Preface

Purpose of This Manual

This manual describes procedure for using the features that are provided by FUJITSU Cloud Service K5 IaaS.

Tip

Service Portal provides a subset of the main features that are provided by K5. In order to use the full set of features please use REST API.

Recommend the following related manuals for reference:

- K5 Portal User Guide
- IaaS Features Handbook
- IaaS API User Guide
- IaaS API Reference

- Foundation Service
- Network
- Application Platform Service
- Management Administration
- Contract Management

Abbreviations

Table 1: Name of product described as follows

<table>
<thead>
<tr>
<th>Name of the Product</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUJITSU Cloud Service K5 IaaS</td>
<td>K5 IaaS</td>
</tr>
<tr>
<td>Microsoft® Windows Server® 2012 SE R2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Microsoft® Windows Server® 2008 SE R2</td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Microsoft® Windows Server® 2008 EE R2</td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux® 6.5 (for Intel64)</td>
<td>RHEL6.5</td>
</tr>
<tr>
<td>Community Enterprise Operating System 6.5</td>
<td>CentOS 6.5</td>
</tr>
<tr>
<td>Community Enterprise Operating System 7.2</td>
<td>CentOS 7.2</td>
</tr>
<tr>
<td>Red Hat Update Infrastructure</td>
<td>RHUI</td>
</tr>
<tr>
<td>Windows Server Update Services</td>
<td>WSUS</td>
</tr>
<tr>
<td>VMware® vSphere®</td>
<td>VMware vSphere</td>
</tr>
<tr>
<td>VMware® ESX®</td>
<td>ESX</td>
</tr>
<tr>
<td>VMware® ESXi™</td>
<td>ESXi</td>
</tr>
<tr>
<td>VMware® vCenter Server™</td>
<td>vCenter Server</td>
</tr>
<tr>
<td>VMware® vSphere® Client</td>
<td>vSphere Client</td>
</tr>
<tr>
<td>VMware Tools™</td>
<td>VMware Tools</td>
</tr>
</tbody>
</table>
Trademark

- Microsoft, Windows, Windows Server, and the names of other Microsoft products are either registered trademarks or trademarks of Microsoft Corporation of United States and/or other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- Xeon is a trademark of Intel Corporation of U.S. and/or other countries.
- Linux® is a registered trademark of Linus Torvalds of United States and other countries.
- Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. of U.S. and other countries where this registered.
- Ubuntu is a registered trademark of Canonical Ltd.
- OpenStack is a registered trademark of OpenStack, LLC of the United States.
- VMware and VMware products are registered trademarks of VMware Inc. of United States of America and/or other countries.
- SAP and SAP logo, SAP R/3, mySAP.com, mySAP Business Suite and other SAP products are registered trademarks of SAP AG of Germany and/or other countries.
- All other company names and product names are trademarks or registered trademarks of their respective owners.

It should be noted that trademark symbol (™ or ®) which is appended to the system names or product names of this document are omitted.

Export restrictions

Export/release of this document to third party may require necessary procedures in accordance with the regulations of resident country and/or US export control laws therefore all the necessary steps must be taken.

Notice

- Information in this document may be subject to change without prior notice.
- No part of the content of this document can be reproduced without written permission of Fujitsu Limited.
- Fujitsu assumes no responsibility for infringement of any patent rights or other rights of third parties arising from the use of information in this document.
# Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date updated on</th>
<th>Section</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>29th February, 2016</td>
<td><em>Creating a Network and Subnet</em> on page 27</td>
<td>Modified explanation</td>
</tr>
<tr>
<td>1.3</td>
<td>1st April, 2016</td>
<td>User Registration User creation Display of previous usage fee (fixed amount)</td>
<td>Associated with K5 portal display, Function transfer</td>
</tr>
<tr>
<td>1.4</td>
<td>19th May, 2016</td>
<td>Addition to Multi region usage procedure.</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>10th November, 2016</td>
<td><em>Certificate Authentication</em> on page 5</td>
<td>Article added</td>
</tr>
</tbody>
</table>
Contents

Part 1: Preface .................................................................................. 1

1.1 Points to Note ......................................................................... 2
1.1.1 Operation Environment ....................................................... 2
1.1.2 Cookies Settings Confirmation .............................................. 2
1.1.3 Certificate Authentication .................................................... 5

Part 2: Assigning a Role to User ....................................................... 6

2.1 Assign an Administrator Role as per Group Registration .......... 7
2.1.1 User Group Registration ....................................................... 7

2.2 Assigning a specific Role ......................................................... 9
2.2.1 Assign Roles for a Specific Project ......................................... 9

Part 3: Creating a Group ................................................................. 11

3.1 Creating a Group That Is Granted a Role for a Specific Project .. 12
3.1.1 Creating a Group for a Specific Project granted with the System Owner role ........ 12

3.2 Creating a Group That Is Granted a Role for Multiple Projects .. 15
3.2.1 Creating a Group for Multiple Projects granted with System Owner role ............. 15
3.2.2 Grant and Verify the Group Role ............................................ 17

Part 4: Utilization of Multi-region ................................................... 18

4.1 Start Region Utilization ........................................................... 19
4.1.1 Start Region Utilization ....................................................... 19
4.1.2 Connect to the Utilized Region .............................................. 21

Part 5: Creating a Virtual System .................................................... 24

