	 64000 32000	
vUVM per system	2	
USB Host port	0	Not supported
Internal Page Zones	100	
System Speed Dial	12,000	
System Speed Dial Zones	50 Groups	
Station Speed Dial, per Station	100	
Total Station Speed Dial	24,000	
Call park	200	
Last Number Redial	10 (23 digits)	
Save Number Redial	1 (23 digits)	
Standard DSS Consoles/Station	9	
Serial DSS - System	500	
Serial DSS - Station (LIP-8000)	4	
Serial DSS - Station (LIP-9000)	4	
SMDR buffer	30,000	
CO Line Groups	200	
Station &Station Groups	200	
Station &Station Group Members	200	
Pickup Groups	200	
Pickup Group Member	2,4000	
Personal Groups	1200	
Conference Group - System	160	MCIM or VCIM are required
Conference Group - Station	100	MCIM or VCIM are required
Executive/Secretary pairs	100	
Authorization Codes	5200	Station:2400, System:2800
Transparent Networking Table	100	
CLI Msg Wait (Missed calls)	4,000	
Local Redundancy	No	
Geographical Redundancy	Yes	
Flex DID Table	10,000	

ITEM	Capacity	Remark
MSN table	2,400	
DID Digits Analysis	4	
Tenancy (ICM) Groups	100	
ICLID table	500	

Built-in vVOIM and vUVM

The features are supported from Unified 5.0. But you remember that they are allowed only when a new vUCP is installed by 5.0 or later image and not allowed when an upgrade from old version is done. If you used them, vUCP, vVOIM, and vUVM can be run in single virtual machine. But the maximum port of vUCP is changed to that of UCP600. You can configure them in PGM 100.



vUCP site which is already installed

To use built-in vVOIM/vUVM

1) Download DB
2) Remove the current vUCP
3) Install vUCP using vUCP 5.0 image (or later)
4) Set system IP
5) License transition with new serial number
6) Upload DB
7) Delete external vUVM/vVOIM if it is not used
8) Enable built-in vUVM/vVOIM in PGM100 if it is used

To use vUCP without change

1) Just upgrade vUCP from 4.1 or below to 5.0
2) Built-in vVOIM/vUVM cannot be enabled in PGM100.

2.2 Virtual Server Support

2.2.1 Supported Virtual Server

VMware vSphere

The VMware vSphere ESXi 6.0 or later version supports the vUCP virtual machines.

AWS(Amazon Web Services)

The AWS is supported from Unified version 3.5.

3 VMware Virtual Machines

3.1 Supported Virtual Server Features

vCenter

vMotion

The vMotion supports the virtual machine migration.

Snapshot

The Snapshot can be used only when the VM is powered off. It can provide easy fall back to stored points. But it is recommended that the unused snapshot is deleted due to the virtual machine performance.

OVF Deployment

Soft Power Off

3.2 Supported Hardware and Virtual Machine Platforms

For proper hardware platforms and hardware requirements for VMware ESXi, refer to
http://www.vmware.com/resources/compatibility/search.php

Current supported VMware software can be found in
https://www.vmware.com/products.html

If you want to find the most up-to-date technical documentation, refer to
http://www.vmware.com/support.html

3.3 Minimum Hardware and Software Requirements

The vUCP software is released in OVF format. Therefore, following specifications must be met.

- VMware vSphere 6.x software
- VMware vSphere client software (web client recommended)
- vCenter (supported but not required)
- CPU: Intel Xeon family with 2.0GHz clock speed or better (2.4GHz recommended)
- Memory: 12G Bytes or higher is recommended. It must satisfy the ESXi requirements in addition to the specific RAM requirements of each deployed virtual machines.
- Network: 1 Ethernet interface
- HDD: 100G Bytes or higher is recommended.

3.4 Profile of Virtual Machine

The OVF of vUCP, vUVM, vMCIM and vVOIM/vVOIMT installs the following default virtual machine.

vUCP

Lower SW version 5.0.x

- CPU: 1 vCore
- Memory: 4G Bytes
- HDD: 24G Bytes (Application) + 1G Bytes (DB data)
- Network: 1 Gigabit

Higher SW version 5.0.x: Internal vUVM, vVOIM is Included.

- CPU: 1 vCore
- Memory: 1G Bytes
- HDD: 8G Bytes (Application) + 1G Bytes (DB data) + 1G Bytes (Voice data, can be changed)
- Network: 1 Gigabit

vUVM

- CPU: 1 vCore
- Memory: 4G Bytes
- HDD: 24G Bytes (Application) + 16G Bytes (Voice data)
- Network: 1 Gigabit

vVOIM

- CPU: 1 vCore
- Memory: 4G Bytes
- HDD: 24G Bytes (Application)
- Network: 1 Gigabit

vMCIM/vVOIMT

- CPU: 1 vCore
- Memory: 1G Bytes
- HDD: 8G Bytes (Application)
- Network: 1 Gigabit

3.5 Restrictions

Multiple virtual servers and disk storage requirements (IOPS/30 per server)

For acceptable performance, the number of virtual machines which run on an ESXi host should not exceed the IOPS (Input/Output Operation per Second) of the disk storage divided by 30.

Refer to the below URL for more information

https://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=1031773&sliceId=2&docTypeID=DT_KB_1_1&dialogID=425694459&stateId=0%200%20486902509

3.6 Disk Type Selection of Virtual Machine

You can select the virtual hard disk type during the virtual machine deployment and you can choose it according to your purpose.

Refer the ‘vSphere Storage Guide’ of ‘ESXi and vCenter Server Product Documentation’at the below URL

https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html

3.6.1 Thick Provision Eager Zeroed

Space required for the virtual disk is allocated at creation time. The data remaining on the physical device is zeroed out during creation. It might take much longer to create disks in this format than to create other types of disks.

3.6.2 Thick Provision Lazy Zeroed

Space required for the virtual disk is allocated during the creation of the disk file. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. The virtual machine does not read stale data from disk.

3.6.3 Thin Provision

Space required for the virtual disk is allocated during creation. This formatting type does not zero out any old data that might be present on this allocated space. A non-root user cannot create disks of this format.

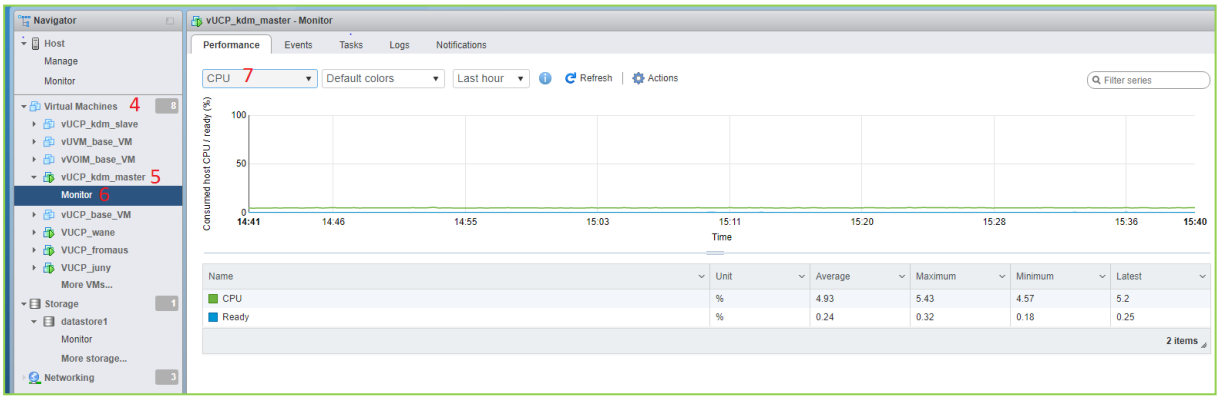
3.6.4 Determining disk type

If you are concerned about disk space, use the thin disks. If you are concerned about security and you want slightly better performance on initial disk writes, use eager zeroed thick disks. If you want easier administration, use the default disk type (lazy zeroed thick disks). Note that once an initial write to a new disk block has been completed, disk performance is equal across all disk types.

3.7 Performance View of Virtual Machines

You can see the performance page in vSphere by following process. If vCenter is used, you can see them on long term basis.

3) Connect to the IP address of ESXi by web browser
4) Click ‘Open the VMware Host Client’.
5) Log in by input ‘Username’ and ‘Password’.
6) Click ‘Virtual Machines in Navigator’
7) Click ‘My VM’.
8) Click ‘Monitor of My VM’
9) You can see the performance of CPU, Memory, Disk, and Network



Refer to ‘vSphere Monitoring and Performance Guide’ of ‘ESXi and vCenter Server Product Documentation’ in the below URL

https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html

3.8 Virtual Machine Deployment

Virtual Machine Deployment Process is as below.

1) Confirm the System Settings
2) Download the software
3) Deploy the OVF file
4) Power on Virtual Machine
5) Connect to Virtual Machine
6) Configure Network Settings and Restart
7) Access to Web and Complete Install Wizard
8) Create Serial Number
9) Order and Generate (download) licenses from the license portal
10) Upload the license file

In case of vUVM, vMCIM and vVOIM/vVOIMT, there is some differences from vUCP;

1) No serial number is supported.
2) No install wizard is supported.
3) No license file is supported.

Therefore,the procedure from 8 to last is not required.

3.8.1 Confirm the System Settings

You must finalize the following values before deploying the virtual machine and obtaining any licenses. If you change some factors after obtaining any licenses, those licenses are invalidated.

- System IP Address
- Router IP Address
- Firewall IP Address

3.8.1.1 Downloading the software

You can download OVF and ROM files from GPS website Library menu.

https://partner.ericssonlg-enterprise.com

3.8.1.2 OVF File

The OVF file is used for the virtual machine deployment.

3.8.1.3 ROM File

The Rom file is used for the application upgrade at the web admin upgrade menu.

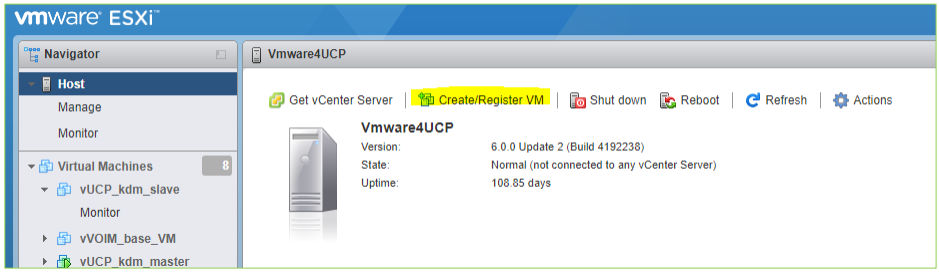
3.8.2 Deploying the OVF File

You can create a new virtual machine by following process. This process can take several hours depending on your network speed.

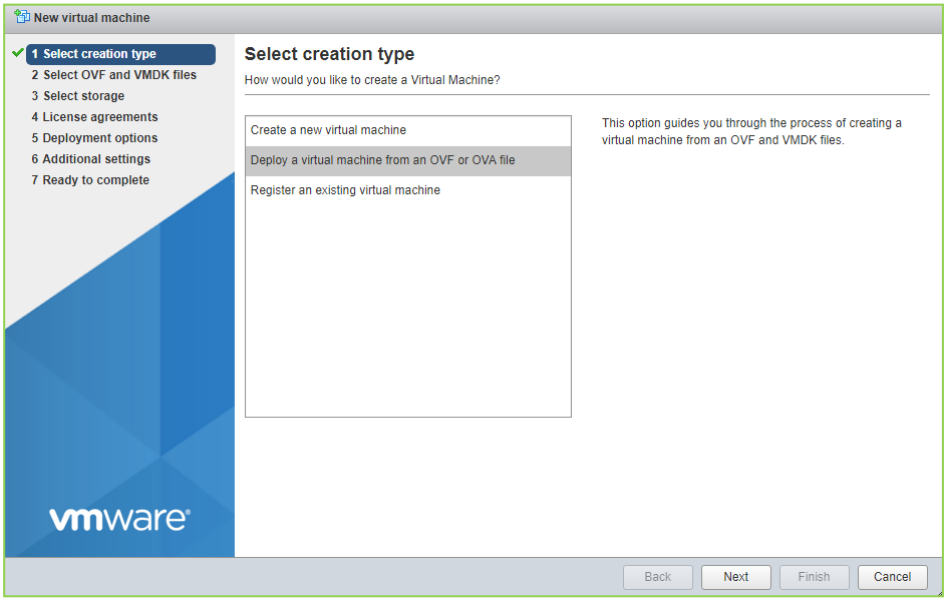
3.8.2.1 Deployment the OVF file using vSphere

1) Log in VMware ESXi.

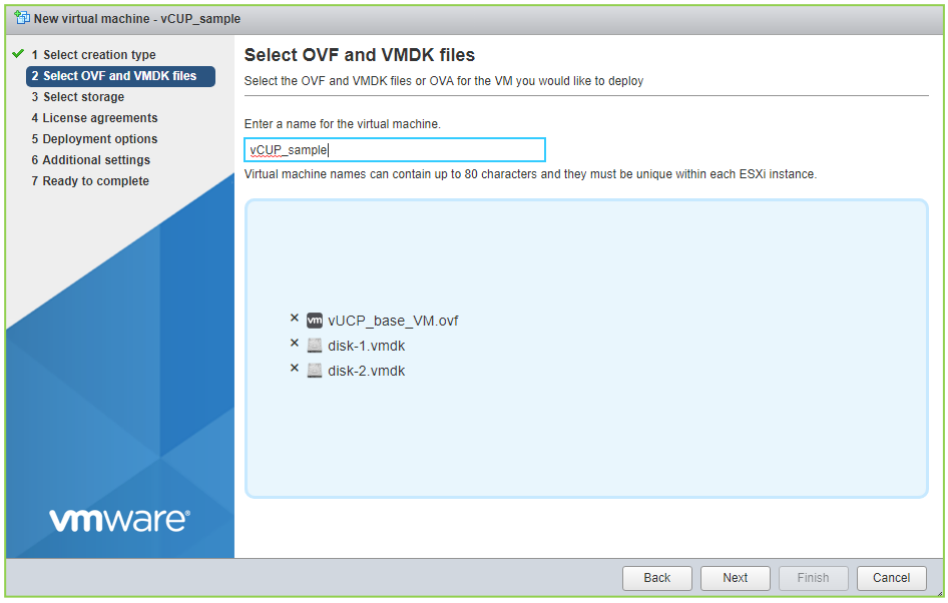
2) Click ‘Create/Register VM’.



