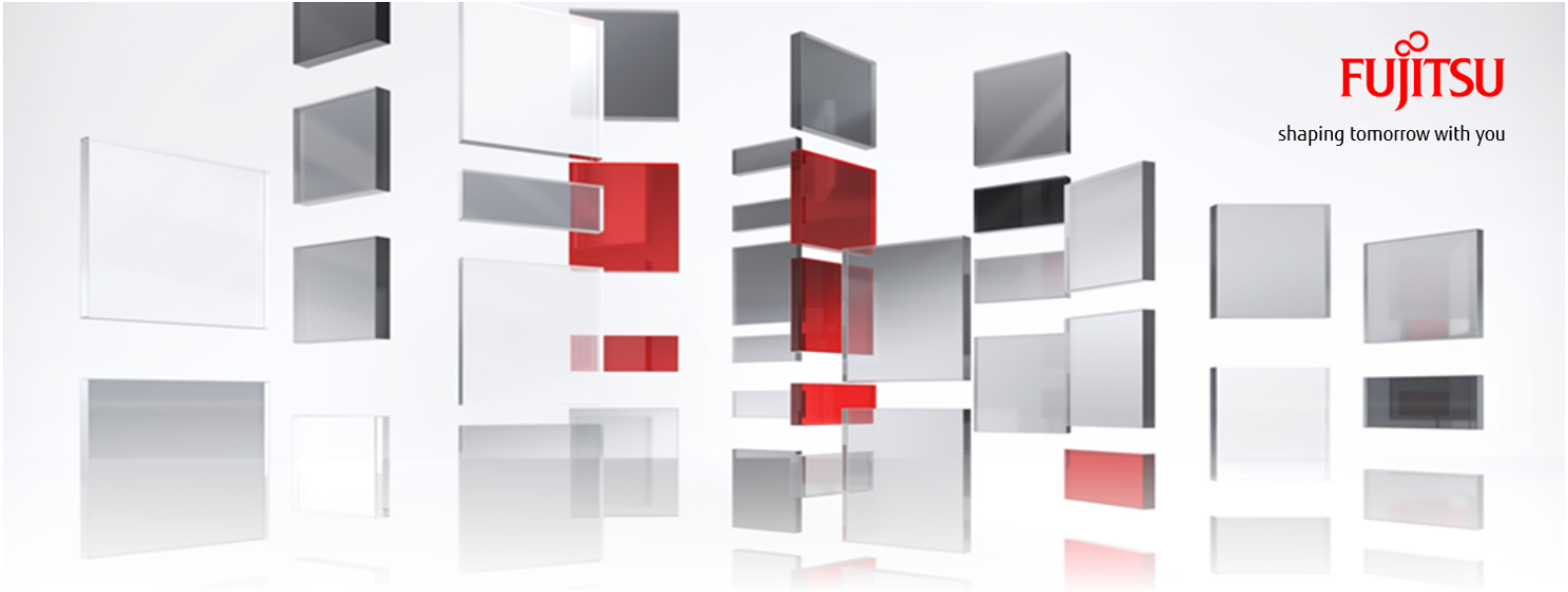


FUJITSU
shaping tomorrow with you

FUJITSU Cloud Service K5 IaaS

Features Handbook

Version 1.9
FUJITSU LIMITED

K5IA-DC-M-004-001E

Preface

Purpose of This Manual

This document explains the functions and services provided by FUJITSU Cloud Service K5 IaaS (K5 IaaS). Use this document in the following cases when developing your applications or services by using K5 IaaS:

- When considering using the services and functions of K5 IaaS (and combinations thereof) that can be used to develop your applications and services that are intended for users
- When considering the scope of system development, the services and functions provided, and the scope of the required design to establish the applications that are intended for users

Audience for This Manual

This manual is intended for those involved in the planning and developing of applications or services using K5 IaaS. To read this manual, you need to possess the following knowledge:

- Basic knowledge of virtualization technology (hypervisors, virtual servers, virtual storage, virtual networks)
- Basic knowledge of OpenStack
- Basic knowledge of your OS
- Basic knowledge of the Internet and Intranet
- Basic security knowledge
- Basic knowledge of system operation, including backups, monitoring, and redundancy

Organization of Manuals

Refer to the related manuals listed below according to your purposes and methods of use.

Manual Title	Purposes and Methods of Use
IaaS Features Handbook (this document)	This document explains the functions provided by this service in detail.
IaaS API User Guide	This document provides instructions on how to use the REST API, including how to build an API execution environment and how to use a sample script that suits the sequence you use.
IaaS API Reference • Foundation Service • Network • Application Platform Service • Management Administration • Contract Management	Refer to these manuals when you require detailed information about how to use the REST API.
IaaS Heat Template Specifications	This document explains the format of the Heat Orchestration Template (HOT) that you create in order to use the orchestration function.
IaaS Service Portal User Guide	This document explains how to use the functions provided by this service via Service Portal (Web GUI).
K5 Portal User Guide	This document explains how to use the functions, including registration and user information management, provided by K5 Portal.