5.1 Building a Virtual Network ..................................................... 25
5.1.1 Creating a Virtual Router .................................................... 25
5.1.2 Connecting a Virtual Router to an External Network .......... 26
5.1.3 Creating a Network and Subnet ............................................ 27
5.1.4 Connecting Virtual Router to Virtual Network .................... 30
5.1.5 Creating a Key Pair .......................................................... 31
5.1.6 Acquiring a Global IP Address ............................................. 33
5.1.7 Creating a Security Group .................................................. 35
5.1.8 Setting Rules for a Security Group ....................................... 36

5.2 Creating a Virtual Server ......................................................... 39
5.2.1 Creating a Virtual Server .................................................... 39
5.2.2 Assigning a Global IP to the Virtual Server ......................... 43

5.3 Creating a Load Balancer ......................................................... 45
5.3.1 Creating a Security Group for the Load Balancer ........................................ 45
5.3.2 Creating a Security Group Rule for the Load Balancer ............................... 46
5.3.3 Creating a Load Balancer ........................................................................... 48
5.3.4 Enabling the Health Check Function of the Load Balancer ....................... 51
5.3.5 Adding a Virtual Server to which the Workload is Distributed by the Load Balancer... 52

5.4 Using a Template ....................................................................................... 55
5.4.1 Creating a Stack and Displaying the Stack Details ..................................... 55
5.4.2 Editing a Stack ......................................................................................... 57
5.4.3 Deleting a Stack ....................................................................................... 58

Part 6: Operating a Virtual System ................................................................. 60
6.1 Connecting to a Virtual Server ................................................................. 61
  6.1.1 Logging in to the Virtual Server via SSH .................................................... 61
6.2 Deleting a Virtual Server ........................................................................... 62
  6.2.1 Deleting a Virtual Server ........................................................................... 62
6.3 Monitoring Service Basics ........................................................................ 65
  6.3.1 Creating an Alarm and Displaying the Details ........................................ 65
  6.3.2 Displaying Monitored Items and Statistics of the Sample Data ................ 67
  6.3.3 Creating a Schedule ................................................................................ 69
  6.3.4 Deleting a Schedule ................................................................................ 71

Part 7: Using the Management Functions ...................................................... 73
7.1 Displaying Usage Fee .............................................................................. 74
  7.1.1 Displaying an Interim Usage Fee ............................................................... 74
Part 1: Preface

Topics:

• Points to Note
1.1 Points to Note

1.1.1 Operation Environment

This section describes the operation environment of Service Portal. Service Portal works on the following operating systems and browsers.

Table 2: Operating Environment

<table>
<thead>
<tr>
<th>Type</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system (OS)</td>
<td>• Windows 7/8/8.1</td>
</tr>
<tr>
<td>Browser</td>
<td>• Microsoft Internet Explorer 11</td>
</tr>
</tbody>
</table>

1.1.2 Cookies Settings Confirmation

In order to use the Service Portal, you need to enable your browser’s cookies.

Procedure

1. From the [Tools] button of Internet Explorer, click on [Internet Options] menu.

2. Click on [Privacy] button, check the internet Zone setting if its on [medium] or not. In case it is not, then please set it on [Medium].

Cookies are now enabled.

Tip: If you are unable to set the level of the Internet zone to “Medium,” Please apply the following below individual site setting.
3. Click the [Site] button.

4. Enter the address of Service Portal in the "Website box Address" and click the [Allow] button.

5. Click the [OK] button.
6. Click the [OK] button to close [Internet Options].

As per above, cookies enabling procedure is complete for each individual site.
1.1.3 Certificate Authentication

When you use K5 services that include Service Portal, you can add client certificate-based authentication. By using a client certificate in addition to ID/password authentication, you can increase the security level for the use of K5 services.

For more about certificate authentication functions, refer to the chapter on authentication information management in K5 Portal User Guide.
Part 2: Assigning a Role to User

Topics:

• Assign an Administrator Role as per Group Registration
• Assigning a specific Role
2.1 Assign an Administrator Role as per Group Registration

2.1.1 User Group Registration

Assign a role to the created user based on the group to be registered.

Before you begin
Login as a registered user on K5 portal.

About this task
Group registration can be done by the user having full administrator rights registered on K5 portal.

Procedure
1. From the left side menu, click [User Management] > [Group]. The [Group] list screen will be displayed.

3. At Group User change screen, under the column [All Users], select the registered user and click on the [Add] button.
4. Confirm if the selected user has been moved to [Group User] column and then click the [Save] button.
2.2 Assigning a specific Role

2.2.1 Assign Roles for a Specific Project

Granting a role for a specific project is also possible.

**Before you begin**

On K5 Portal, log in as a registered user.

**About this task**

This section describes the procedure to grant the [Operator role], the [System Owner role], or the [Observer role] and creating a user for a specific project.

In this section, the following three users are created as examples:

- User A
- User B
- User C

**Procedure**

1. On the [User] screen, click on [Action] menu provided for each created users, and then click on [Change Role] button.

2. From the [Change User Role] screen, click on [Project] Tab.

3. Set the role for each user as shown below, and then click the [Change] button.
4. Check the settings on the confirmation screen and click the [OK] button.
Part 3: Creating a Group

Topics:

- Creating a Group That Is Granted a Role for a Specific Project
- Creating a Group That Is Granted a Role for Multiple Projects
3.1 Creating a Group That Is Granted a Role for a Specific Project

3.1.1 Creating a Group for a Specific Project granted with the System Owner role

It is possible to create a new group and grant any role to that group for a specific project.