3) Click ‘Deploy a virtual machine from an OVF or OVA file’ and then click ‘Next’



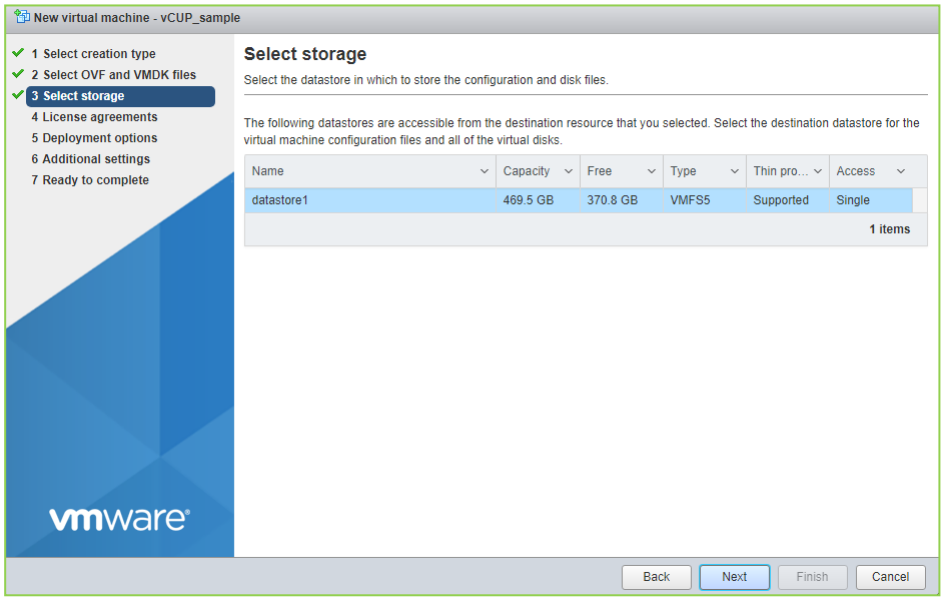
4) Input the name for the virtual machine, click to select files or drag/drop and then click ‘Next’



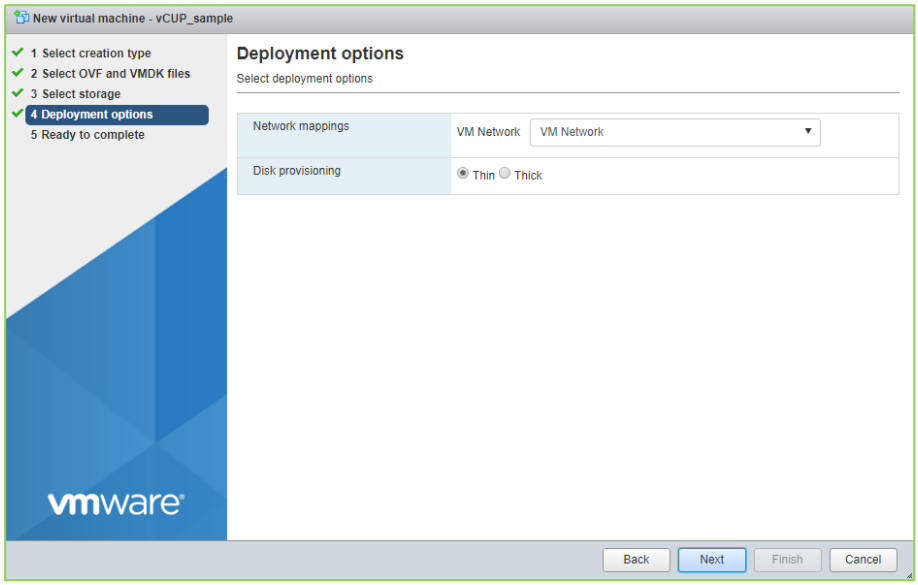
The number of ‘vmdk' files is different;

- vUCP (Lower SW version 5.0): 2 vmdk files, 32GB (application) + 1GB (DB data)
- vUCP (Higher SW version 5.0): 3 vmdk files, 8GB (application) + 1GB (DB data) + 1GB (Voice data)
- vUVM: 2 vmdk files, 32GB (application) + 16GB (VM messages)
- vVOIM: 1 vmdk file, 32GB (application)
- vMCIM: 1 vmdk file, 8GB (application)
- vVOIMT: 1 vmdk file, 8GB (application)

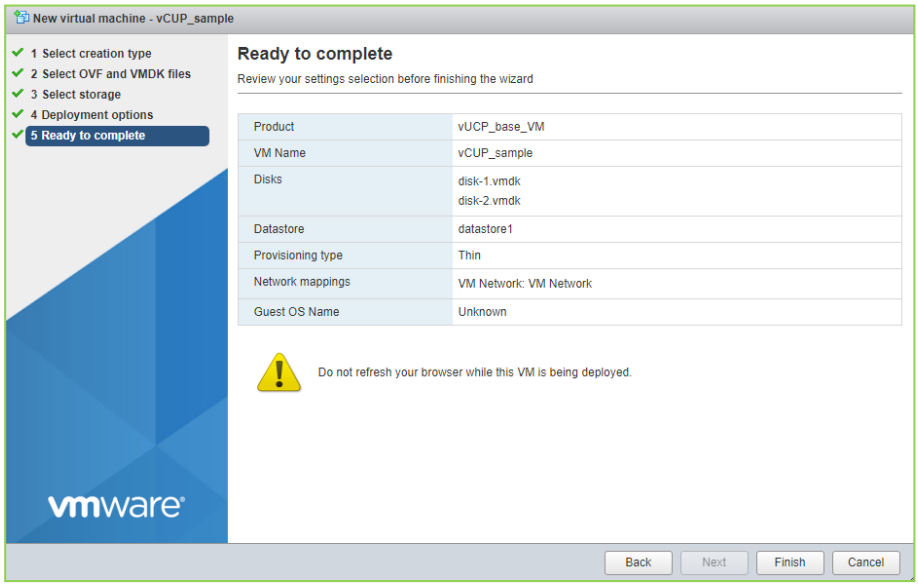
5) Select storage and then click ‘Next’.



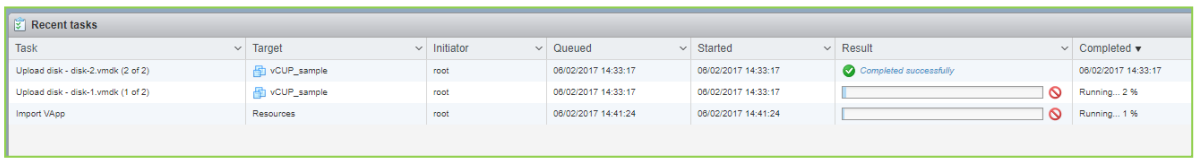
6) Select Network mappings and Disk provisioning and then click ‘Next’



7) Review the settings and then click ‘Finish’.



8) Wait until VM is created successfully



9) Once deployment has completed, the new virtual machine appears in Virtual Machines.

10) Change the disk size of ‘Hard disk 3’ for voice data (Optional, Higher SW version 5.0)

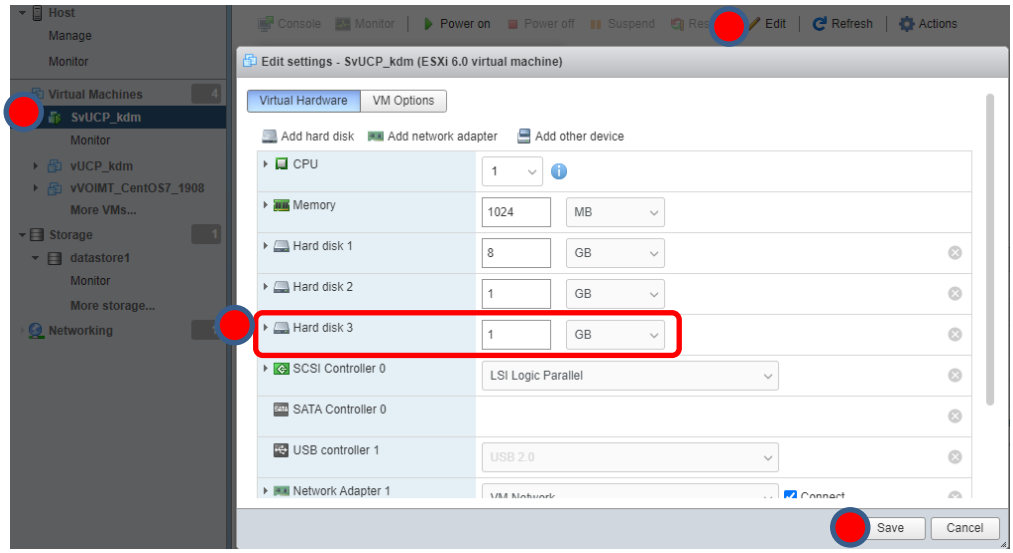
① Power off the VM

② Select VM

③ Click ‘Edit’

④ Modify

⑤ Click ‘Save’

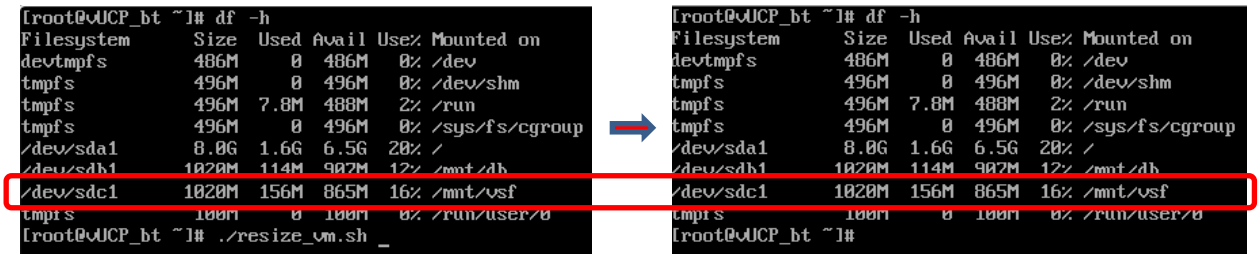


⑥ Power on the VM

⑦ Login as root

⑧ Input ‘./resize_vm.sh’

⑨ After reboot, check the status by ‘df –h’ command



You can find a required size in the following table.

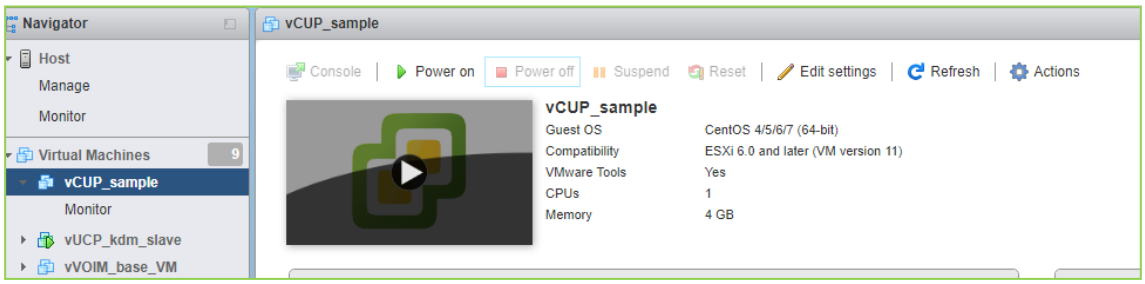
	100 hours	200 hours	300 hours	400 hours	500 hours
Disk Size	3 G Bytes	6 G Bytes	9 G Bytes	12 G Bytes	15 G Bytes

Note

You don’t need to change the profile of vUCP, vUVM, vVOIM/vVOIMT, vMCIM.

3.8.3 Power on VM

After clicking the created virtual machine, you can ‘Power on’ the system.



3.8.4 Connecting to Virtual Machine

After power on, you can connect to the virtual machine by SSH or Console of ESXi web.

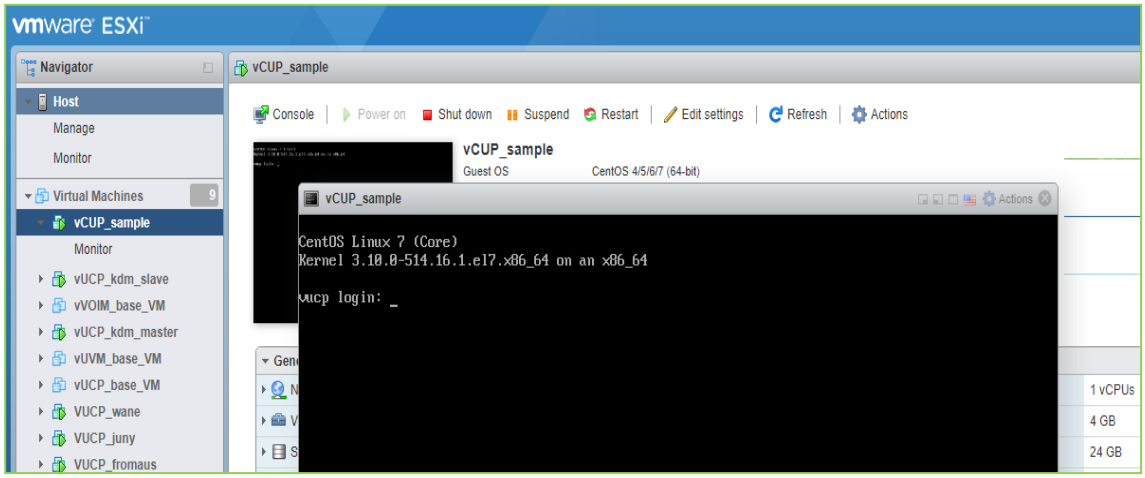
Default login values

- User: root
- Password: centos4vucp

You can find the default IP address. Refer to the chapter 3.8.5.1Default IP address.

3.8.4.1 Console of ESXi web

You can run local console by clicking ‘Console’ or the displayed figure.



3.8.4.2 SSH

You can access the virtual machine by SSH application such as putty. Use default SSH port number 22(vMCIM: 60022). If you want to enable or disable the SSH service, you can do it by below command after log in.