Abbreviations Used in This Manual

In this manual, product names are abbreviated as follows.

Official Name	Abbreviation	
FUJITSU Cloud Service K5 IaaS	K5 IaaS	
Microsoft® Windows Server® 2012 SE R2	Windows 2012 R2	Windows
Microsoft® Windows Server® 2008 SE R2	Windows 2008 R2	
Microsoft® Windows Server® 2008 EE R2		
Red Hat® Enterprise Linux® 6.5 (for Intel64)	RHEL6.5	Linux
Red Hat® Enterprise Linux® 7.2 (for Intel64)	RHEL7.2	
Community Enterprise Operating System 6.5	CentOS 6.5	CentOS
Community Enterprise Operating System 7.2	CentOS 7.2	
Red Hat Update Infrastructure	RHUI	
Windows Server Update Services	WSUS	
VMware® vSphere®	VMware vSphere	VMware
VMware® ESX®	ESX	
VMware® ESXi™	ESXi	
VMware® vCenter Server™	vCenter Server	
VMware® vSphere® Client	vSphere Client	
VMware Tools™	VMware Tools	

Trademarks

- Microsoft, Windows, Windows Server and other Microsoft product names and model names are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Java is a registered trademark of Oracle Corporation and its subsidiaries or affiliates in the United States and/or other countries.
- Xeon is a trademark of Intel Corporation in the United States and/or other countries.
- Linux® is a registered trademark of Linus Torvalds in the United States and/or other countries.
- Red Hat and Red Hat Enterprise Linux are trademarks of Red Hat, Inc. registered in the United States and/or other countries.
- Ubuntu is a registered trademark of Canonical Ltd.
- OpenStack is a registered trademark of OpenStack, LLC in the United States.
- VMware and VMware product names are either trademarks or registered trademarks of VMware, Inc. in the United States and/or other countries.
- SAP and SAP logos, SAP R/3, mySAP.com, mySAP Business Suite, and other SAP products are either trademarks or registered trademarks of SAP AG in Germany and/or other countries.
- Akamai and Akamai Intelligent Platform are either trademarks or registered trademarks of Akamai Technologies, Inc.
- Other company names and product names mentioned in this manual are trademarks or registered trademarks of their respective companies.

In this manual, the registered trademark symbols (™ or ®) next to system names or product names have been omitted.

Export Administration Regulations

When exporting or giving this document to a third party, be sure to familiarize yourself with the regulations related to export administration valid in your country of residence and the United States, and follow the necessary procedures.

Note

- The content of this manual may change without prior notice.
- The reproduction of this manual without permission is prohibited.
- We do not assume responsibility for any violation of patent rights or any other rights of a third party that may occur due to the use of the data in this manual.

Revision History

Edition	Date of Update	Location	Overview
1.2	Jan. 18, 2016	*Procedure to Run Sysprep on Windows OS* on page 41	Description added
		Logging in to a Virtual Server on page 17 *IPsec VPN Function* on page 101	Points to note added
1.3	Feb. 29, 2016	*Sharing Virtual Server Images* on page 40 *NAS Software Image* on page 84 *SSL-VPN Connection* *Creating a Virtual Database Server* on page 125	Function added
		Preset Roles and Privileges on page 190 *Software Support Service* on page 27	Description modified
1.4	Apr. 1, 2016	Compute overall	Functional category changed
		Dedicated Virtual Server on page 19 *Software Provision Service* on page 25 *Virtual Server for SAP* *Dedicated Virtual Server for SAP* on page 70	Function added
		New User Registration User Management	Function transferred due to establishment of K5 Portal
1.5	Apr. 7, 2016	*Region* on page 5 *Region Management* on page 189 User Management	Function added due to addition of new region
		Port Management on page 97 *Limiting Values* on page 202	Description modified
1.6	May 19, 2016	Application Deployment Message Queue	Description of unprovided functions deleted
		Checking Console Log on page 19 *Dedicated Virtual Server* on page 19 *Dedicated Virtual Server for SAP* on page 70 *Table 77: Creating a Port (List of Items That Can Be Set)* on page 97 *Table 84: List of Firewall Rule Settings* on page 103	Description modified

Edition	Date of Update	Location	Overview
		Setup of an OpenVPN Client (Windows) *Limiting Values* on page 202	
		Available Commands and SQL Statements on page 134	Article added
1.7	Aug. 4, 2016	*OS Provision Service* on page 22 *OS Patch/Update Settings* on page 23 *Japanese Language Settings for Red Hat Enterprise Linux/CentOS (for version 7.x)* on page 24 *Software Support Service* on page 27 *System Storage* on page 74 *List of Software Support Service IDs* on page 213	OS image added
1.8	Aug. 19, 2016	*Content Delivery Network Service* on page 151 *Limiting Values* on page 202	Function added
1.9	Sep. 16, 2016	*Software Provision Service* on page 25 *SQL Server 2014 Standard Edition Usage Guide* on page 222	Software image added