Before you begin

Log in as a user who was granted a role in User Group Registration on page 7.

About this task

This section explains the procedure of creating a new group and grant the System Owner role to the group for a specific project.

Procedure

1. From the left-side menu, click on [User Management] > [Group]. The [Group] list screen will be displayed.

2. Click the [Create Group] button on the [Group] screen.

3. On the [Create Group] screen, enter a name for the group and click the [Create] button on the upper right corner of the screen.

![Create Group Screen](image)

4. On the [Group] screen, click the [Action] menu of the created group, and then click [Change Role].
5. When the [Change Group Role] screen appears, assign the required roles, and then click the [Change] button on the upper right corner of the screen.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Target</td>
<td>Select a specific project</td>
</tr>
<tr>
<td>Role</td>
<td>From the [Preset] column, select the [System Owner Role] and add to the [Role to Assign] column.</td>
</tr>
</tbody>
</table>

6. From the screen of [Result of Group Role Change], check the contents and complete the procedure by clicking the [OK] button displayed on the top right corner.
### Result of Group Role Change

#### Global Operation

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Allocation Target Session</th>
<th>Control Type</th>
<th>Role Type</th>
<th>Success / Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

#### Regional Operation

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Allocation Target Session</th>
<th>Control Type</th>
<th>Role Type</th>
<th>Success / Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

---

Copyright 2015-2018 © FUJITSU LIMITED
3.2 Creating a Group That Is Granted a Role for Multiple Projects

3.2.1 Creating a Group for Multiple Projects granted with System Owner role

With one single group creation, you can set a group having specific role for multiple projects.

Before you begin

- Login as the user who was granted with role in User Group Registration on page 7.
- Use the project that was created in Creating a Group for a Specific Project granted with the System Owner role on page 12.

About this task

In the following procedure, additional project's role will be granted to the target project.

Procedure

1. From the left-side menu, click [User Management] > [Group]
   The [Group] list screen will be displayed.

2. On the Group screen, click on [Change Role] from the [Action] menu, and select the target group.

3. On the [Change Group Role] screen, assign the required roles, and then click on [Change] button.
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Target</td>
<td><strong>Tip</strong> Select a different project from the project which has already granted a role.</td>
</tr>
<tr>
<td>Role</td>
<td>From the [Project] column, select [System Owner Role] and add to the [Role to Assign] column.</td>
</tr>
</tbody>
</table>

4. From the [Result of Group Role Change] screen, check the contents, and click the [OK] button to complete the procedure.
3.2.2 Grant and Verify the Group Role

Even if the user is not granted with the role, if user belongs to that group then it is possible to perform the work granted to that group.

Before you begin

- Log in as the user who was granted a role in User Group Registration on page 7.
- Prepare the users who have only the Member role.
- Use the project that was created in the procedure described in Creating a Group for a Specific Project granted with the System Owner role on page 12.

About this task

This section describes the procedure of how to add the users who have only the Member role to a group.

Procedure

1. From the left-side menu, click [User Management] > [Group]. The [Group] list screen will be displayed.

2. From the [Group] screen, find the group which has specific role, and click on [Change Group User] from the [Action] menu of the group.

3. From the [Change Group User] screen, find users who have only the Member role from the [All Users] column, search, select and then click on [Add] button.

4. Confirm that the target users have been added to the [Group User] column, and then click [Save] button to complete the procedure.
Part 4: Utilization of Multi-region

Topics:

- *Start Region Utilization*
4.1 Start Region Utilization

4.1.1 Start Region Utilization

In case of using a different region other than the current region then, follow the "start usage procedure" of that region.

Before you begin

• Login as Contractor role User.
• There might be some regions which are not used yet out of multiple regions that exists.

About this task

Below steps explains "start usage procedure" of the region.

Procedure

1. Click on [Region Management] from left side menu.

2. From the [Manage Regions Used] screen, out of the regions which have [Not Used] status, in order to start the usage of those region, click on [Start Use] from the [Action] menu.
3. Once the screen is changed to [Manage Regions Used], check for [Preparing] status.

4. Refresh the screen after a while, check for the status as [In use] of the region which was previously [Preparing].
4.1.2 Connect to the Utilized Region

When the user starts the usage of the region in a Contractor role, that user and all the users of that domain can start the usage of that region.

Before you begin

Arrange the user and operate which belongs to domain with Contractor role created as mentioned in Start Region Utilization on page 19

About this task

When the "usage" of that region has been implemented, then login to that region is possible.

Procedure

1. Open the Login Page
2. Open the drop down menu, select the region which need to be used.

3. When you enter the [Contract number], [User name], [Password] and click on [Login] button, you can login to the desired region. If the header part is selected as region name, then please make sure that the selected region name is included in the URL.
KS IaaS Service has been launched.
Part 5: Creating a Virtual System

Topics:

- Building a Virtual Network
- Creating a Virtual Server
- Creating a Load Balancer
- Using a Template
5.1 Building a Virtual Network

5.1.1 Creating a Virtual Router

Create a virtual router to communicate with virtual resources that are created on the K5 IaaS system.

About this task
This section describes the procedure for creating a virtual router.