- Disable SSH

  # systemctl stop sshd.service

  # systemctl disable sshd.service
- Enable SSH

  # systemctl start sshd.service

  # systemctl enable sshd.service

3.8.5 Changing Network Settings

The IP address must be changed through console or SSH. (Secure Shell)

Because this process is related with Serial Number, you must change network settings to the confirmed values.

3.8.5.1 Default IP address

When you create new virtual machine using vUCP OVF files, each machine has following default IP addresses. When starting, if a duplicate IP address exists, each machine cannot run correctly. Therefore, you should change them by CLI command after deployment.

vUCP

- Virtual Machine IP address: 10.10.10.2
- Subnet mask: 255.255.0.0
- Router IP address: 10.10.10.1

vUVM

- Virtual Machine IP address: 10.10.10.3
- Subnet mask: 255.255.0.0
- Router IP address: 10.10.10.1

vVOIM

- Virtual Machine IP address: 10.10.10.4
- Subnet mask: 255.255.0.0
- Router IP address: 10.10.10.1

vMCIM

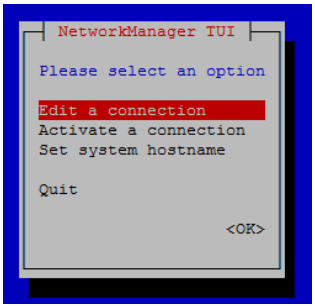
- Virtual Machine IP address: 10.10.10.9
- Subnet mask: 255.255.255.0
- Router IP address: 10.10.10.1

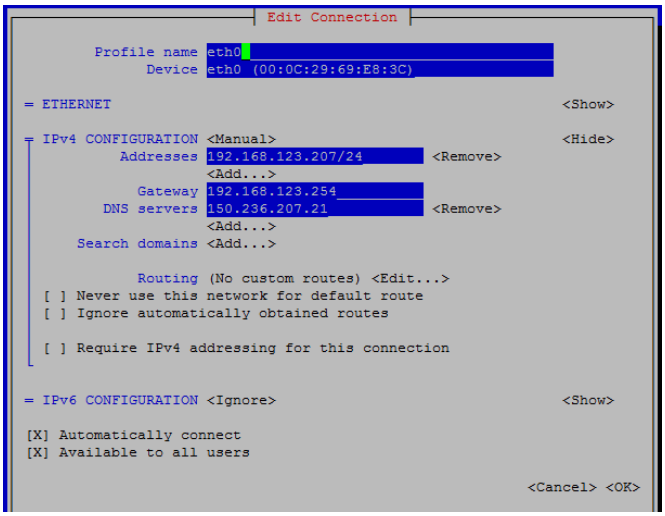
vVOIMT

- Virtual Machine IP address: 10.10.10.5
- Subnet mask: 255.255.255.0
- Router IP address: 10.10.10.1

3.8.5.2 Changing IP address

Input ‘nmtui’ and press enter key. When following figure is displayed, configure the network settings of eth0.





Note:

You can set system hostname, but it is optional.

vMCIM use other method. Refer to6.1.4vMCIM Installation.

3.8.5.3 Changing root password

Input ‘passwd’ and press enter key. Then you can change the root password.Remember the new root password. Otherwise you cannot access virtual machines to change IP address.

3.8.5.4 Restarting the Virtual Machine

After changes, input ‘restart’ and press enter key.

3.9 Reference Documents

Refer to theVMware related documents in the below URL

https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html

- vSphere Installation and Setup Guide
- vSphere Software Download

Refer to the vUCP related documents in the GPS website

https://partner.ericssonlg-enterprise.com

- vUCP Manuals
- Software Download (OVF)
- Upgrade Software Download (ROM)
- License Portal Link

4 Amazon Web Services Virtual Machines

From Unified version 3.5, vUCP is supported as AWS virtual machines, referred to as ‘instances’. Each AWS instance is created using below resources;

Region and Availability Zone

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links. This achieves the greatest possible fault tolerance and stability.

Machine Instance

This is serviced as Amazon Elastic Compute Cloud (Amazon EC2). AWS EC2 provides scalable computing capacity in the Amazon Web Services (AWS) cloud. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. AWS provide some types of machine instances (https://aws.amazon.com/ec2/instance-types). The type should be selected according to therequirements of vUCP.

Amazon Machine Image (AMI)

AWS supports Amazon Machine Image(AMI). AMI provides the information required to launch an instance, which is a virtual server in the cloud. To create instances for the service of vUCP system, you have to selectone of provided public AMIs such as vUCP, vVOIM/vVOIMT, vMCIM, and vUVM.

Disk Storage

Amazon EC2 provides you with flexible, cost effective, and easy-to-use data storage options for your instances. EC2 instance for vUCP systems will use EBS (Elastic Block Storage), and the storage is already defined and associated with the virtual machine. You can select the type of EBS volume during creating a EC2 instance. Refer to the Amazon EBS volume types in the below URL;https://aws.amazon.com/ebs/details/?nc1=h_ls

Security Groups

This acts as a virtual firewall for your instance to control inbound and outbound traffic.When you launch an instance in a VPC, you can assign up to five security groups to the instance. For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

Elastic IPs

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. An Elastic IP address is a public IPv4 address, which is reachable from the internet.

Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.This documentation does not cover the configuration of the customer's VPC.

The process of combining the elements above is referred to as ‘launching an instance’. At each process, you should define details of the components according to the AWS menus.

This section outlines the steps required to install vUCP systems. Before that, you have to select AWS region.

Installer and Maintainer Requirements

In addition to iPECS training, the installer must also have certified training on the specific virtual platform type or be supported by someone who has that certification. The same requirement applies to the system maintainer.

4.1 Profile of Virtual Machine

The Instance of vUCP, vUVM, vMCIM and vVOIM/vVOIMThas the following default value.

vUCP

- Instance type: t2.micro
- HDD: 8G Bytes (Application) + 1G Bytes (DB data) + 16G Bytes (Voice data, Higher SW version 5.0)
- Network: 1 Ethernet, DHCP

vUVM

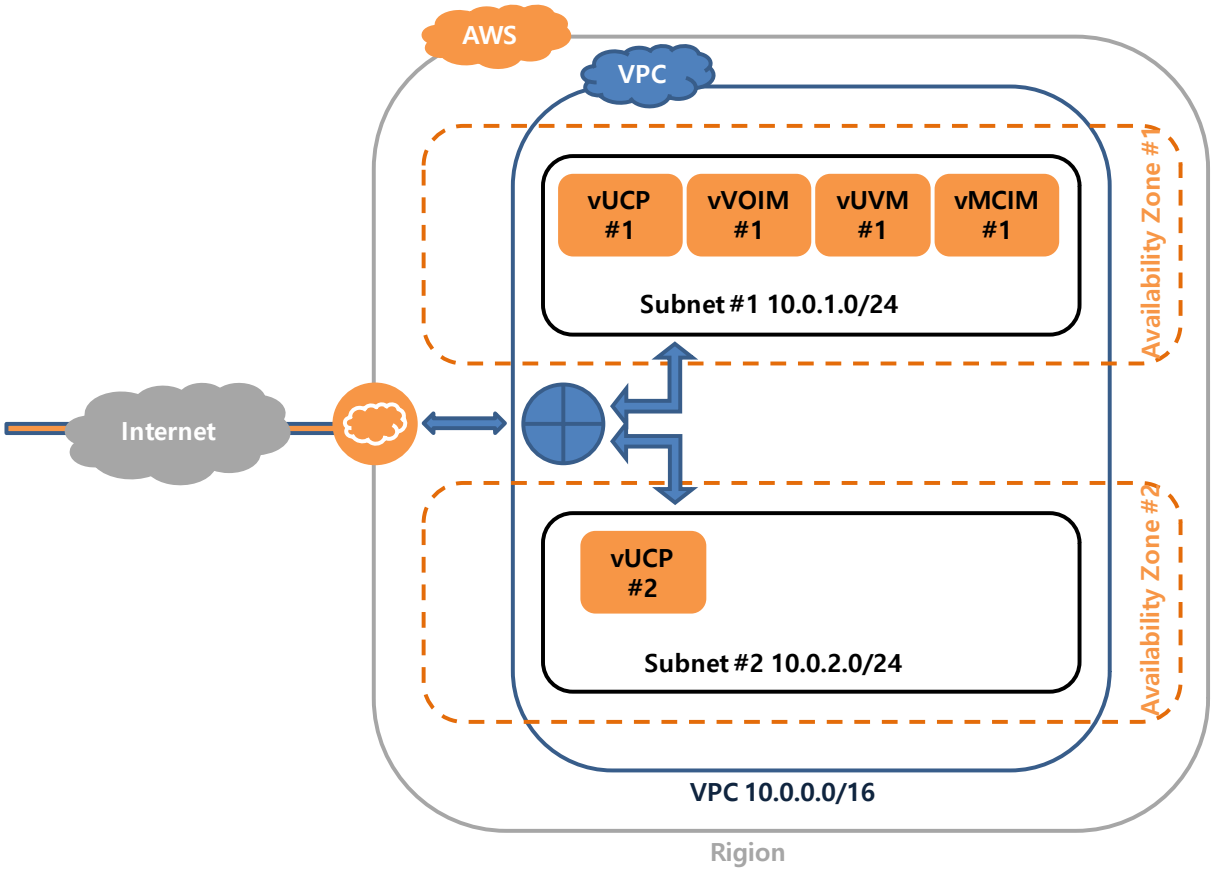
- Instance type: t2.micro
- HDD: 8G Bytes (Application) + 16G Bytes (Voice data)
- Network: 1 Ethernet, DHCP

vVOIM, vMCIM, vVOIMT

- Instance type: t2.micro
- HDD: 8G Bytes (Application)
- Network: 1 Ethernet, DHCP

4.2 Creating VPC

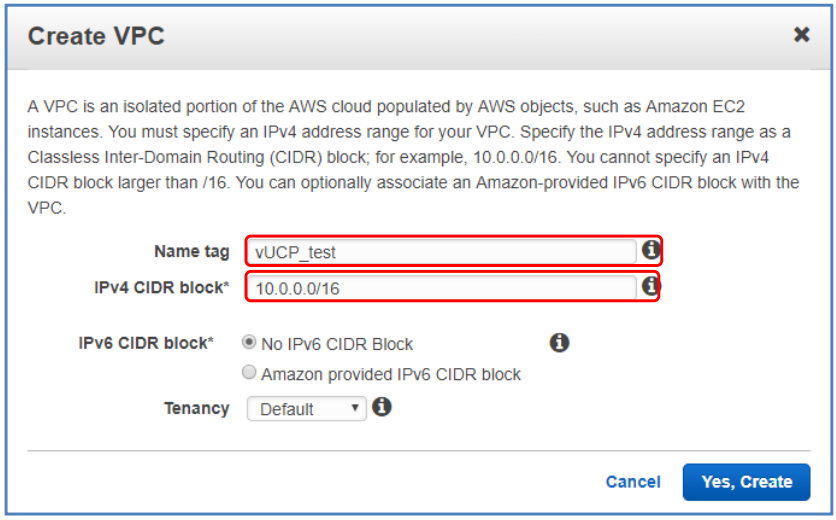
The following is a possible VPC configuration for vUCP system. You can create a VPC for your own purpose.This documentation does not cover the configuration of the customer's VPC because the configuration of VPC varies according to the customer's needs.



4.2.1 Create VPC

- VPC > Your VPCs > Create VPC > Input ”Name tag” and “IPv4 CIDR block” > Click “Yes, Create”

Input ‘Name tag’ and ‘Ipv4 CIDR block’.



4.2.2 Create Subnet

- VPC > Subnets > Create Subnet

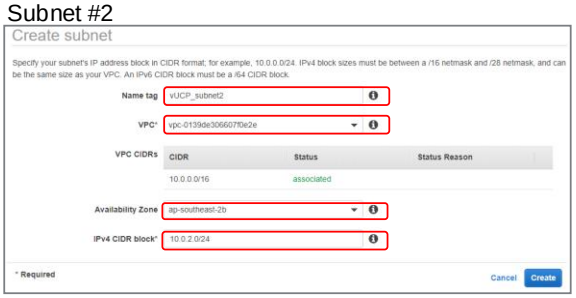
Input ‘Name tag’ and select ‘VPC’ (4.2.1 *Create VPC*).

Select ‘Availability Zone’ and input ‘Ipv4 CIDR Block’. Then click ‘Create’.

Repeat at each Availability Zone.

Subnet #1

Subnet #2

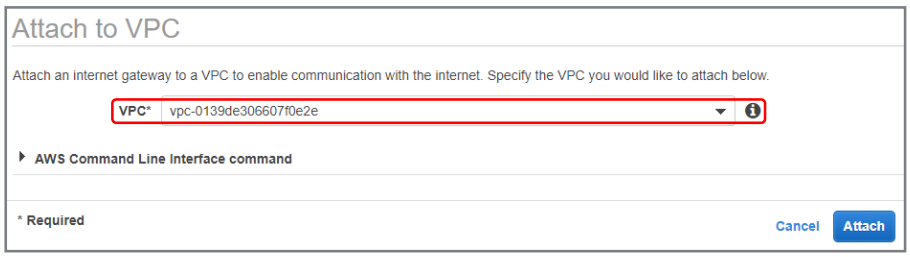


4.2.3 Create Internet Gateway

- VPC > Internet Gateways > Create Internet Gateway > Select ‘created igw’ > Attach to VPC

Input ‘Name tag’ and click ‘Create’

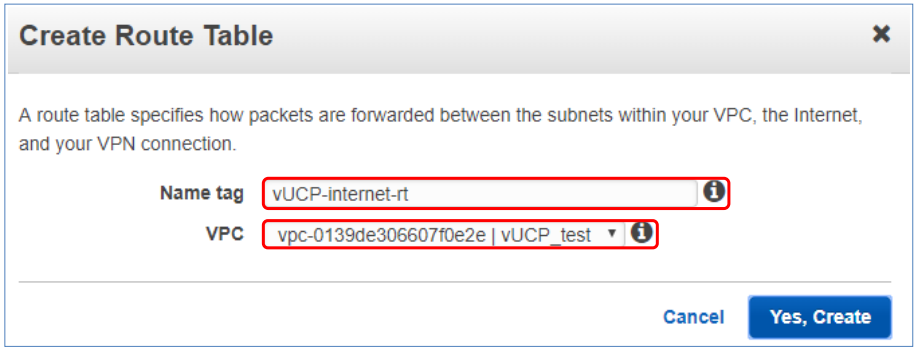
Select ‘VPC’ (4.2.1 *Create VPC*) and click ‘Attach’



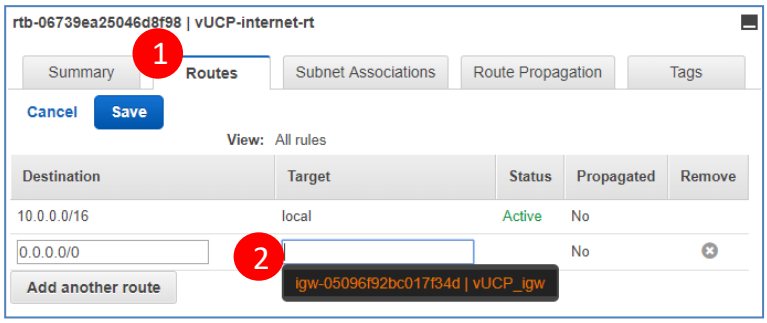
4.2.4 Create Route Table

- VPC > Route Tables > Create Route Tables > Select ‘mydemovpc-internet-rt’ > Routes > Subnet Associations

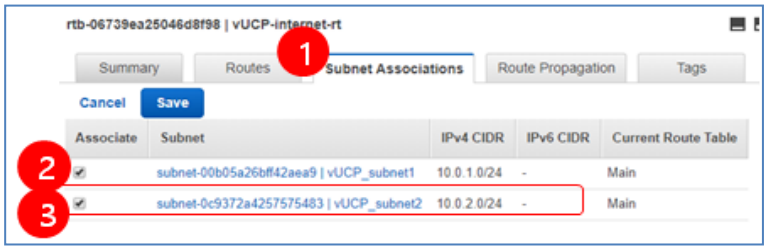
Input ‘Name tag’ and select ‘VPC’ (4.2.1 *Create VPC*).