Contents

Part 1: Preface

Topics:

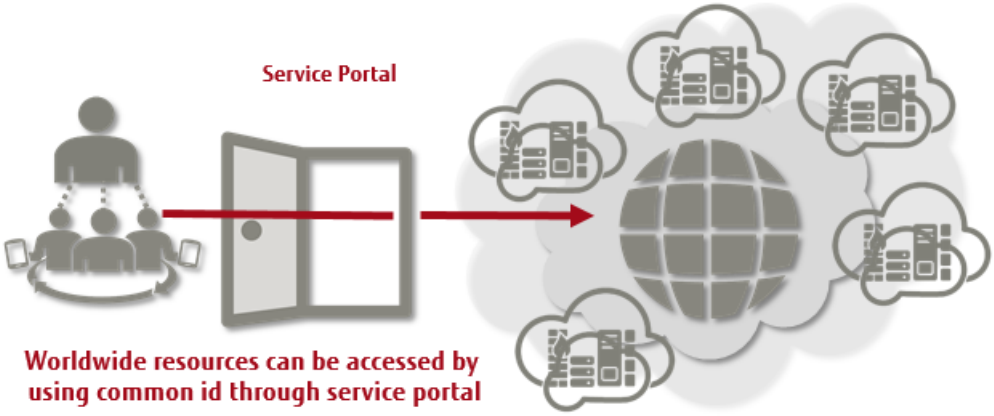
This chapter describes the concept of K5 IaaS services, the menu of available services, and the regions that are covered in relation to using the services.

1.1 Service Concept

1.1.1 Service Overview

K5 IaaS is a global cloud service provided by Fujitsu that allows for flexible on-demand use of virtual servers, storage systems, and other computing resources, with time-based pricing.

Figure 1: Global Cloud Service by Fujitsu

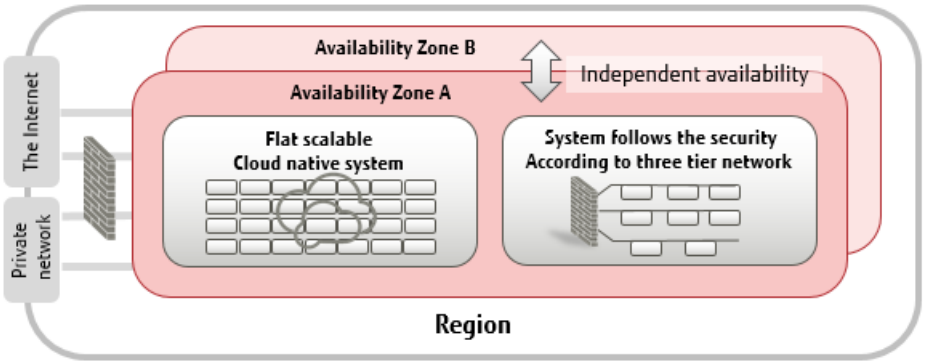


Tip FUJITSU Cloud Service K5 IaaS is a service designed for cloud-native applications. Service Portal is complementary to the API and provides a subset of the main functions available with K5 IaaS. To use the full set of all functions, use the REST API.

High Level of Security

- Both scalable environments connected via flat networks and secure environments divided into multiple network tiers are supported
- Each region contains multiple availability zones (physically independent environments), ensuring high availability
- The authentication and access control functions protect cloud resources.
- The network security service prevents attacks from the outside.

Figure 2: Providing Flexible Network Environment and Availability

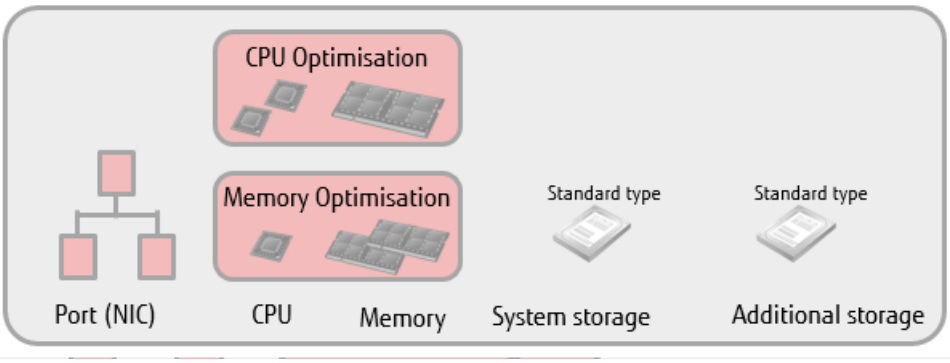


Speed and Flexibility

- Combinations of vCPUs and memory capacity types are provided as virtual server types (flavors) to fit different use cases such as CPU optimization and memory optimization

- Flexible combinations of disk capacities and networks are provided
- Metered billing based on actual use time