Procedure
1. From the left-hand menu, select [Network] > [Virtual Router], and then click on [Create Virtual Router] button.

2. From the [Create Virtual Router] screen, enter the settings items and click on [Create] button.
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AZ</td>
<td>Select the availability zone where the virtual router will be created</td>
</tr>
<tr>
<td>Virtual Router Name</td>
<td>Specify a name for the virtual router</td>
</tr>
</tbody>
</table>

3. The procedure is complete when the created virtual router has been added on the [Virtual Router List] screen and the status is [Active].

5.1.2 Connecting a Virtual Router to an External Network

Configure the settings to enable the created virtual router to communicate with an external network (Internet).

About this task

This section explains the procedure to connect an external network to the virtual router that was created in Creating a Virtual Router on page 25.

Procedure

1. From the left-hand menu, click on [Network] > [Virtual Router]. The [Virtual Router List] screen will be displayed.


4. Click the [Setting] button in the upper right corner of the screen to complete the procedure.

5.1.3 Creating a Network and Subnet

Create a virtual network and subnet in order to deploy the Virtual servers etc.

About this task

This section describes the procedure for creating a virtual network and configuring settings of private IP addresses range as its subnet.

Procedure

1. From the left-hand menu, click on [Network] > [Virtual Network].

   ![Virtual Network List Screen]

   The [Virtual Network] list screen will be displayed

2. On the [Virtual Network] list screen, click the [Create Virtual Network] button.
3. On each tab of the [Create Virtual Network] screen, enter the settings items and click the [Create] button.

**Virtual Network** tab

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AZ</td>
<td>Select an availability zone for the creation destination</td>
</tr>
<tr>
<td></td>
<td>Tip: Select the availability zone that was selected in Creating a Virtual Router on page 25.</td>
</tr>
<tr>
<td>Virtual Network Name</td>
<td>Specify any virtual network name</td>
</tr>
<tr>
<td>Management State</td>
<td>Select [UP]</td>
</tr>
</tbody>
</table>

**[Subnet] tab**
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Subnet</td>
<td>Select [Yes]</td>
</tr>
<tr>
<td>Subnet Name</td>
<td>Specify any subnet name</td>
</tr>
<tr>
<td>Virtual Network Address</td>
<td>Specify the network address which is used for virtual server in the CIDR notation</td>
</tr>
<tr>
<td></td>
<td>Example: 192.168.123.0/24</td>
</tr>
<tr>
<td></td>
<td>Tip</td>
</tr>
<tr>
<td>Gateway</td>
<td>Select [Yes]</td>
</tr>
<tr>
<td>Gateway IP</td>
<td>Specify in accordance with the virtual network address</td>
</tr>
</tbody>
</table>

**Subnet Details tab**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>IP address allocation pool</td>
<td></td>
</tr>
<tr>
<td>DHC Server</td>
<td></td>
</tr>
<tr>
<td>Add Route Setting</td>
<td></td>
</tr>
<tr>
<td>Item Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DHCP</td>
<td>Select [Enabled]</td>
</tr>
<tr>
<td>IP address allocation pool</td>
<td>Do not set</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Select the DNS server of Availability Zone for the creation Destination Ex: Such as for 'uk-1a', set 62.60.39.9 and 62.60.39.10</td>
</tr>
<tr>
<td>Add Route Settings</td>
<td>Do not set</td>
</tr>
</tbody>
</table>

4. The procedure is complete once the row of created virtual network has been added on the [Virtual Network] screen.

5.1.4 Connecting Virtual Router to Virtual Network

Configure the settings to enable an external network (Internet) to communicate with the virtual network via a virtual router.

About this task

This section describes the procedure of connecting a virtual network created in Creating a Network and Subnet on page 27 to the virtual router that is used in Connecting a Virtual Router to an External Network on page 26.

Procedure

1. From the left-hand menu, click [Network] > [Virtual Router]. The [Virtual Router] list screen will be displayed.
2. On the [Virtual Router] list screen, click the name of the target virtual router.
3. On the [Virtual Router Details] screen, click the [Add Interface] button.
4. From the [Interface Setting] screen, enter the following settings items, and then click the [Setting] button.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet</td>
<td>Select the subnet which is connected to the virtual router</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specify the gateway IP address of the above subnet</td>
</tr>
</tbody>
</table>

5. The procedure is complete once the set interface has been added on the [Virtual Router Details] screen.

5.1.5 Creating a Key Pair

Create a key pair to be used while logging into Linux Virtual Server.

**About this task**

This section describes the procedure of creating a key pair that is used for SSH logins and downloading of the created key file.

**Procedure**

1. From the left-hand menu, click on [Compute] > [Access and Security].
The [Access and Security] screen will be displayed.


3. Click the [Create Key Pair] button.

4. From the [Create Key Pair] screen, enter the following items and then click the [Create] button.
### Item Name | Description
--- | ---
Key Pair Name | Specify any key pair name
AZ | Select the availability zone in which the key pair will be created

5. When the Key file has been downloaded, the save confirmation will be displayed. Save to any local folder as .pem file.

Note

In case if the download of the key file fails, it cannot be retrieved again. Please create a new key pair.

### 5.1.6 Acquiring a Global IP Address

Acquire a global IP address in order to connect to the virtual server via the Internet.