Click ‘Routes’ and Input ‘Destination’ and ‘Target’(0 *Create Internet Gateway*).



Click ‘Subnet Associations’ and associate all subnets.

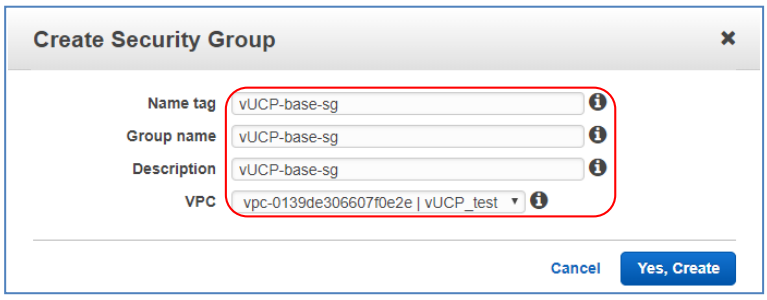


4.2.5 Create Security Groups

- VPC > Security Groups > Create Security Group > Select ‘vUCP-base-sg’ > Inbound Rules > Edit

Input ‘Name tag’, ‘Group name’, and ‘Description’.

Select VPC(4.2.1 *Create VPC*).



Click ‘Inbound Rules’ and add your rules.

Above ‘Inbound Rules’ is created to let the test easy. Therefore, you have to add the rules for your purpose.

Before launching any instances, you should create security groups. When launching a new instance, you can select security group that it should be use.

- ✓ When launching a new instance, you should a highly restricted security group which allows minimum access. For example, one that allows access from your IP address and using HTTPS (port 443) and SSH (port 22) access.
- ✓ Once the instance is ignited and an initial configuration is completed, you can change the security group of that instance.

Refer to the Security Groups in the below URL;

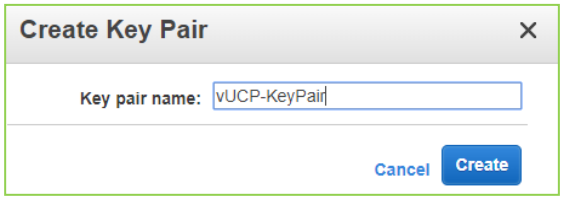
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

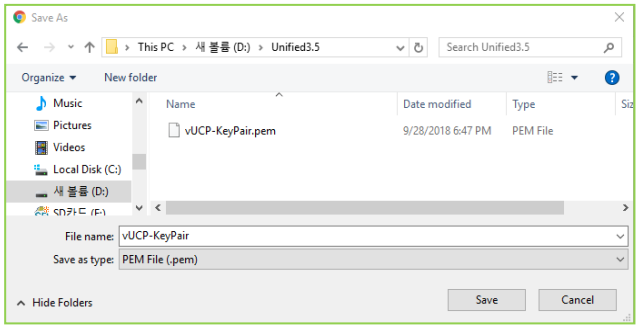
4.3 Launching a New Instance

4.3.1 Create Key pair

Before launching a new instance, you had better created the key pair which will be used to access to the instance. Of course, it might be created during the launching a new instance.

- EC2 > Key Pairs > Create Key Pair > Input “Key pair name” and click “Create” > Save the key file to the local disk.





The keyfile should be kept secure because it is used to access your virtual machine. Whenit is leaked, all your virtual machines would be at risk. And if you lose it, you will not able to access your virtual machines by SSH.

4.3.2 Prerequisite

If you want to use AMI images of iPECS system outside of ‘Asia Pacific (Seoul)’ region, you should copy AMI images to your region. Using the AMI Copy function, it is only possible to copy those AMI images that belong to your account. It is not possible to copy AMI images belonging to others.Refer to below link.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html

To get around this, you can:

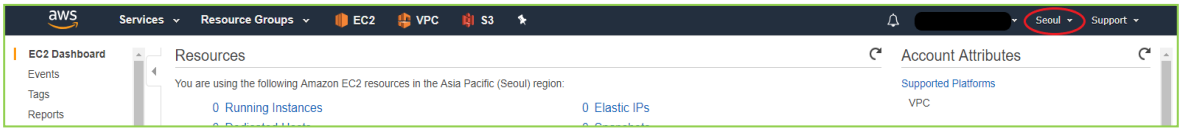
1) Launch an instance in ‘Asia Pacific (Seoul)’ region with the wanted AMI. Note that you had better just launch and stop it before allocating an EIP, because an initial setup or registration is useless. Refer to 4.3.3Launching a New Instance.
2) Create a new AMI from your instance. Refer to 4.5Creating an AMI image.
3) Copy that AMI to your desired new region. Refer to 4.6Copying an AMI image.
4) Launch an instance in your target region with your copied AMI. Refer to 4.3.3Launching a New Instance.
5) If you don’t use the instance in any region, delete the original instance, snapshot, and AMI image not to pay an additional charge. Refer to 4.7Deleting unused resources.

The following is a general example for launching a new virtual instance. The exact process may vary because the customer’s requirements are different for VPC and external networks.

4.3.3 Launching a New Instance

To launch a new AWS virtual machine:

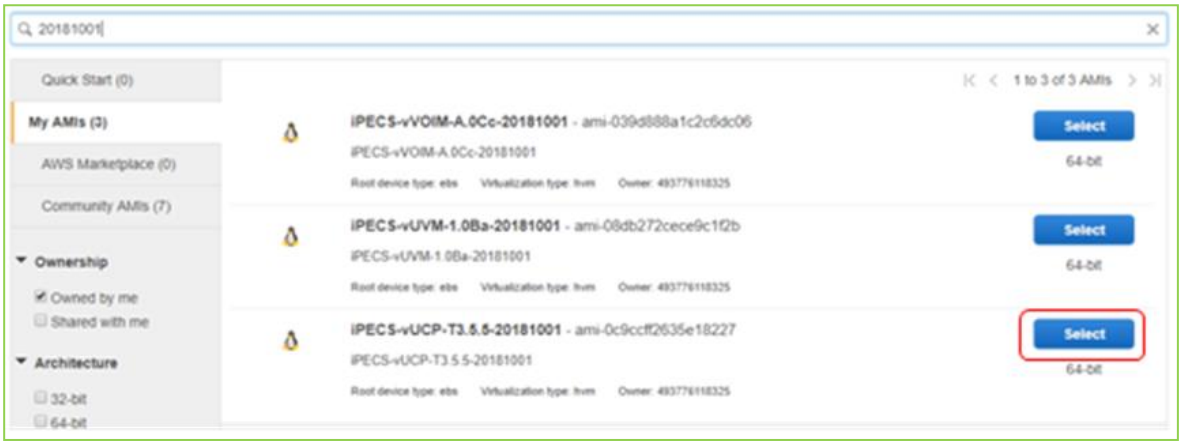
1) Sign into your AWS account. Click **Services** and select **EC2**.
2) Select the region, for example **Asia Pacific (Seoul)**. It is recommended that the selected region is closer to the serviced area.



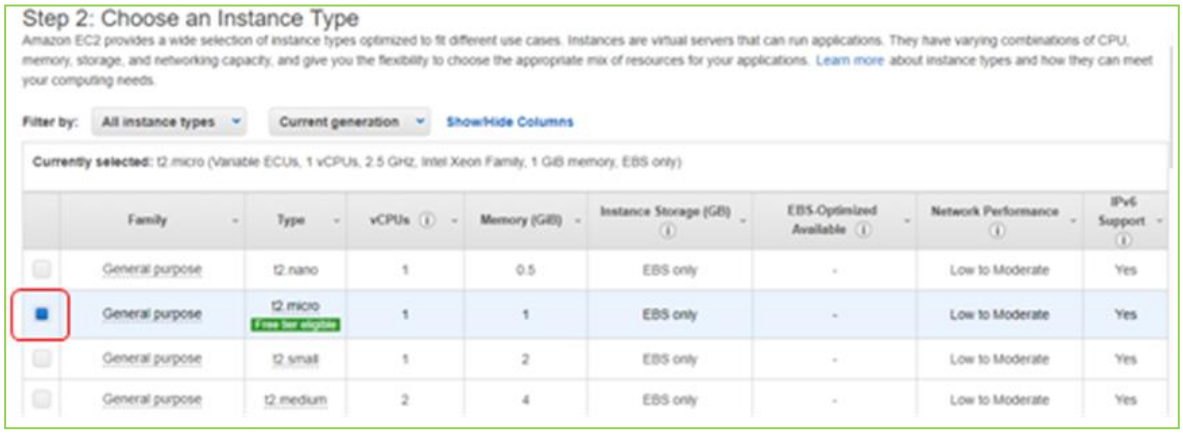
3) Click **Launch Instance**. Select **Community AMIs** and enter **iPECS** as the search sting. Note that, outside of **Asia Pacific (Seoul),** you should prepare your own AMI images refering to **4.3.2 Prerequisite**. If you already copy the AMI images to yourdesired AWS region, the AMI image would be displayed in **My AMIs**.
4) Click **Select** where the required AMI is located. The name will show a system name and a version. For example, **iPECS-vUCP-R3.5.5** is the AMI for vUCP Release 3.5.5. You also find other systems like **vVOIM/vVOIMT, vUVM, and vMCIM**.

Case 1: Search results in Community AMIs in Seoul region.

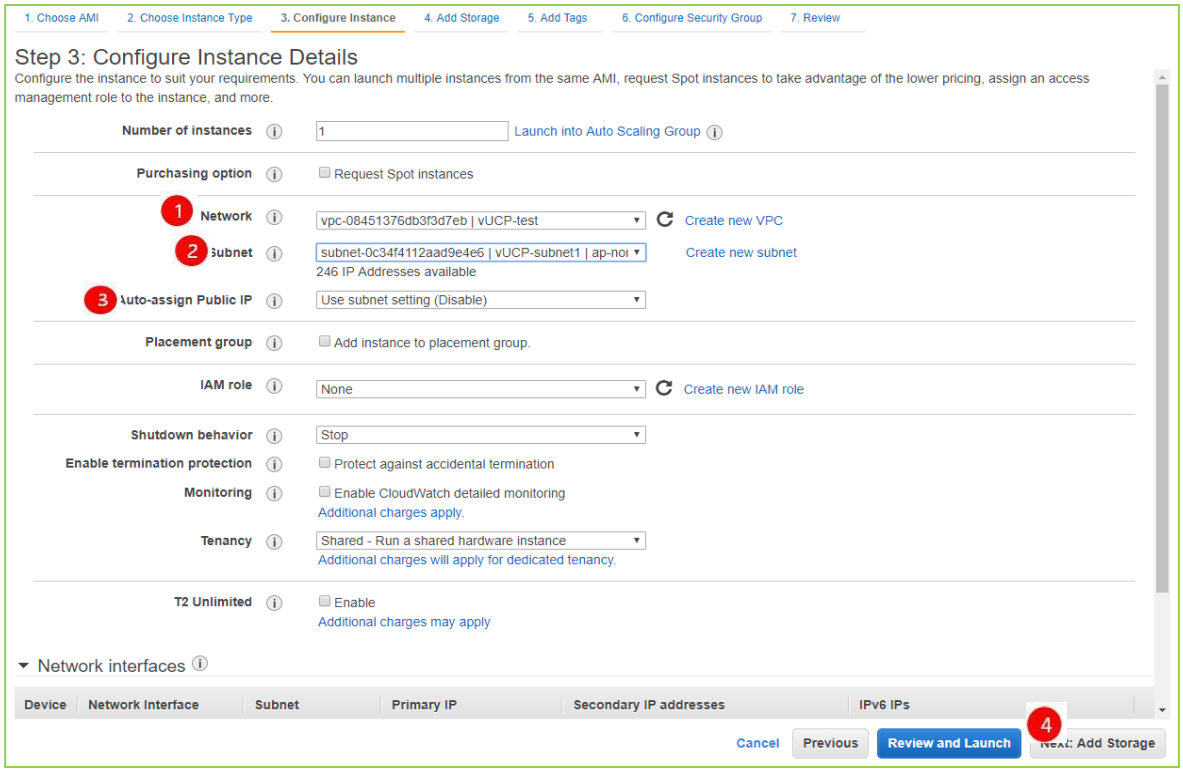
Case 2: Copied AMI images in **My AMIs in your region.**



5) Select a machine instance that matches the 4.1Profile of Virtual Machine and click “Next”. The “t2.micro” is used for iPECS system.



6) Click Next: Configure Instance Details.