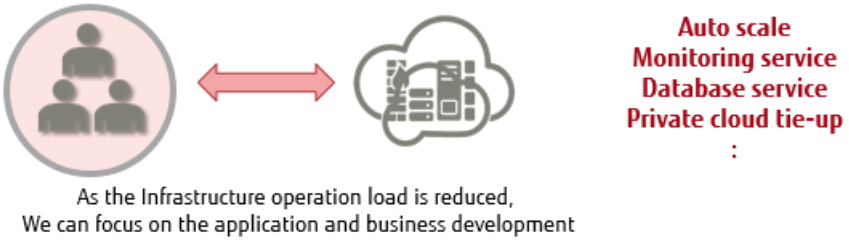
Figure 3: Providing Flexible Combinations of Virtual Resources to Fit Different Use Cases



Lower Operation Burden

- Auto-scaling linked with system monitoring, Database as a Service, and other functions lower system setup costs and operation costs
- Email functions, DNS, and other relevant services required for Internet services are provided

Figure 4: Providing Services and Functions that Reduce Operation Costs

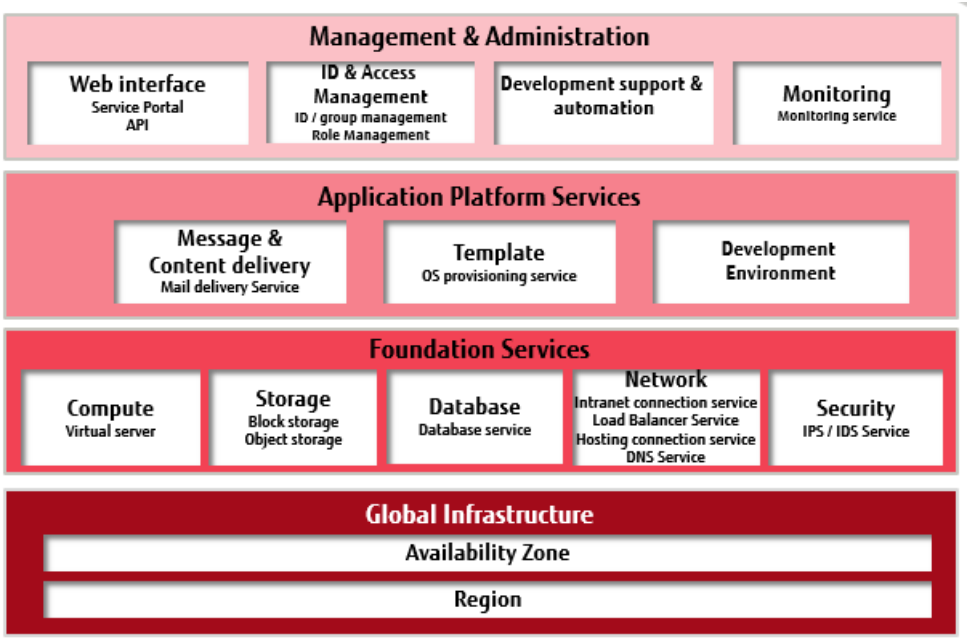


1.1.2 Overview of Services

This section provides an overview of the services available in K5 IaaS.

On each of the four layers in the figure below, K5 IaaS provides services specifically designed for your purposes and needs.

Figure 5: Structure of Services Available



Global Infrastructure

Global Infrastructure makes K5 IaaS available at global locations. The following two location services are provided:

- Region

  Used to protect against regional disasters (disaster recovery purposes).

  Tip

  Overseas regions will be provided as they become available.

- Availability Zone

  Used to minimize the influence of failure at data center facilities.

Foundation Services

Foundation Services provide a virtual infrastructure where you can run your applications and services. Foundation Services provide services that allow you to flexibly combine virtual servers, virtual storage, virtual networks, and other resources via an API or Service Portal to set up an execution environment quickly and as needed.

Application Platform Services

Application Platform Services provide services that support the configuration of large-scale systems, such as services for coordination between your applications and services developed on the base of Foundation Services, or for automatic creation and deployment of built systems.

Management & Administration

The Management & Administration services provide support for continuous operation of your applications and services on Foundation Services.