#### About this task

This section describes the procedure of acquiring a global IP address from the IP address pool which is provided by the system.
Procedure

1. From the left-hand menu, click [Compute] > [Access and Security]. The [Access and Security] screen will be displayed.


3. Click on the [Allocate Global IP] button.

   Tip
   Select the pool which is applicable to the external network which was connected in Connecting a Virtual Router to an External Network on page 26.

4. From the [Allocate Global IP] screen, select the pool and click on the [Allocate] button.

   The procedure is complete when the new IP address has been added to the global IP list given on the [Global IP] tab.
5.1.7 Creating a Security Group

Create a security group to limit the unnecessary communication from the Internet and allow only necessary communication.

About this task

This section describes the procedure of creating a security group for SSH connections.

Procedure

1. From the left-hand menu, click on [Compute] > [Access and Security].
   The [Access and Security] screen will be displayed.


3. On the [Create Security Group] screen, enter the following settings items and then click on the [Create] button.
### 5.1.8 Setting Rules for a Security Group

**About this task**

At the time of security group creation, security default rules are set automatically. Set rules in order to make necessary communication.

This section describes the procedure of creating a rule used for SSH connections.

**Procedure**

1. From the left-hand menu, click on [Compute] > [Access and Security]. The [Access and Security] screen will be displayed.


---

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Group Name</td>
<td>Specify any security group name</td>
</tr>
<tr>
<td>Description</td>
<td>Specify a description for the security group which is to be created.</td>
</tr>
</tbody>
</table>

4. On the [Add Rule] screen, enter the following additional items of the receiver rules and then click the [Add] button.
### Item Name | Description
--- | ---
Rule | Select [Custom TCP Rule]
Direction | Select [Reception]
Open Port | Select [Port]
Port | Specify "22"
Connected Virtual Server | Select [CIDR]
CIDR | Specify the IP address of the client PC for communication.

5. Also enter the following additional items of the sender rules and add them by repeating step 3 though step 4.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>Select [Custom TCP Rule]</td>
</tr>
<tr>
<td>Direction</td>
<td>Select [Send]</td>
</tr>
<tr>
<td>Open Port</td>
<td>Select [Port]</td>
</tr>
<tr>
<td>Port</td>
<td>Specify &quot;22&quot;</td>
</tr>
<tr>
<td>Connected to</td>
<td>Select [CIDR]</td>
</tr>
<tr>
<td>CIDR</td>
<td>Specify the IP address of the client PC for communication.</td>
</tr>
</tbody>
</table>

The procedure is complete once the created rules have been added to the [Manage Security Group Rules] screen.
5.2 Creating a Virtual Server

5.2.1 Creating a Virtual Server

Create a virtual server.

About this task

This section explains the procedure of creating a new virtual server using a CentOS image.

Procedure

1. From the left-hand menu, click [Compute] > [Virtual Server].

The [Virtual Server] list screen will be displayed.

2. From the [Virtual Server] list screen, click the [Create Virtual Server] button.

3. From [Creating virtual server] screen, enter the following setting item on each tab [Details] tab
### Item Name | Description
--- | ---
AZ | Specify the availability zone to deploy virtual server
Virtual Server Name | Specify any virtual server name
Virtual Server Type | Select a virtual server type according to the performance requirement
Boot Source of the Virtual Server | Select [Boot from image (create new storage)]
Image | Select [CentOS 6.5 64bit(English) xx]
**Tip**
xx is a two-digit number.
Device Size (GB) | Specify "30."
Device Name | Specify "a."

[Access and Security] tab
### Item Name | Description
--- | ---
**Key Pair** | Select the key pair name that was created in *Creating a Key Pair* on page 31
**Security Group** | Check the security group name that was created in *Creating a Security Group* on page 35

---

**Tip**
Clear the [default] check box.

---

**[Network] tab**
Select the virtual network that was created in *Creating a Network and Subnet* on page 27 from the [Available Virtual Network] column, and then click the [Add] button.

---

**[Post Creation] tab**
Tip
Leave the Windows Administrator password as blank.

[Advanced setting] tab

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Partition</td>
<td>Select [Automatic]</td>
</tr>
</tbody>
</table>

4. Once information entering is completed in each tab, click on the [Create] button.

5. The procedure is complete once the created server has been added to the [Virtual Server] list screen.

Tip
The status is [BUILD] immediately after creation. Refresh the screen after a brief period of time. If the status is [ACTIVE], starting of the virtual server is complete.
5.2.2 Assigning a Global IP to the Virtual Server

Assign a global IP address to a running virtual server in order to connect to the internet.

About this task

This section describes the procedure of assigning a global IP address to the virtual server which was created in Creating a Virtual Server on page 39.

Procedure

1. From the left-hand menu, click [Compute] > [Virtual Server]. The [Virtual Server] list screen will be displayed.

2. Click on [Global IP Allocation] from the [Action] menu of the virtual server, to which you want to assign the global IP address.

3. From the [IP Address] tab of the [Global IP allocation management] screen, set the following items and then click the [Global IP Allocation] button.
Item Name | Description
---|---
Global IP Address | Select the IP address which was acquired in Acquiring a Global IP Address on page 33
Global IP allocation port | Do not change the default selection

4. Procedure is completed once, the global IP address is added to the [Virtual Server] list screen, in the [IP address] column of the Virtual server row to which the IP address was assigned.
5.3 Creating a Load Balancer

5.3.1 Creating a Security Group for the Load Balancer

Create a security group in order to protect the load balancer from an unauthorised communication which can be accessed from the Internet.