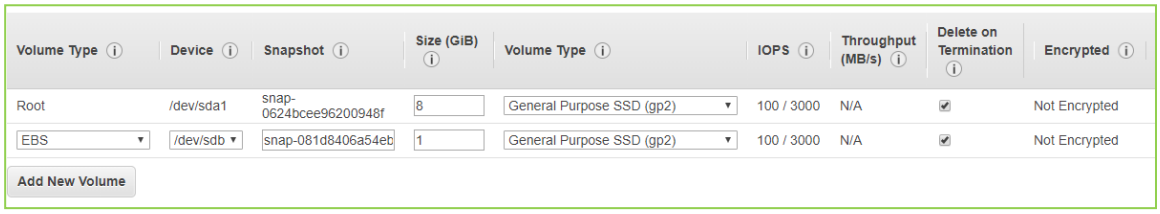


Select the customer’s VPC and the subnet.

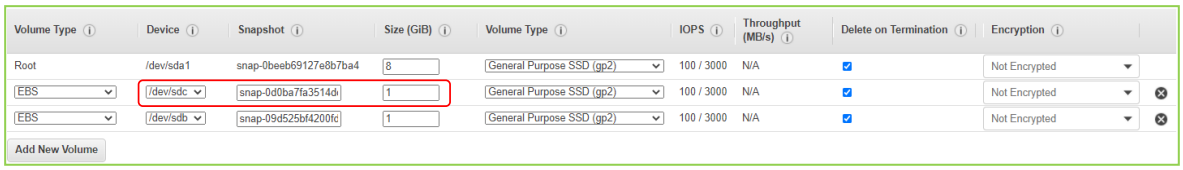
Select ‘**Use subnet setting (Disable)**’ as Auto-assign Public IP. Because vUCP systems use a persistent public IP address, you should use an Elastic IP address (EIP) instead. You can allocate your own EIP and associate it to your instance after launch.

7) Click Next: Add Storage.

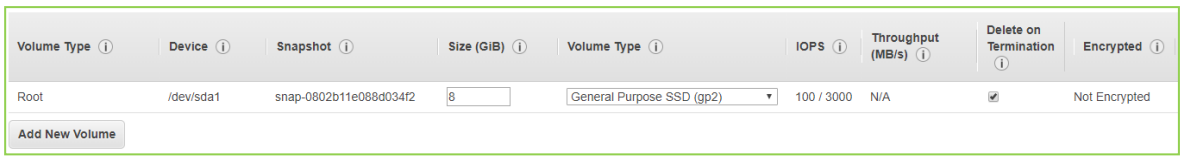
vUCP (Lower SW version 5.0): Do not change



vUCP (Higher SW version 5.0): Change the disk size of 'dev/sdc' for voice dat

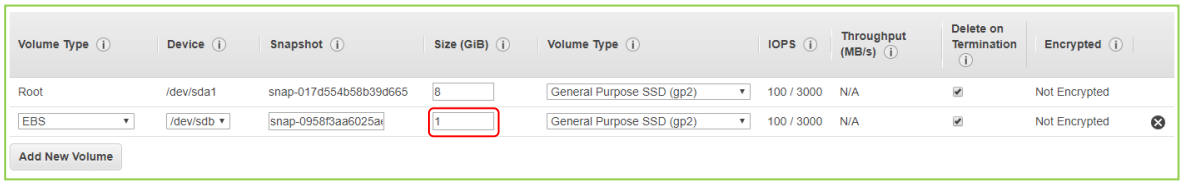


vVOIM/vVOIMT, vMCIM: Do not change

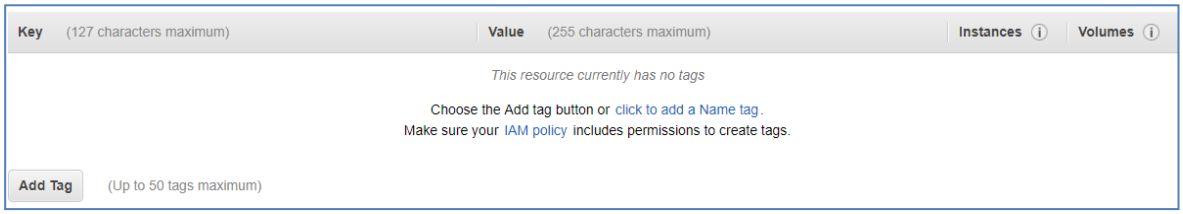


vUVM: Change the disk size of '/dev/sdb' for voice storage according to the recording time.

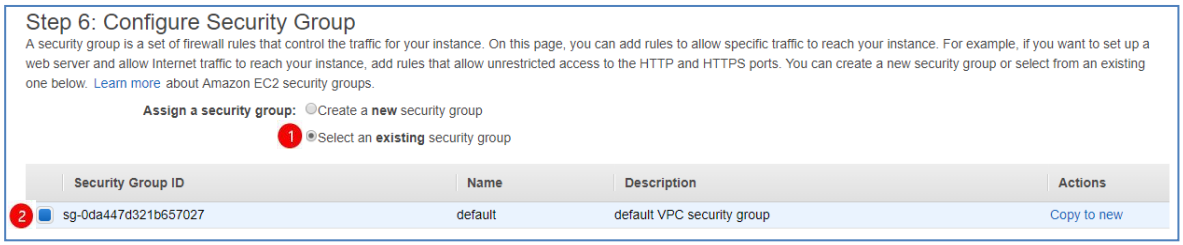
	100 hours	200 hours	300 hours	400 hours	500 hours
Disk Size	3 G Bytes	6 G Bytes	9 G Bytes	12 G Bytes	15 G Bytes



8) Click **Next: Add Tags.** Enter any tags that you want associated with this instance. Tags can be displayed and used in other EC2 menus to display, sort and group matching resources



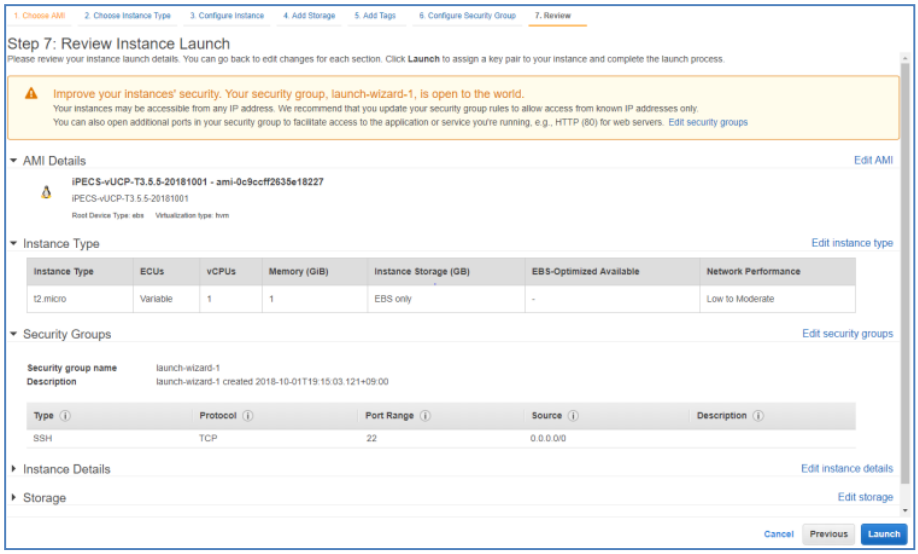
9) Click **Next: Configure Security Group.** Select the system installer's security group that you previously created in **4.2Creating VPC**.



Note: Allows minimum hosts and protocols such as HTTPS (port 443). This is needed until the initial configuration is completed because the default passwords are applied in the new instances.

If you don't select a created group, a default security group would be created.

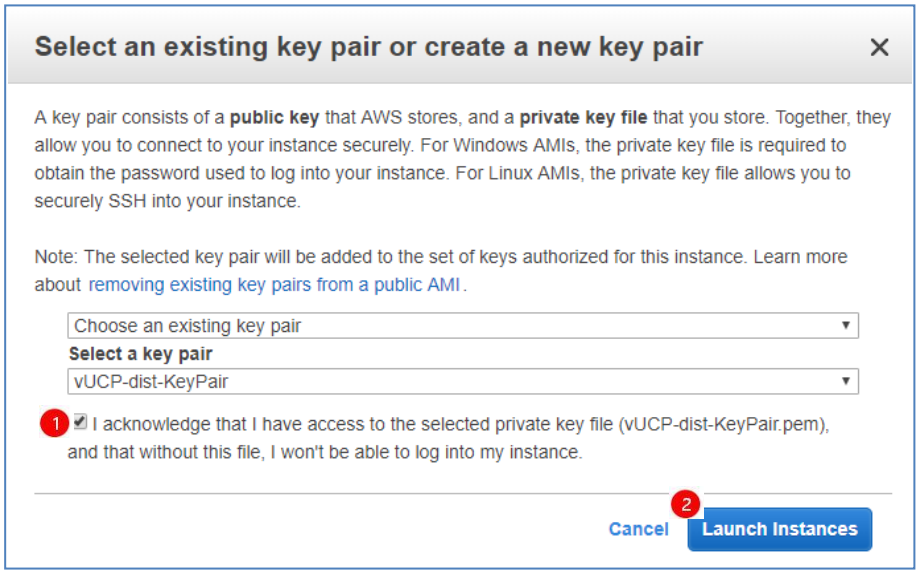
10) Click **Review and Launch**. Check all details. If so, click **Launch**.



Pop up: Select an existing key pair or create a new key pair.

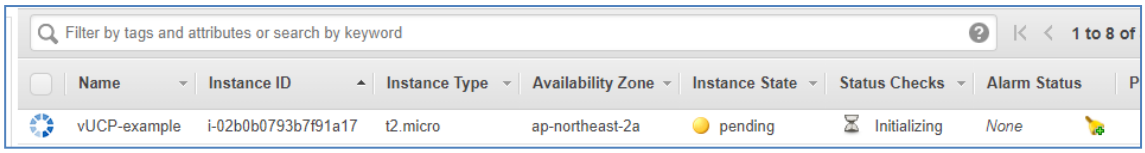
This key file provides a security certificate for secure SSH access to the virtual machine. You can use the key pair file which is created in 4.3.1Create Key pair.

If you want to create a new key pair, click Download Key Pair and make sure that you stored it in a safe place.



11) Click Launch Instances.

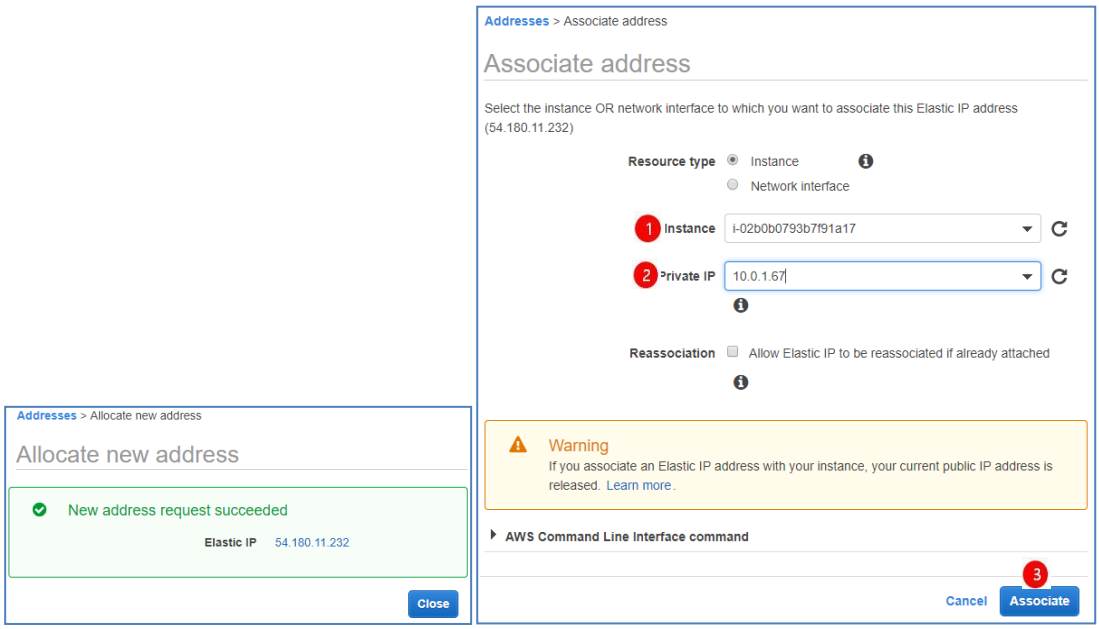
12) If all is successful, click **View Instances**, or select **Services > EC2 > Instances**. The new virtual machine should be displayed in the list of your instances.



13) The machine starts by performing initial formatting and partitioning of the storage. This takes approximately 5 to 10 minutes to complete.

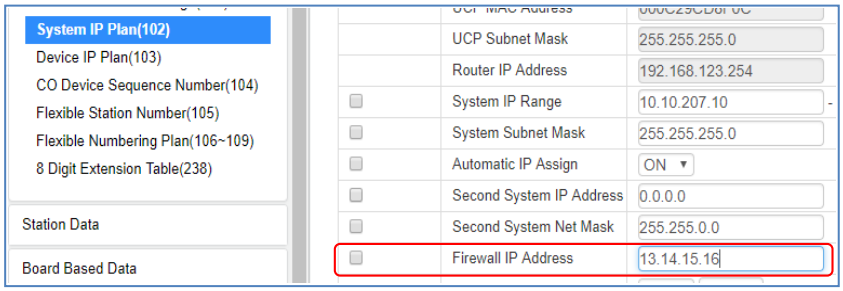
14) Allocate **EIP.**

- Select Services > EC2 > Network & Security > Elastic IPs.
- Click Allocate new address.
- Click Allocate.
- Click Close.
- Mark the new created EIP, and then select Actions > Associate address.
- Set instance and Private IP to the new created.
- Click Associate.