1.2 Location Services

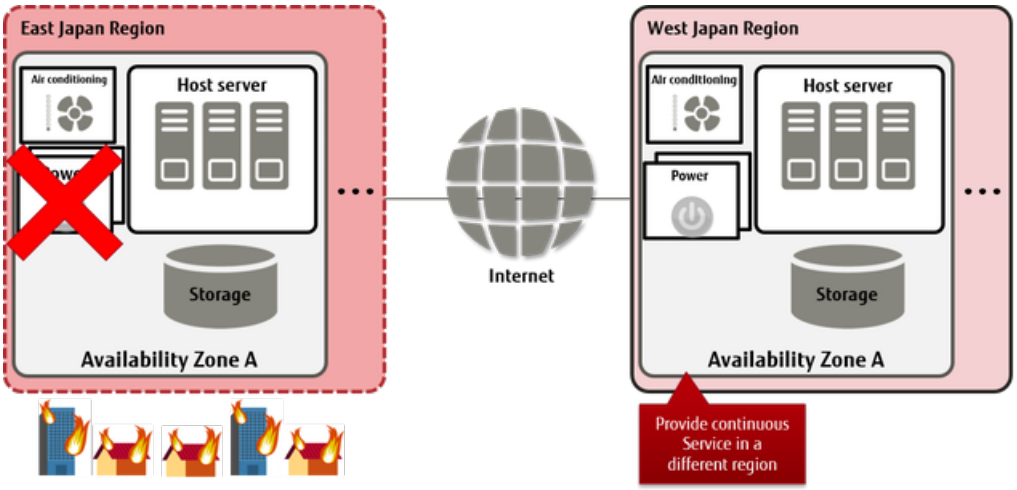
1.2.1 Region

This function provides an environment where multiple regions can be used with a single K5 IaaS account. Such an environment can be used to develop large-scale services or as a measure against disaster.

Regions are geographical areas of Japan or other countries that are separated, such as would be created by splitting along a north-south or east-west divide. Regions are connected via the Internet to form a Wide Area Network.

For protection against disasters that occur in regions where the system is running, you can use multiple regions to prepare a backup system for service continuity and achieve high availability for your business system.

Figure 6: Example of Using Multiple Regions



Available Regions

The following regions are provided.

Table 1: List of Available Regions

Country	Name of Region	Region Identifier
Japan	Eastern Japan Region 1	jp-east-1
	Western Japan Region 1	jp-west-1
	Western Japan Region 2	jp-west-2
United Kingdom	UK Region 1	uk-1

K5 IaaS Service Configurations

- Global Services

  Global services have a single API endpoint as K5 IaaS, and provide resources and services that are not dependent on region. They are used by acquiring global tokens.
- Regional Services

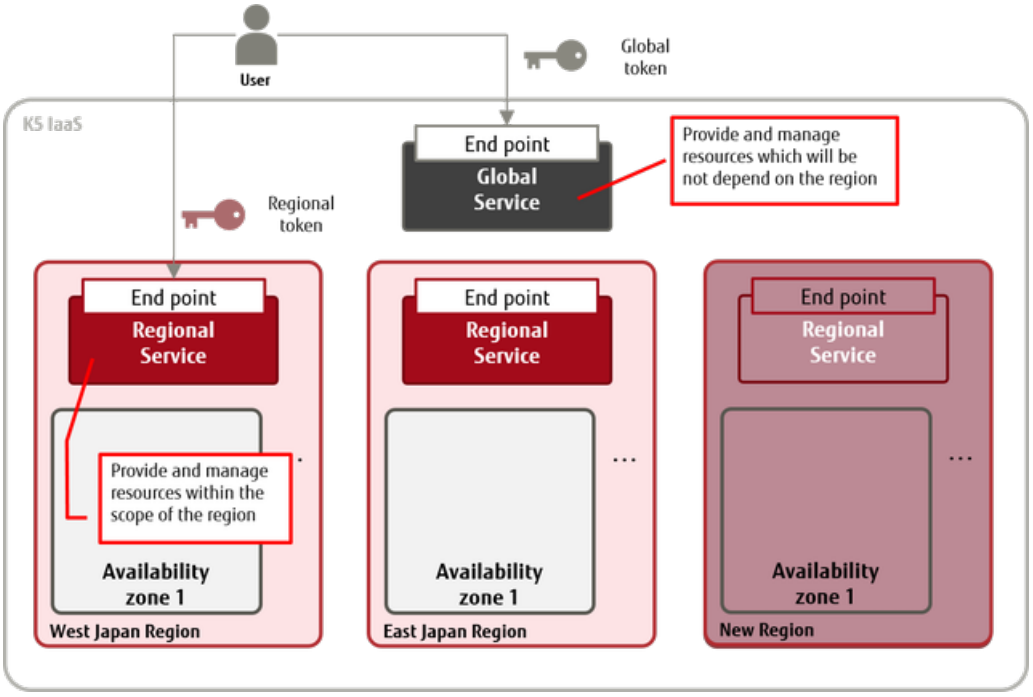
  Regional services have a single API endpoint for each region, and provide resources and services within the region. They are used by acquiring regional tokens.