About this task

While creating the load balancer, create the security group beforehand. The creation procedure is as shown below.

Procedure

1. From the left-hand menu, click in the order of [Compute] > [Access and Security].

The [Access and Security] screen will be displayed.


3. On the [Create a Security Group] screen, enter the following settings items and then click the [Create] button.
5.3.2 Creating a Security Group Rule for the Load Balancer

Create a rule, for the security group which was created for the load balancer.

About this task

Create a rule that allows the following type of communication for the security group which was created in Creating a Security Group for the Load Balancer on page 45:

- HTTP

Procedure

1. From the left-hand menu, click [Compute] > [Access and Security]. The [Access and Security] screen will be displayed.
4. On the [Add Rule] screen, enter the following settings and then click the [Add] button.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>Select [Custom TCP Rule]</td>
</tr>
<tr>
<td>Direction</td>
<td>Select [Reception]</td>
</tr>
<tr>
<td>Open Port</td>
<td>Select [Port]</td>
</tr>
<tr>
<td>Port</td>
<td>Specify &quot;80&quot;</td>
</tr>
<tr>
<td>Connected to</td>
<td>Select [CIDR]</td>
</tr>
<tr>
<td>CIDR</td>
<td>xxx.xxx.xxx.0/24</td>
</tr>
</tbody>
</table>

**Tip**
Limit the allowed range (source address) as per requirement

The procedure is complete once the configured settings have been added to the [Security Group Rules] Administration screen.

### 5.3.3 Creating a Load Balancer

Deploy load balancer in order to handle by using auto scale, in the case of excessive Access or to increase the availability usage in Availability Zone.

**About this task**
This section describes the procedure to create a load balancer and deploy it for use with the virtual servers that were created in Creating a Virtual Server on page 39. In this example, the protocol for distribution is HTTP.
Procedure

1. From the left-hand menu, click [Network] > [Load Balancer].

The [List of Load Balancer] screen will be displayed.

2. Click the [Create Load Balancer] button on the [List of Load Balancer] screen.

3. On each tab of the [Create Load Balancer] screen, set the following items.

   **[Load Balancer Settings] tab**

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancer Name</td>
<td>Specify a load balancer name</td>
</tr>
<tr>
<td>Type</td>
<td>Select [Public]</td>
</tr>
</tbody>
</table>

   **Note** When the [Public] type creation is completed, it can be referred on the internet.
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade</td>
<td>Select [Standard]</td>
</tr>
</tbody>
</table>

Table 3: [Listener] Section

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancer Protocol</td>
<td>Select [HTTP]</td>
</tr>
<tr>
<td>Load Balancer Port</td>
<td>Specify &quot;80&quot;</td>
</tr>
<tr>
<td>Virtual Server Protocol</td>
<td>Select [HTTP]</td>
</tr>
<tr>
<td>Virtual Server Port</td>
<td>Specify &quot;80&quot;</td>
</tr>
<tr>
<td>Certificate</td>
<td>Do not set</td>
</tr>
</tbody>
</table>

[Subnet Settings] tab
Select the subnet in order to deploy the load balancer from the [Subnet] column, and then click the [Add] button.

[Security Group Settings] tab
Select the security group which was created in *Creating a Security Group for the Load Balancer* on page 45 from the [Security Group] column, and then click the [Add] button.
4. When entering the information is completed in each tab, click the [Create] button. The procedure is complete once when the created load balancer has been added on the [List of Load Balancer] screen.

5.3.4 Enabling the Health Check Function of the Load Balancer

Health check can be carried out for the virtual servers in which the load is distributed by the load balancer.

About this task

This section describes the procedure for enabling the health check function for the load balancer that was created in Creating a Load Balancer on page 48.

Procedure

1. From the left-hand menu, click [Network] > [Load Balancer]. The [List of Load Balancer] screen will be displayed.


3. Set the following items on the [Health Check Information Setting] screen, and then click the [Setting] button.
### 5.3.5 Adding a Virtual Server to which the Workload is Distributed by the Load Balancer

After you have finished configuring the settings of the security group, the distribution protocol, and the health check function for the load balancer, add the virtual servers which require workload distribution.

**Before you begin**

Create two or more virtual servers by following the steps in *Creating a Virtual Server* on page 39.

**About this task**

This section describes the procedure for adding multiple virtual servers to a single load balancer. It also describes the procedure for configuring the settings related to session maintenance.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold of health check Successes to be Considered as Healthy</td>
<td>Specify <em>2</em></td>
</tr>
<tr>
<td>Health Check Execution Interval (s)</td>
<td>Specify <em>10</em></td>
</tr>
<tr>
<td>Protocol</td>
<td>Select [HTTP]</td>
</tr>
<tr>
<td>Port</td>
<td>Specify <em>80</em></td>
</tr>
<tr>
<td>URL</td>
<td>Specify the URL of the landing page of Apache that is installed in the virtual server</td>
</tr>
<tr>
<td>Health Check Timeout Period (s)</td>
<td>Specify <em>3</em></td>
</tr>
<tr>
<td>Threshold of Health check Fails to be Considered Unhealthy</td>
<td>Specify <em>2</em></td>
</tr>
</tbody>
</table>

4. Click the appropriate load balancer name on the [List of Load Balancer] screen.

5. The procedure is complete once the configured settings are displayed on the [Health Check Information] tab of the [Load Balancer Details] screen.
Procedure

1. From the left-hand menu, click [Network] > [Load Balancer]. The [List of Load Balancer] screen appears.


3. On the [Add Virtual Server] screen, select and check mark all the virtual servers which require workload distribution, and then click the [Add] button.