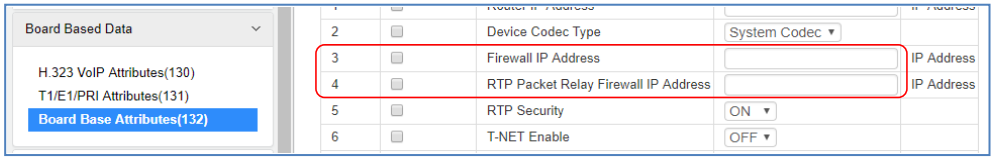


Note

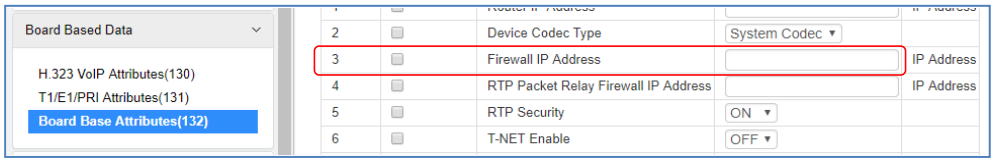
- vUCP: Need EIP for external access. It should be used as the firewall IP address in PGM102.Therefore you should generate system serial number after setting the firewall IP.



- vVOIM/vVOIMT: Need EIP for external access. it should be used as the firewall IP address and RTP Packet Relay Firewall IP Address in PGM132.



- vUVM: Need EIP for external access. It should be used as the firewall IP address in PGM132.



- vMCIM: Not need EIP, but you can use it for your purpose.

15) Proceed with **4.4 Connecting to Virtual Machine** and 5**. License and Serial Number.**
You can access to the vUCP systems through the assigned public IP address.
The private IP address is assigned automatically and is used within the custom VPC.
Therefore, in case of AWS, you don't need to configure the IP address of virtual machine, but the EIP address is treated as the system's firewall IP address because VPC is used.

4.4 Connecting to Virtual Machine

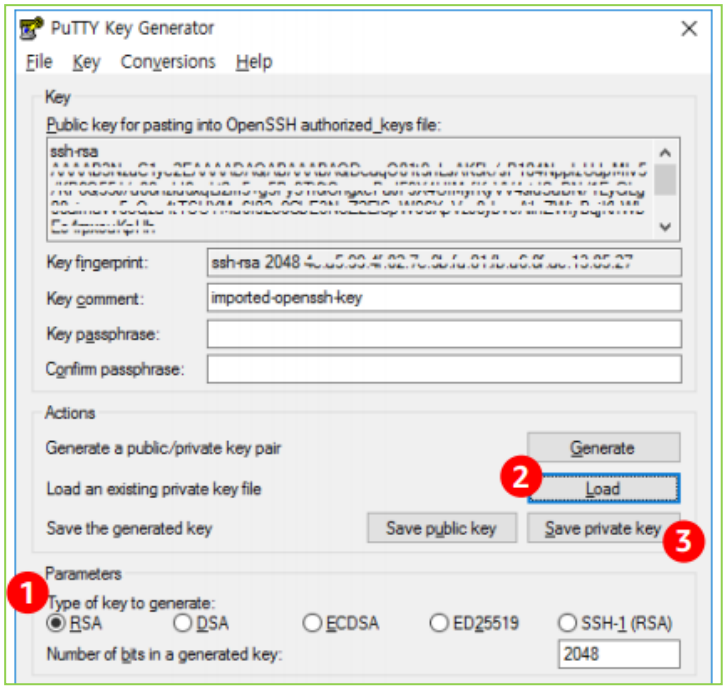
After power on, you can access to the virtual machine by SSH. Note that you should use the public IP address of EC2 instance and the default SSH port number is 22.

You should use your private key(refer to 4.3.1Create Key pair) which was get from AWS (PEM ► PPK);

PuTTYgen and PuTTY are needed.

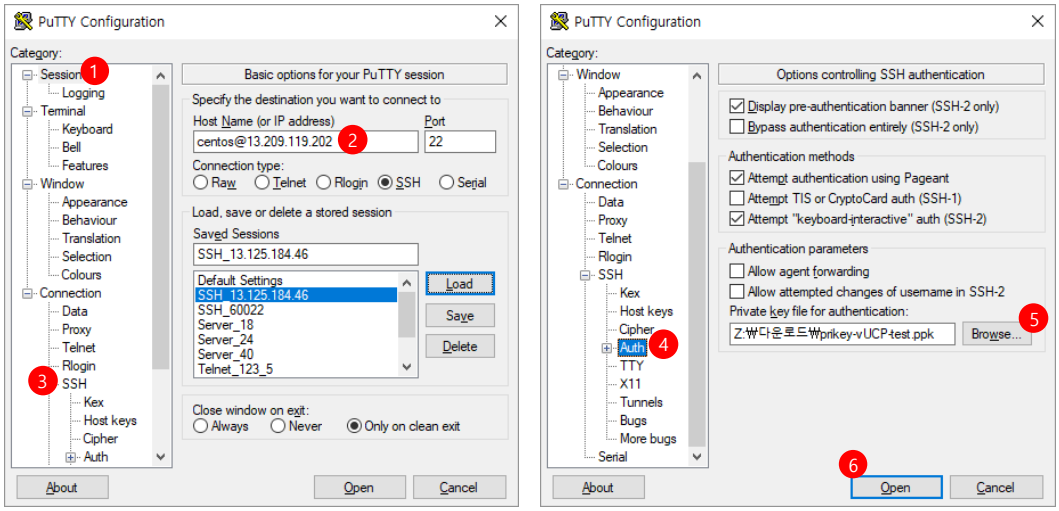
Private key creation

1) Start PuTTYgen.
2) Select [RSA (SSH-2)]
3) Load the saved PEM file by [Load]
4) Covert to the PPK file by [Save private key]



PuTTY Session

1) Start PuTTY
2) Select [Category > Session] and input “centos@public IP”
3) Select [Category > Connection > SSH > Auth], lick [Browse] and select PPK file
4) Click [Open]



Login user is “centos” and no password was needed, due to the authentication method.

Remember that you should add “sudo”before the shell command, because current user is “centos” and does not have ‘root’ permission. For example, “***sudo*** systemctl stop watchdog”.

4.4.1 Changing Network Settings

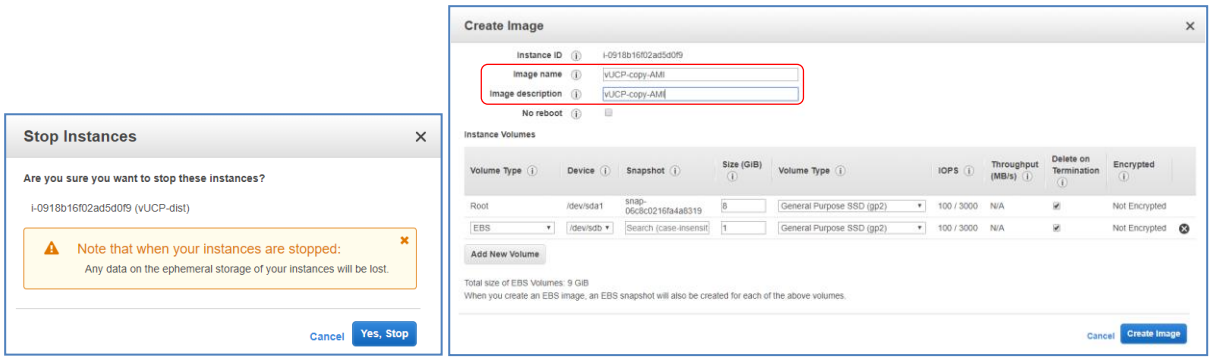
You don’t need to change the network settings of EC2 instance, if you use the VPC and EIP. The assigned values are not changed until the instance settings are not varied.

Note : if you use EIP for vUCP, the firewall IP address of vUCP would be the EIP. If you use other your own network such as NAT, you should set a correct value as the firewall IP of vUCP.

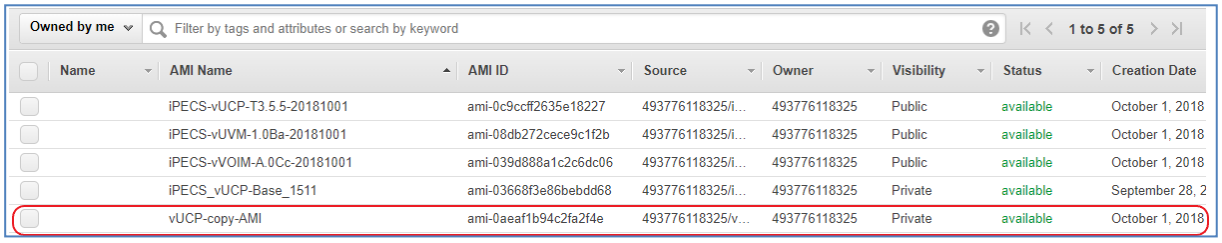
4.5 Creating an AMI image

After launching an instance, you can create your custom AMI image.

- EC2 > Instance > “Select the instance” > ‘Actions > Instance State > Stop’> ‘Actions >Image >Create Image’



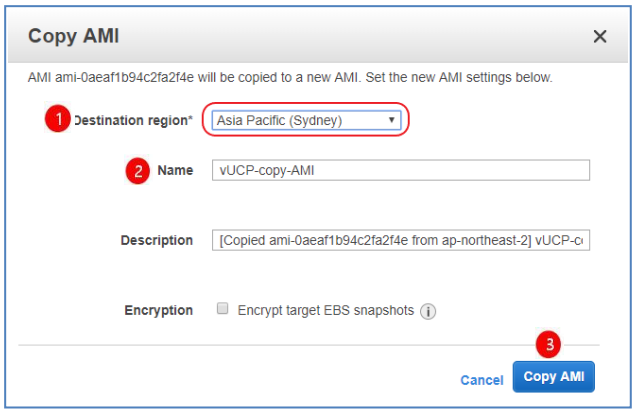
You can find the created AMI image in “EC2 > IMAGES> AMIs”.



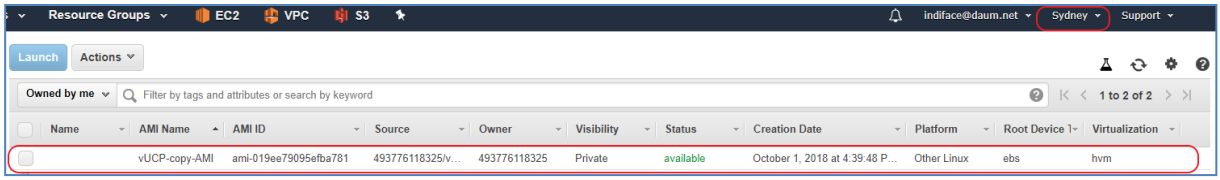
4.6 Copying an AMI image

To use AMI images in other AWS region, you have to copy them to other AWS region.

- EC2 > IMAGES> AMIs > “Select the AMI image” > Actions > Copy AMI > “Select Destination region” > Click “Copy AMI” > Click “Done”



You can find the copied image in “EC2 > IMAGES> AMIs” in the destination region.

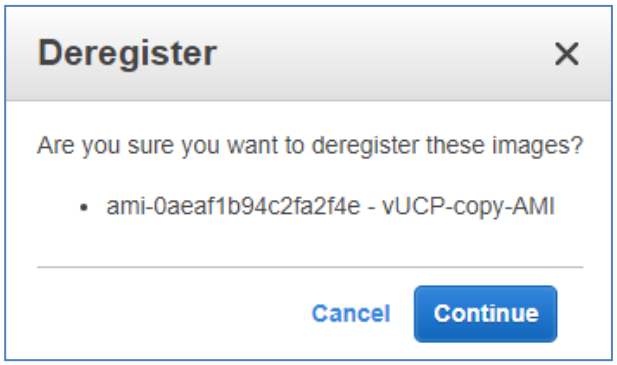


4.7 Deleting unused resources

After copying AMI images to other AWS region, you had better remove the resources like AMI images, snapshots, instances, and volumes, which are not used anymore in ‘Seoul’ region. And after launching AMI images in other AWS region, you had better also remove the resources like AMI images, and snapshots. Otherwise you might have to pay an additional charge.

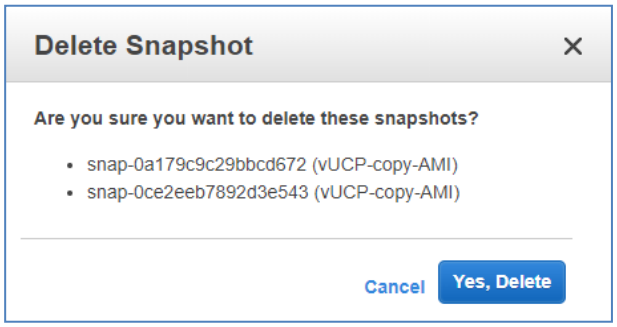
4.7.1 Deregister AMI images

- EC2 > Instance > “Select the instances” > Actions > Deregister > Click “Continue”



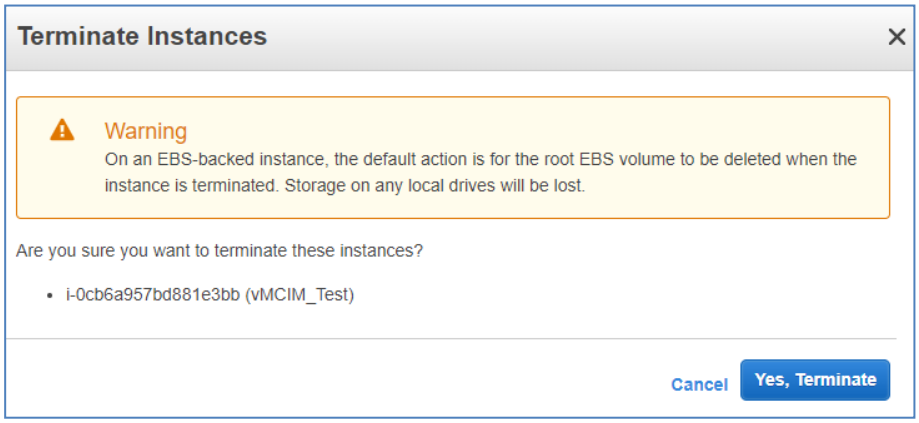
4.7.2 Deleting Snapshots

- EC2 > Elastic block store > Snapshots > “Select Snapshots” > Actions > Delete > Click “Yes, Delete”



4.7.3 Deleting Instances

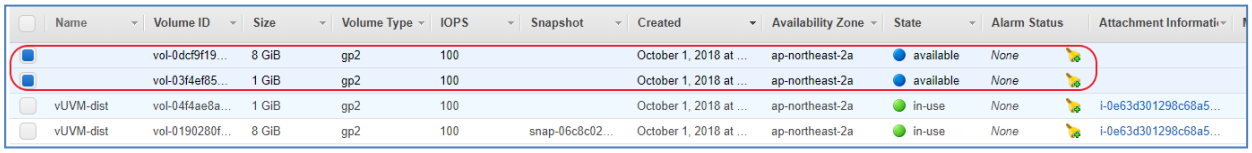
- EC2 > Instance > “Select the instances” > Actions > Instance State >Terminate > Click “Yes, Terminate”

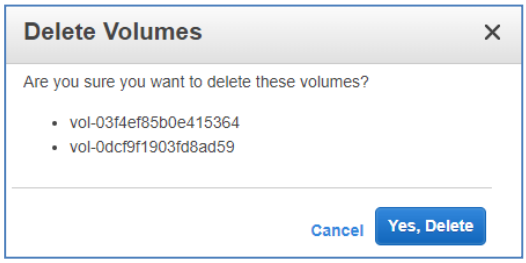


4.7.4 Deleting Volumes

After deleting instances, detached volumes might be left. You had better remove them to avoid an addition charge.