Tip

For details, refer to the following manuals:

- Explanations of services in *K5 IaaS Features Handbook*
- *K5 IaaS API Reference Manual*

Figure 7: Concept of Global Services and Regional Services



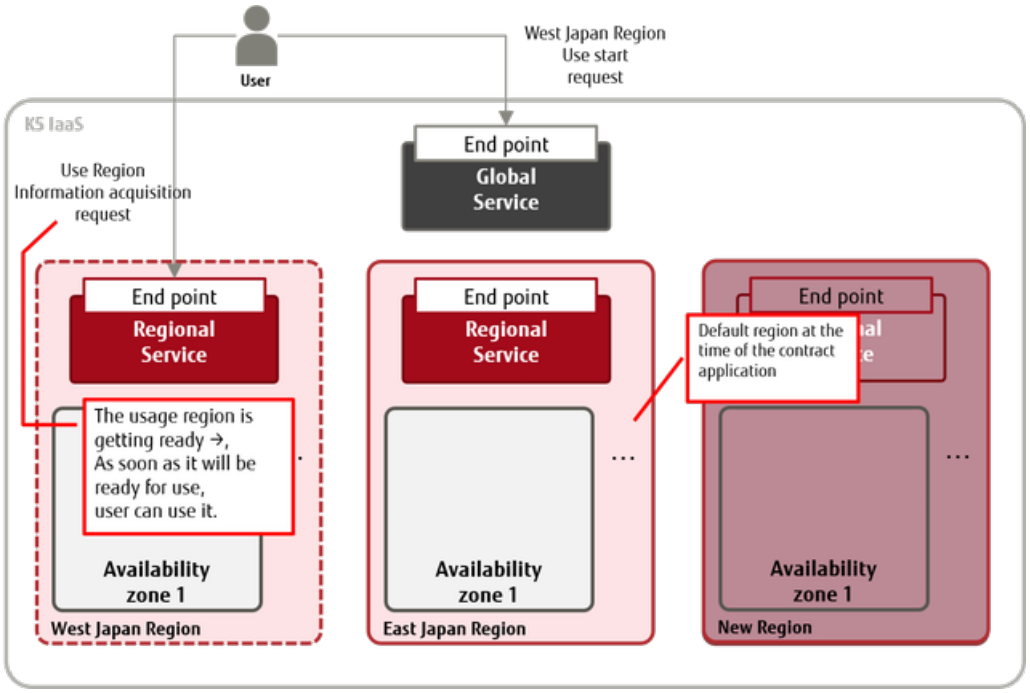
Functions Included

- Region Activation Function

  This function is used to add a different region to a region that is currently being used.

Tip When a contract number (domain) is acquired, "Eastern Japan Region 1 (jp-east-1)" can be used as the default region.

Figure 8: How to Use a Different Region



- Function for Acquiring Information about Regions Currently in Use

  You can acquire a list of regions that are currently in use, as well as their availability ("active" or "ready").
- Authentication Functions
  - Global Authentication Function

    The global token acquisition function is provided to allow the use of global services.

    Tip Use the global user management service to acquire tokens.
  - Regional Authentication Function

    The regional token acquisition function is provided to allow the use of regional services.

    Tip Use the regional user management service to acquire tokens.

Table 2: List of Global Services

Name of Service	Endpoint
Subscription Management	https://contract.gls.cloud.global.fujitsu.com
Global User Management	https://identity.gls.cloud.global.fujitsu.com
Billing Management	https://billing.gls.cloud.global.fujitsu.com
DNS Service	https://dns.gls.cloud.global.fujitsu.com
Product Management	https://catalog.gls.cloud.global.fujitsu.com

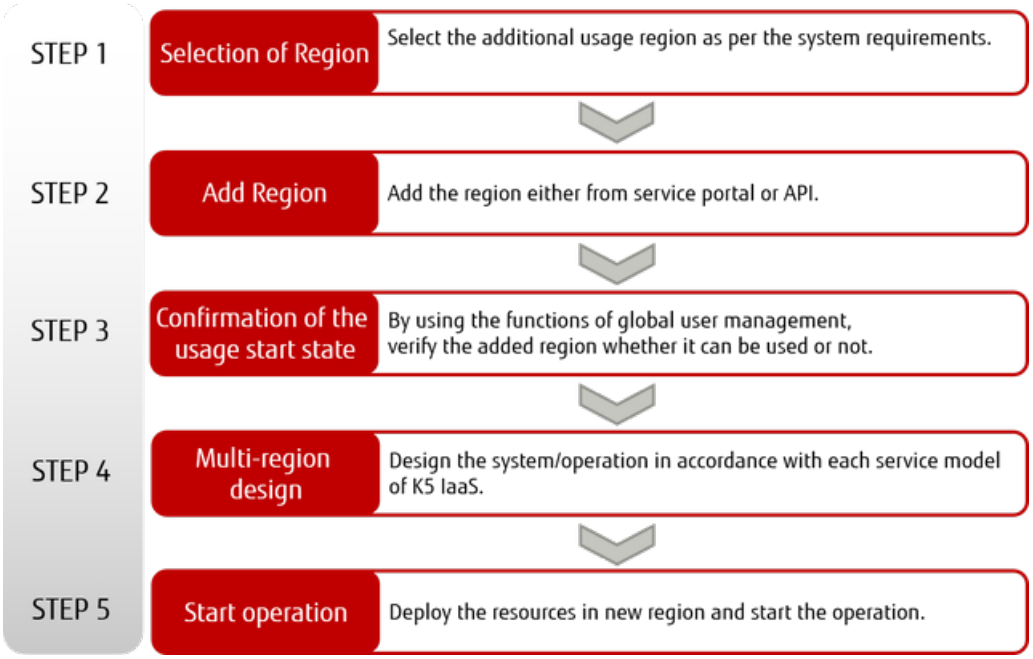
Name of Service	Endpoint
Content Delivery Network Service	https://cdn.gls.cloud.global.fujitsu.com