5. Set the following items on the [Create Session Maintenance Policy] screen, and then click the [Create] button.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Specify a policy name</td>
</tr>
<tr>
<td>Item Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Maximum Session Persistence Time (s)</td>
<td>Specify &quot;300&quot;</td>
</tr>
</tbody>
</table>

6. Click the appropriate load balancer name on the [List of Load Balancer] list screen.

7. The procedure is complete once the configured settings are displayed on the [Virtual Server Information] tab and on the [Policy Information] tab which are located on the [Load Balancer Details] screen.
5.4 Using a Template

5.4.1 Creating a Stack and Displaying the Stack Details

You can deploy virtual resources in bulk by using a template in the YAML format. The set of virtual resources that are deployed using the template can be managed as a stack.

About this task

This section describes the procedure for deploying virtual resources in bulk by using a template (text file) in the YAML format.

Procedure

1. From the left-hand menu, click [Compute] > [Stack].

The [Stack] list screen will be displayed

2. On the [Stack] list screen, click the [Create Stack] button.

3. On the [Create Stack] screen, enter the following settings items.
### Description

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Name</td>
<td>Specify any stack name</td>
</tr>
<tr>
<td>How to specify a template</td>
<td>Select [File]</td>
</tr>
<tr>
<td>File</td>
<td>Specify the template file that has been created</td>
</tr>
<tr>
<td>Parameters to be passed to the template</td>
<td>Specify the required parameter names and values according to the contents of the template file to be used</td>
</tr>
<tr>
<td>Timeout (minutes)</td>
<td>Specify &quot;10&quot;</td>
</tr>
<tr>
<td>Rollback</td>
<td>Select [False] to delete the resources for which deployment has failed, in cases when the timeout period elapses and deployment still cannot be carried out</td>
</tr>
<tr>
<td>Tip</td>
<td>[True] disables the rollback.</td>
</tr>
</tbody>
</table>

The procedure is complete when the created stack is displayed on the [Stack] list screen.

4. Click the stack name on the same row as the created stack.
The details screen of the corresponding stack will be displayed.

5.4.2 Editing a Stack

You can edit the deployed stack by using a YAML template whose configuration has been changed.

About this task

This section describes the procedure for editing the deployed stack by using a YAML template file whose configuration has been changed.

Procedure

1. From the left-hand menu, click [Compute] > [Stack]. The [Stack] list screen will be displayed.


3. Change the following items on the [Edit Stack] screen and then click the [Update] button.
### How to Specify Template

**Select [File]**

**File**

Click the reference button of the [File] column and specify the template file that has been created.

**Parameters to be passed to Template**

Specify the required parameter items and values according to the contents of the template file to be used.

**Timeout (minutes)**

Specify '15'

---

**5.4.3 Deleting a Stack**

Delete a deployed stack that is no longer required.

**About this task**

This section describes the procedure for deleting a stack.

**Procedure**

1. From the left-hand menu, click [Compute] > [Stack].
   The [Stack] list screen will be displayed.

3. When the [Delete Stack] window appears, click the [Delete] button.

The procedure is complete once the corresponding operated stack has been deleted from the [Stack] list screen.

Tip

It takes some time to complete the deletion. (During the deletion, [DELETE_IN_PROGRESS] is displayed.)
Part 6: Operating a Virtual System

Topics:

• Connecting to a Virtual Server
• Deleting a Virtual Server
• Monitoring Service Basics
6.1 Connecting to a Virtual Server

6.1.1 Logging in to the Virtual Server via SSH

Login to the Virtual server, by connecting through internet with the Global IP address assigned to the virtual server.

**Before you begin**

Install an SSH client such as TeraTerm on the PC.

**About this task**

Connect via SSH to the global IP address that was assigned to the virtual server in Assigning a Global IP to the Virtual Server on page 43. This section describes the procedure of connecting to Linux Virtual Server.

**Procedure**

1. Connect to the global IP address to SSH, by using the SSH client.
2. Undergo the authentication process in order to login to the virtual server.
   - Authentication Using Key Pair
     When the authentication window appears, specify the ID that was entered in the [Post Creation] tab in Creating a Virtual Server on page 39 and the key file that was created in Creating a Key Pair on page 31.

**Results**

When the authentication information is correct, the prompt will be displayed.
6.2 Deleting a Virtual Server

6.2.1 Deleting a Virtual Server

Delete a deployed virtual server.

About this task

This section describes the procedure for deleting a virtual server.

Procedure

1. From the left-hand menu, click on [Compute] > [Virtual Server].

The [Virtual Server] list screen will be displayed.

2. On the [Virtual Server] list screen, click the name of the virtual server machine which needs deletion and [Virtual Server Details] screen will be displayed.
3. Click the [Back] button to return to the [Virtual Server] list screen.