- EC2 > Elastic block store > Volumes > “Select Volumes” > Actions > Delete Volumes > Click “Yes, Delete”





4.7.5 Deleting EIPs

If you don’t need EIPs anymore after deleting instances, you had better remove them to avoid an addition charge.

- EC2 > Elastic IPs > “Select EIPs”> Actions > Release addresses > Click “Release”

5 License and Serial Number

The vUCP requires licenses to enable vUCP system and to use various business applications and advanced features. In order to get the license, unique software serial numberneeds to be created after installing vUCP software on a virtual server and configuring mandatory parameter from the system Web-admin. Unique software serial number is built in the combination with virtual machine related factors and system related factors described in the following sub sections. This means that new installation on another virtual machine or any change of parametersimpact the system serial number and this causes system goes into the limited service mode,which allows only internal calls and emergency external calls. Therefore, it is strongly recommended that all these parameters are finalized before creating the software serial number from the Web-admin. Before the licenses order, you can create a unique Serial Number at any time. But after the order and upload of a license file, you should transfer the existing licenses by a license transition process, if you want to change the virtual machine or the system related factors.

5.1 Related Factors of vUCP Serial Number

5.1.1 Virtual Machine Related Factors

One of related factors is the information of virtual machine. If you redeploy the virtual machine, the Serial Number will be changed and the system will immediatelygo to ‘Limited Service Mode’. If you use old licenses in new virtual machine, you should transfer the existing licenses to new virtual machine through our license portal. To move the virtual machine to another virtual server platform without requiring new licenses, use the vMotion.

5.1.2 System Related Factors

Other related factors are following system information:

- System IP address
- Router IP address
- Firewall IP address

If you change one or more among above IP addresses, the Serial Number will be changed and the system will immediatelygointo ‘Limited Service Mode’. But if the information of IP addresses is restored to original value, the Serial Number will be also restored and you can use it normally. Of course, if you want to change the IP addresses, you should transfer the existing licenses.

Note: in AWS, EIP should be used as firewall IP.

5.1.3 Grace period

When Serial Number is invalid, the system goes into‘Limited Service Mode’. At that time, you can restore the system related factors or select ‘transfer’ in ‘License Upload’ menu of web admin. If you click‘transfer’ button, the system will exit from ‘Limited Service Mode’ and the 30-day grace period will start. During that grace period, you can use the system normally, but should transferexisting licenses to new generated Serial Number in our License Portal. Otherwise it will go to ‘Limited Service Mode’ again, and remain in that state until uploading a new license file.

5.2 Serial Number Creation and License Transfer

Serial Number is used to activate the licenses in vUCP. Therefore, after deployment of vUCP virtual machine, you should create it in system web admin and upload a license file.

After uploading a license file, you should transfer the licenses in below cases. It is possible through system web admin and license portal.

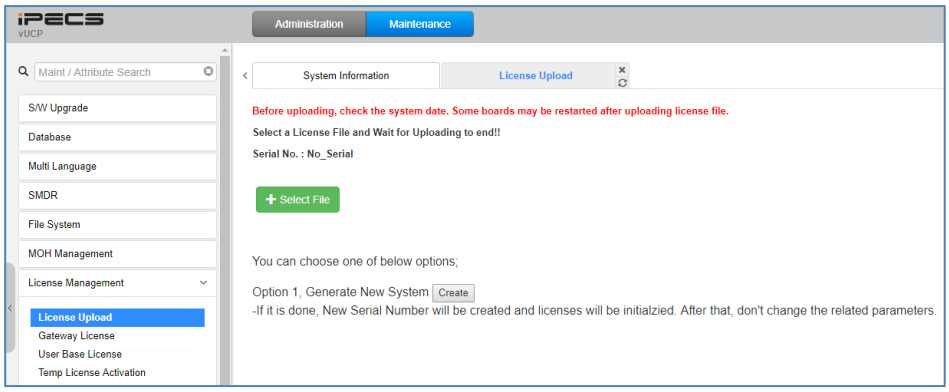
1) The server which contains the vUCP virtual machine is replaced with new one.
2) The virtual machine was moved to another virtual machine without vMotion.
3) The IP address of vUCP system, router, or firewall is changed.

5.2.1 Serial Number Creation

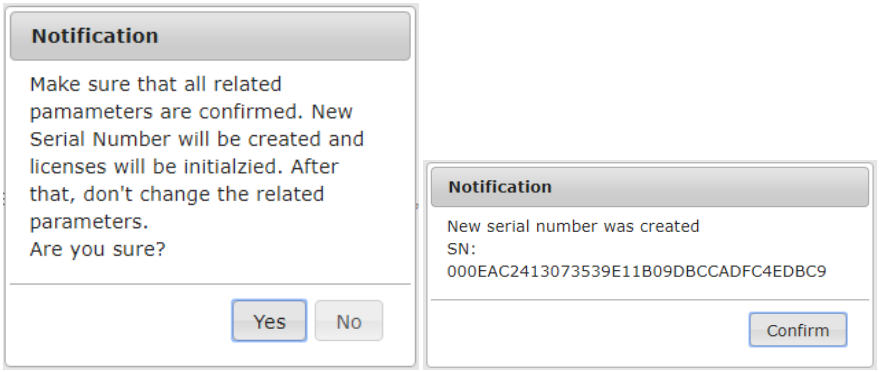
After installing the vUCP applications and configured all required parameters, you can create the Serial Number only in system web admin.**Note that, in AWS, EIP should be used as firewall IP.**You can download an official license file using this unique serial number.Uploadingthe license file on to the system enables the system run in a normal operation mode.

Don’t change the related parameters after a new Serial Number is created by ‘create’ button. If you change them, the Serial Number will be invalid, and the system will go to limited service mode.

The creation is done in ‘Maintenance > License Management > License Upload’ of web admin. You can create a Serial Number by clicking ‘Create’ button.



After that, confirm the below popup windows.



After the creation of Serial Number, you can create a license file with that. If you upload the license file on to system, it will run in normal mode. Note that, before uploading the license file, the vUCP will remain in limited service mode.

5.2.2 License Transition

If you want to change virtual machinesor the system related factors, you can transfer current existing licenses from the current Serial Number to new one. Make sure that the transfer process should be done after all related factors are confirmed.

The transfer of licenses should be done both in system web admin and in license portal.

Refer to following procedures;

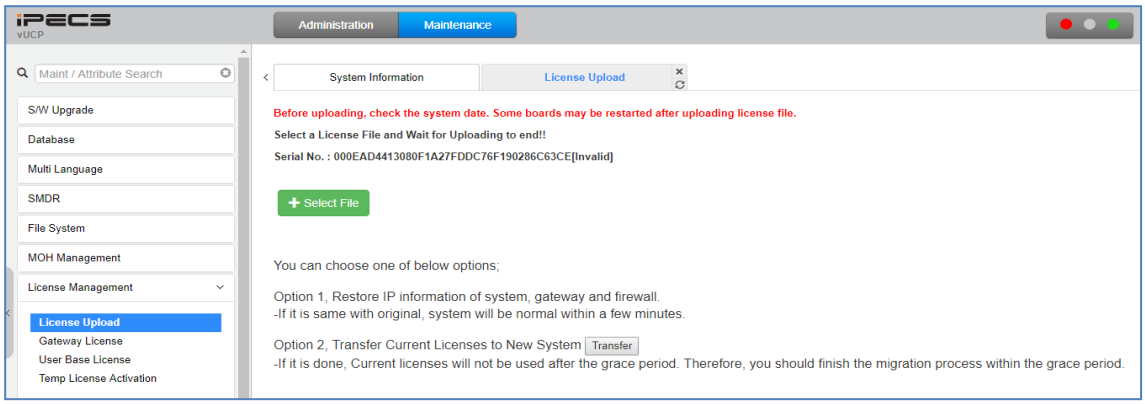
1) In system web admin, click the ‘transfer’ button to create a new Serial Number. If you do that, the system can run normally for 30-day grace period.
2) In license portal, transfer licenses from old Serial Number to new one and create a new license file. Use the same menu of H/W replacement at the license portal.
3) Upload the new license file to system.

Remember that after the start of transfer process by clicking ‘transfer’ button, it should be done within 30-daygrace period. Otherwise the system will go to the limited service mode and remain in that state until uploading a new license file.

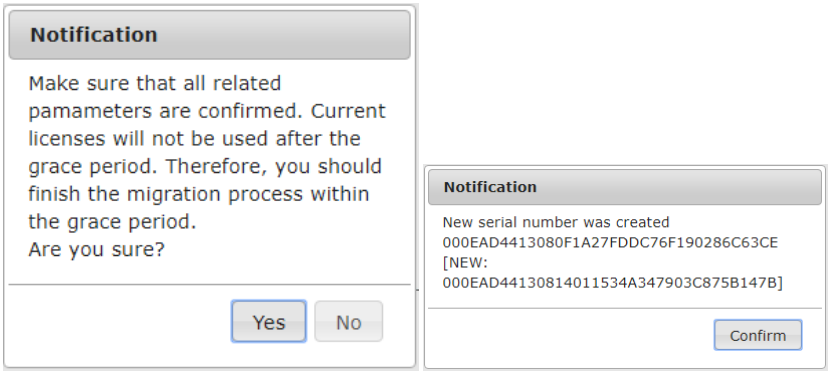
After the completion of license transition, you cannot use old licenses anymore, and they are blocked in license portal. Note that all running vUCP’s are monitored. Therefore, if you use the systems illegally, all systems with old and new serial number may be blocked, and it may result in legal sanctions.

System Web Admin

Firstly, transfer process starts in ‘Maintenance > License Management > License Upload’ of web admin. You canmakea new Serial Number by clicking ‘Transfer’ button. You can also see the current serial number is invalid.



After that, confirm below popup windows.



If you confirm the ‘transfer’ of licenses, the state will be changed to ‘After Transfer’, and the grace period will be started. You can use the system and licenses with old serial number for 30days. Within 30-day grace period, you should complete ‘Transfer’ process by uploading a new license as below. Otherwise the system will go to ‘Limited service mode’ again.

License Portal

To transfer license in license portal from old serial number to new created one, you canuse the same menu of H/W replacement at the license portal.

If you upload a new license file to system, you can use the system and licenses, which is transferred to new serial number.

5.2.3 Trial License

If you want to try vUCP system before the official use, you can use ‘vUCP trial license’. It provides all system features and application to maximum capacity for 90 days. It is applicable only before uploading an official license file. The followings shows the procedure to get the trial license.

The system goes to the limited mode if no valid commecial license after trial expiration. You can find the status of trial license in the system licese overview of web admin. The system send an expiring notice with attendant alarm and email, once before 30 days and daily from 7 days before expiration.

Process to get the tiral license

1) Distributor orders vUCP-CS2400S(SWL), vUCP-MNTD-TRIAL, vUCP-SPLD
2) Distributor generates license with target system S/W serial number
3) Distributor orders vUCP-MNT1 in License Detail page with “Maintenance” button
4) Distributor downloads license file.
5) Distributor sends generated license file (*.DAT) to : Minsoo Park minsoo.park@ericsson.com & Jinho Choi jinho.choi@ericsson.com
6) Updated license file with vUCP-TRIAL license (90-days) will be provided by email.

Migrate trial version to commercial version before expiration

1) Partners to send the trial license reset request (using “reset form” attached) to ELG license manager before expiration
2) ELG to reset the trial license.
3) Then, Partner can download the commercial licenses using the same serial number.
   - vUCP-CS2400S, vUCP-SPLD, vUCP-MNTD, vUCP-MNT1 + required systems licenses and application licenses in use (or to use).

5.3 vUCP Gateway licenses

There is no serial number for vUVM, vVOIM/vVOIMT, and vMCIM, and these are controlled by vUCP system. Therefore it is only necessary to download vVOIM/vVOIMT, vMCIM channel license or vUVM channel/storage licenses as required.

5.4 Differences from UCP

5.4.1 CPU

- UCP100/600/2400: ARM based
- vUCP: Intel based

5.4.2 Serial Number

- UCP100/600/2400: Already marked in factory.
- vUCP: Created by user after deployment.

5.4.3 No USB Support

There is no USB in vUCP because virtual machine is deployed.

5.4.4 VMware Tools(VMware only)

The VMware Tools are already installed in vUCP virtual machines. Therefore there is no need to install and update them.

5.4.5 Network Interface

- UCP100: 1 Ethernet
- UCP600/2400: 2 Ethernets
- vUCP: 1 Ethernet

5.4.6 Redundancy

The vUCP support only Geographical Redundancy.

5.4.7 Configuration of system network

UCP100/600/2400: system IP address, subnet mask, and route IP address can be changed in web admin

The vUCP: They are not editable in web admin and the change of them is possible in ESXi console or SSH shells. Because there may be a trouble suchas duplicated IP addresses after the initialization of system.