Table 3: List of Regional Services

Name of Service	Endpoint (*** indicates the region identifier)
Regional User Management	https://identity.***.cloud.global.fujitsu.com
Key Management	https://keymanagement.***.cloud.global.fujitsu.com
Software Management	https://software.***.cloud.global.fujitsu.com
Compute (Standard Service)	https://compute.***.cloud.global.fujitsu.com
Image Management	https://image.***.cloud.global.fujitsu.com
Virtual Server Import	https://vmimport.***.cloud.global.fujitsu.com
Compute (Service for SAP)	https://compute-w.***.cloud.global.fujitsu.com
Auto-Scaling	https://autoscale.***.cloud.global.fujitsu.com
Block Storage	https://blockstorage.***.cloud.global.fujitsu.com
Object Storage	https://objectstorage.***.cloud.global.fujitsu.com
Virtual Network	https://networking.***.cloud.global.fujitsu.com
Virtual Network Extension	https://networking-ex.***.cloud.global.fujitsu.com
Load Balancer	https://loadbalancing.***.cloud.global.fujitsu.com
Database	https://database.***.cloud.global.fujitsu.com
Email Delivery	https://mail.***.cloud.global.fujitsu.com
Orchestration	https://orchestration.***.cloud.global.fujitsu.com
Monitoring	https://telemetry.***.cloud.global.fujitsu.com

How to Use This Service

Figure 9: How to Start Using Multiple Regions



Points to Note

- Common
  - Once you have started using a region, you cannot stop using that region.
  - Global tokens and regional tokens that are acquired with the authentication function cannot be used interchangeably. Use tokens correctly according to the services and resources that you want to use.
    - Use of regional services with global tokens
    - Use of global services with regional tokens
- Global Services
  - Global User Management Service
    - If you use the global user management service to create or change resources, there will be a time lag until all regions are synchronized.

      Tip: You can use the "Check Synchronization between Regions" function provided by the global user management service to check if synchronization is complete in the region you want to use.
  - DNS Service

    Important: The following operations are required to use a DNS service.
    - Create a project in "Eastern Japan Region 1 (jp-east-1)," and register in that project the user who will use the DNS service.
    - Use a regional token.
  - FQDN Compatibility with Old Endpoints

Access to a global service endpoint that was used before the multi-region function was released is transferred to a new endpoint as shown below.

Table 4: List of FQDN Compatibility for Service Endpoints Before and After the Multi-Region Function was Released

Name of Service	Old Endpoint	New Endpoint
Subscription Management	contract.cloud.global.fujitsu.com	contract.gls.cloud.global.fujitsu.com
User Management	identity.cloud.global.fujitsu.com	identity.jp-east-1.cloud.global.fujitsu.com
Key Management	keymanagement.cloud.global.fujitsu.com	keymanagement.jp-east-1.cloud.global.fujitsu.com
Billing Management	billing.cloud.global.fujitsu.com	billing.gls.cloud.global.fujitsu.com
Product Management	catalog.cloud.global.fujitsu.com	catalog.gls.cloud.global.fujitsu.com
DNS Service	dns.cloud.global.fujitsu.com	dns.gls.cloud.global.fujitsu.com

- Regional Services
  - Email Delivery Service

Only "Eastern Japan Region 1 (jp-east-1)" is provided.

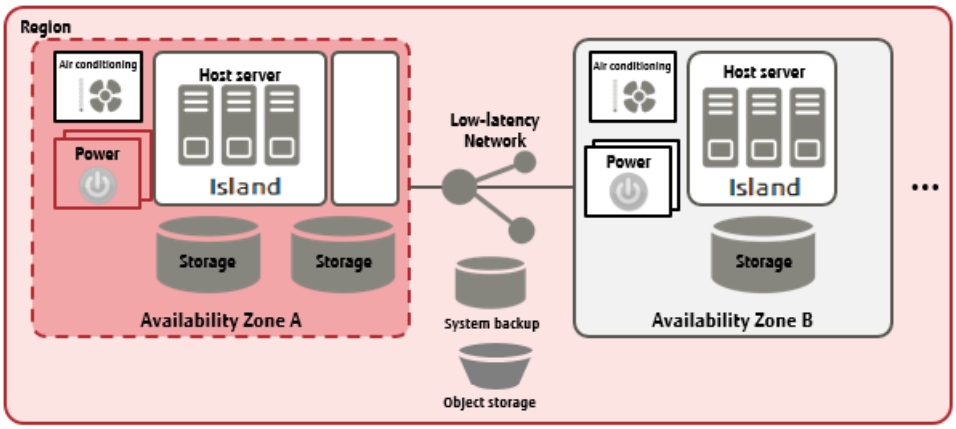
Note

1.2.2 Availability Zone

An availability zone is a unit for sharing physical facilities, such as data center facilities and service provision facilities. Multiple availability zones are provided in each region.