4. Select the virtual server which needs to be deleted and use either of the following methods for deletion
   • On the [Virtual Server] list, use the check box on the left end of the list to select the target, and then click the [Delete] button
   • On the [Virtual Server] list, select [Delete] on the [Action] menu that is in the right end of the row for the target virtual server
5. When a confirmation message appears, click the [Delete] button.

**Results**

After the [Virtual Server] list screen appears, confirm that the deleted virtual server is not displayed on the list.

**Tip**

As per the processing status, the virtual server is will left behind. In that case, after waiting for a while, please refresh by clicking the [Refresh] button.
6.3 Monitoring Service Basics

6.3.1 Creating an Alarm and Displaying the Details

You can create an alarm that contains the settings such as a threshold, for a specific monitored item, and an "action" when the threshold is reached.

About this task

This section describes the procedure to create an alarm for a monitored item, for example, the CPU utilization of a virtual server.

Procedure

1. From the left-hand menu, click [Monitoring] > [Alarm]. The [Alarm List] screen will be displayed.

2. Click the [Create Alarm] button on the [Alarm List] screen.

3. On each tab of the [Create Alarm] screen, enter the settings and click the [Create] button.

   [Alarm Information] tab
Click the [Setting] button for the [Monitoring Item] column, and select the CPU utilization rate, "fcx.compute.cpu_util", of the virtual server which needs to be monitored.

[Time Constraints] tab

[Action] tab
Creation is complete when the created alarm appears in the [Alarm List] screen.

4. To check the details of the created alarm, click the link of the alarm name on the [Alarm List] screen.

5. When the [Alarm Detail] screen appears, and you can check the details of the alarm.

### 6.3.2 Displaying Monitored Items and Statistics of the Sample Data

You can check and display the items of the virtual resources that are provided by standard system.

**About this task**
This section describes the procedure to use the following display functions related to item to be monitored.
• Displaying the monitored item list
• Filtering the monitored items
• Displaying statistics related to the monitored items

Procedure

1. From the left-hand menu, click [Monitoring] > [Monitoring]. The [Monitoring Item] list screen appears.

2. In order to narrow down the list of monitored items, enter a string in the input column, and click the [Filter] button. Monitored Item name will display the narrowed down monitoring items which includes the entered string.

3. On the monitored item list, click the name of the monitored item, in order to check the required statistics.
The sample statistics of the monitoring items which were clicked, these can be checked by the graphical change displayed on the screen.

6.3.3 Creating a Schedule

Create a schedule to send a signal (apply the scaling policy) to a stack at the specified time.

Before you begin
You need to create a stack that includes auto-scaling settings in advance.

About this task
This section describes the procedure to create a schedule for the stack that was created in Creating a Stack and Displaying the Stack Details on page 55.

Procedure

1. From the left-hand menu, click [Compute] > [Schedule].
The [List Schedule] screen appears.

2. Click the [Create Schedule] button on the [List Schedule] list screen.

3. On the [Create Schedule] screen, set the following items, and then click the [Create] button.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Name</td>
<td>Specify a schedule name</td>
</tr>
<tr>
<td></td>
<td><img src="Note" alt="Note" /> The schedule name must be unique to the domain.</td>
</tr>
<tr>
<td>Stack</td>
<td>Select the target stack</td>
</tr>
<tr>
<td>Resource</td>
<td>Select the target to apply this schedule</td>
</tr>
<tr>
<td>Time to Execution</td>
<td>Specify the time in the format of &quot;Minute Hour DOM Month DOW&quot; (with the fields separated by single-byte spaces)</td>
</tr>
<tr>
<td></td>
<td><img src="Example" alt="Example" /> Example: 00 02 * * *</td>
</tr>
</tbody>
</table>
Table 4: Format of the [Time to Execution] Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Values That Can Be Specified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minute</td>
<td>From 0 to 59, * specifies every minute</td>
</tr>
<tr>
<td>Hour</td>
<td>From 0 to 23, * specifies every hour</td>
</tr>
<tr>
<td>DOM</td>
<td>From 1 to 31, * specifies every day</td>
</tr>
<tr>
<td>Month</td>
<td>From 1 to 12, or from jan to dec, * specifies every month</td>
</tr>
<tr>
<td>DOW</td>
<td>From 0 to 7 (0 and 7 specifies Sunday), or from sun to sat, * specifies all days</td>
</tr>
</tbody>
</table>

The procedure is complete once the created schedule appears on the [List Schedule] list screen.

### 6.3.4 Deleting a Schedule

Delete a schedule that is no longer needed.

**About this task**

This section describes the procedure to delete a created schedule.

**Procedure**

1. From the left-hand menu, click [Compute] > [Schedule].

   ![Image of the List Schedule screen]

   The [List Schedule] list screen appears.

2. Click [Delete] on the [Action] menu for the schedule to be deleted.
3. Once the confirmation message appears, Click the [Delete] button.

The procedure is complete when the deleted schedule no longer appears on the [List Schedule] list screen.
Part 7: Using the Management Functions

Topics:
• Displaying Usage Fee
7.1 Displaying Usage Fee

7.1.1 Displaying an Interim Usage Fee

Display the usage fees of amount which is not fixed, such as fees for the current month.

About this task

You can check the following information on the screen that displays the interim usage fees:

- Total amount that was used for all projects within the contract number
- Total amount for each project and its usage details

Procedure

From the left-hand menu, click [Usage Fee] to display the [Usage Details(Interim)] screen.