5.4.8 Manual DIP switches

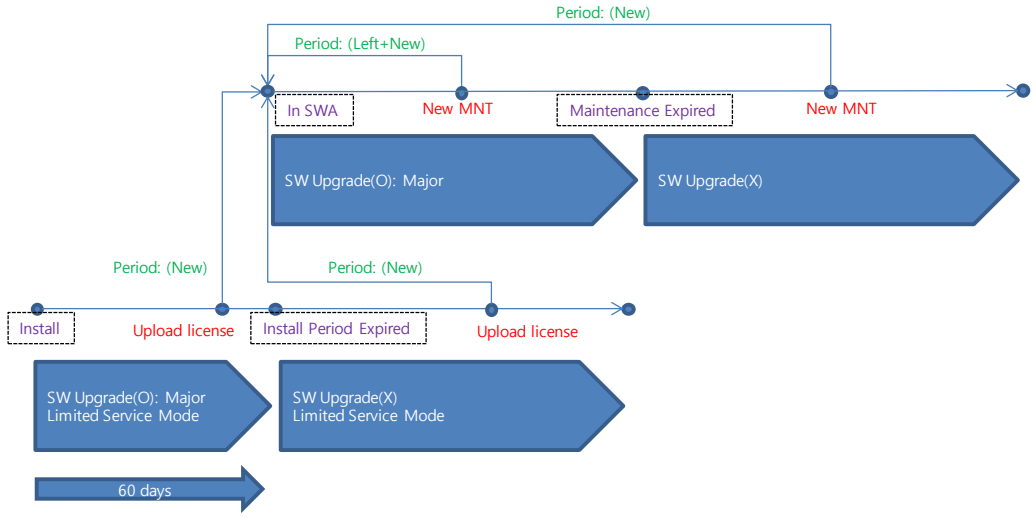
In vUCP, there are no manual switches which are Master/Salve and mode selection. But those related actions are possible through web admin. Refer to ‘Maintenance > Trace > Dip Switch Status’. If you need a redundancy function, you should set those in each vUCP.

5.4.9 Maintenance

The vUCP is treated as LME systemunlike existing UCP systems. Therefore, following policies are adopted:

During 60 days after Install:

- Limited Service Mode until uploading a license file. Only system attendant can make external outgoing call even in 'Limited Service Mode'
- Minor/Major Upgrade is available
- Device Registration after temp license activation.



6 Server Configuration

6.1 Access to Web and Install Wizard

6.1.1 vUCP

You can access the vUCP by web browser.

Default login values;

- User ID/Password: Admin/1234
- Method: HTTPS and port number 443

If the vUCP is in initial state due to the first creation or initialization, you should complete Install Wizard.

Note: The state of vUCP is ‘Limited service mode’ until uploading a new license file. In case of AWS, EIP should be set as firewall IP in PGM 102.

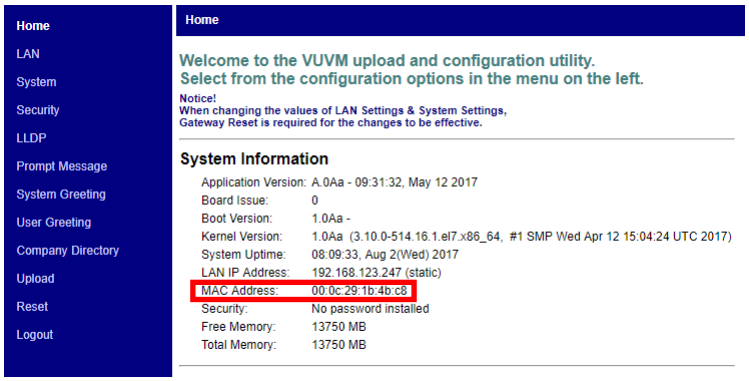
6.1.2 vUVM

You can access the vUVM by web browser, and change the system configuration.

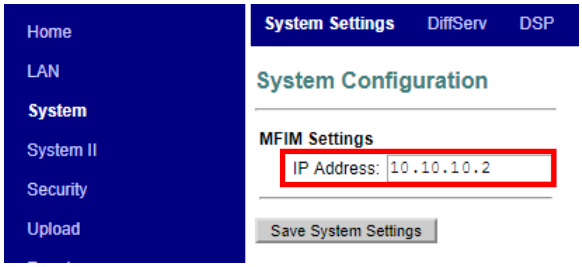
Default login values;

- User ID: No default user ID
- Password: No default password. You should change it in ‘Security’ page.
- Method: HTTP and port number 80.

You can find ‘MAC address which is used for registration



Also, you can modify the ‘Server Settings’ of System Configuration.



Note; vUVM should use “Local-Remote” instead of “Local” mode. In case of AWS, EIPshould be used as the firewall IP address in PGM132.

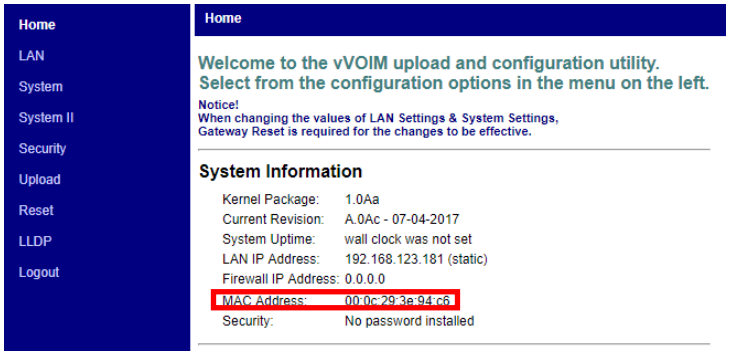
6.1.3 vVOIM/vVOIMT

You can access the vVOIM/vVOIMT by web browser, and change the system configuration.

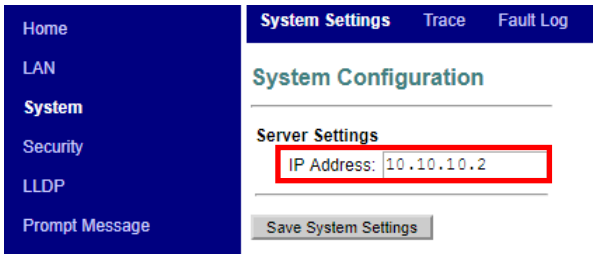
Default login values;

- User ID: No default user ID
- Password: No default password. You should change it in ‘Security’ page.
- Method: HTTP and port number 80.

You can find ‘MAC address which is used for registration



Also, you can modify the ‘Server Settings’ of System Configuration.



Note;

vVOIM/vVOIMT should use “Local-Remote” instead of “Local” mode.

In case of AWS, EIPshould be used as the firewall IP address and RTP Packet Relay Firewall IP Address in PGM132.

6.1.4 vMCIM

6.1.4.1 Configure Network Settings vMCIMv1

1) Check the datetime of host (UCP)

The datetime of vMCIM is set to sync with the vUCP and is used to get soft-DSP licenses.

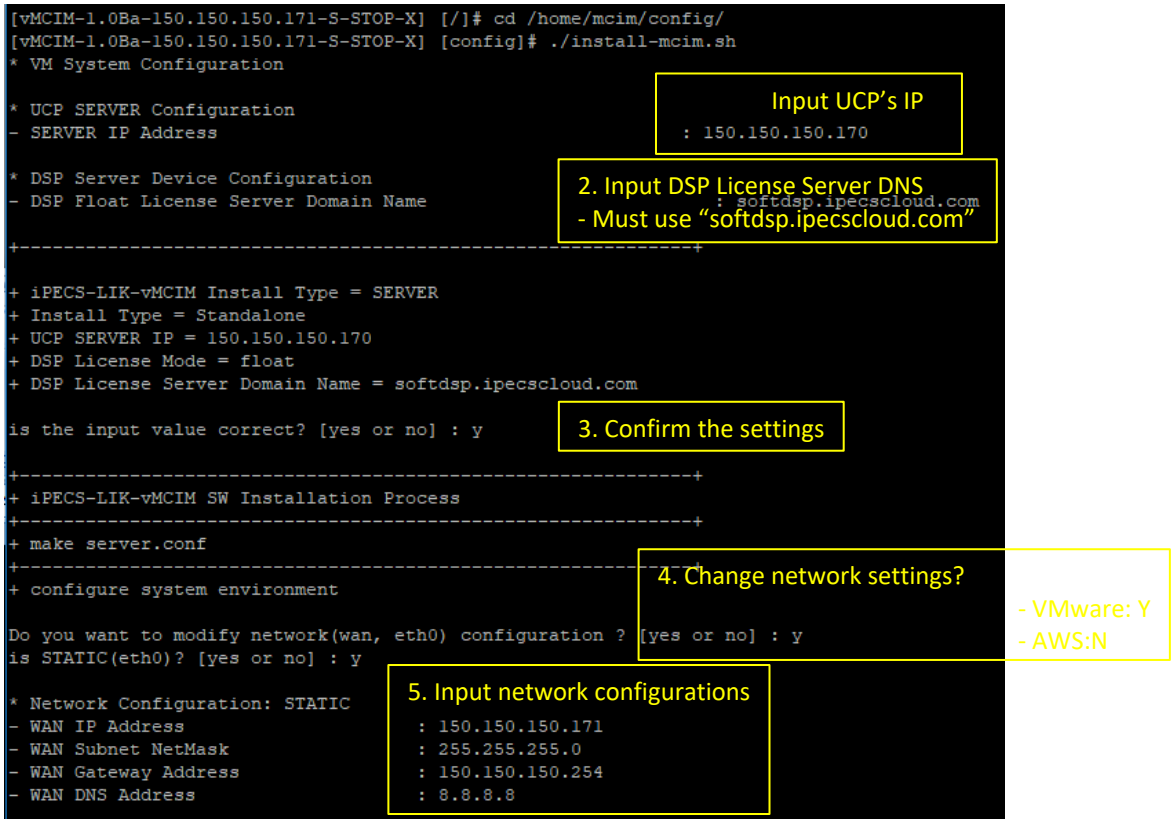
=>NTP Server Service field in PGM195 should be set to “Enable”. And the datetime of vUCP is also set to correctly because the license server checks the datetime based on the GMT time.

2) Access vMCIM by SSH (port number 60022)

- VMware: ID and password is required.
- AWS: ID is “centos” and key authentication is required.

3) Execute “install-mcim.sh’ file.

- VMware:
  # cd /home/mcim/Config
  # ./install-mcim.sh
- AWS: “sudo” should be added before the command.



4) Execute ‘restart.sh’ to restart.

- VMware:
  # cd /home/mcim
  # ./restart.sh
- AWS: “sudo” should be added before the command.

6.1.4.2 Configure Network Settings vMCIMv2

You can configure this by the same method as vVOIM.

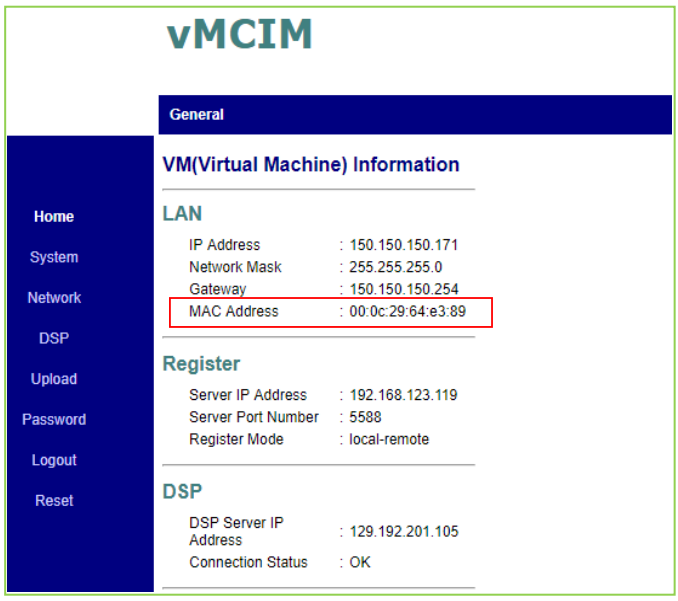
Web Access

You can access the vVCIM by web browser, and change the system configuration.

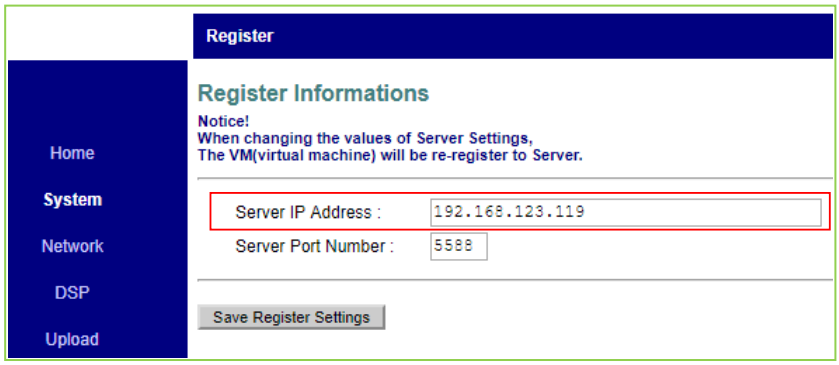
Default login values

- User ID: No default user ID
- Password: “ipkts”. you should change it in ‘Password’ page.
- Method: HTTP and port number 80.

You can find ‘MAC address which is used for registration



Also, you should modify the ‘Server IP Address’ of System Configuration.



Note;

vMCIM should use “Local-Remote” instead of “Local”.

6.2 Creating Serial Number

If it is the first time of vUCP virtual machine deployment, Serial Number will not be set. Therefore, you must create a new Serial Number for licensing. ***Before that, make sure again that all IP configurations are set correctly. Especially, in AWS, EIP should be used as the firewall IP.***

Refer to the chapter 2.4.3.1 for a Serial Number creation.

6.3 Ordering and Uploading a License File

After creating a Serial Number, you canorder and generatelicenses in License Portal, and upload a generated license file to the system in Web admin.

You canalso register devicesto vUCP by activating a Temp License, even if a license file is not uploaded. But because the state of vUCP is ‘Limited Service Mode’, only system attendant can make external outgoing call.

7 System Upgrade

The vUCP systems are initially provided as OVF file format. Therefore, you do better upgrade the system to the latestversion after deploying OVF file.This upgrade is done through the web admin maintenance page like the current UCP upgrade process.

7.1 Requirement

You must check if the software maintenance state is upgradable in advance to upgrade vUCP system, but vUVM and vVOIM/vVOIMT can upgrade at any time such as other UCP gateways.

You can download the ROM files for upgradeat theGPS website.

https://partner.ericssonlg-enterprise.com.

7.2 Backup DB

It is better to create a DB file in web admin and save it to your desktop or laptop before system upgrade. You can use it to restore the system DB data.You can also use the‘Snapshot’ feature in vSphereto prepare unwanted conditions.

7.3 Web Upgrade

Refer to the UCP manual.It is same as UCP systems.

Thanks for purchasing iPECS system.

iPECS is an Ericsson-LG Brand