Availability zones are connected via low-latency networks. Distributing your business system over multiple availability zones ensures high availability for your business system.

Figure 10: Example of Using Availability Zones



Part 2: Compute

Topics:

With physical computers separated by virtualization technology, K5 IaaS provides a virtual infrastructure that is accessible via the Internet.

2.1 Standard Services

2.1.1 Virtual Server

2.1.1.1 Creating/Deleting a Virtual Server

You can select the virtual server you want to create from several types, according to the purpose (such as to serve as a web server or as an application server). You can also delete servers that are in use at any time if they are no longer needed.

Creating a Virtual Server

You can create a virtual server from one of the image types explained below.

- Standard

  Image prepared by using the *OS Provision Service* on page 22 or *Software Provision Service* on page 25
- Created by the user

  Image prepared through *management of the virtual server image*
- Imported by the user

  Image prepared by using the *virtual server import service*

When you create a virtual server, specify the following:

- Region and availability zones for the virtual server
- *Virtual server type (flavor)*
- System block storage type and OS
- Port and the subnet of the connection destination
- Security groups
- Key pair for login to the virtual server
- *Provisioning script*
- Automatic failover

Important In order to use the functions available when you create a virtual server, a virtual router must be connected to the network to which the virtual server connects.

Administrator Password for a Virtual Server

- For Windows

  When you create the virtual server, specify the key pair name that you have created as a parameter. Use key file (*.pem) of the specified key pair to acquire the random Administrator password that is issued by the system.

  Example: How to decrypt the random password that was issued

```
$ COMPUTE=endpoint of virtual server API
$ OS_AUTH_TOKEN=token string acquired
$ SERVER_ID=ID of created Windows virtual server
$ PROJECT_ID=project ID of created Windows virtual server
$ curl -s $COMPUTE/v2/$PROJECT_ID/servers/$SERVER_ID/os-server-password -
X GET -H "X-Auth-Token: $OS_AUTH_TOKEN" | jq .
{
  "password": "password string"
}
$ PASSWORD=password string acquired by above command
```

```
$ echo $PASSWORD | openssl base64 -d -A | openssl rsautl -decrypt -inkey
 key file(.pem)
```

Note After you have created the virtual server, confirm that it is in an ACTIVE state, and then acquire the password string.

Deleting a Virtual Server

If you no longer need a certain virtual server, you can delete it at any time.

Note When you create a virtual server, specify whether to retain the system storage of the server upon deletion.

Tip If you specify to retain the system storage, we recommend that you stop the server in advance in order to avoid damage to the data in the system storage.

Available Virtual Server Types

The types (flavors) of virtual servers that are provided are as follows:

Table 5: List of Provided Virtual Server Types (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
S-1	1	4
S-2	2	8
S-4	4	16
S-8	8	32
S-16	16	64
M-1	1	8
M-2	2	16
M-4	4	32
M-8	8	64
M-16	16	128
XM-4	4	128

Automatic Failover

If the server stops during an operation due to issues such as failure of the physical host machine at the data center, you can automatically move the virtual server that was operating on that host machine to a different host machine and operate the server there. When you create a virtual server, specify whether to enable an automatic failover.

Important You cannot select virtual machines for which you enabled an automatic failover as targets of auto-scaling.

2.1.1.2 Provisioning Script Function

This function carries out the initial processing such as exchange of data and automatic processing by script when the virtual server is created.

The provisioning script function relays the required information when the virtual server is created through the following multiple methods:

- Metadata
- User data

Metadata Settings

Associate the virtual server with data in the KeyValue format to configure the settings. In addition to the data that is automatically set when the server is created, you can configure other settings that you need. For example, information for recognizing a collection of servers as one system, such as VSYS_NAME=e-learning.

User Data Settings

The user data function transfers data in text format to the virtual server. You can set a script to be executed when the virtual server is started.

- For CentOS

  Describe the script using sh or bash.
- For Red Hat Enterprise Linux

  Describe the script using sh or bash.
- For Windows

  Describe the script using PowerShell or Windows Batch.

Note

The script is executed by the software function below that is appropriate for the OS. For details, refer to the support site of the software involved.

Table 6: Software That Provides the Script Function by OS Type

OS Type	Software That Provides the Script Function
CentOS	Cloud-init
Red Hat Enterprise Linux	Cloud-init
Windows	Cloudbase-init

2.1.1.3 Scaling Up and Scaling Down of a Virtual Server

You can change the type of a virtual server that has been created, as necessary.

If, due to the operational conditions of the virtual server, the performance of the virtual server type that you selected when you created it is insufficient or is excessive, you can change the specifications of that virtual server.

Tip

If the specifications of the virtual server are more than enough to satisfy the requirements of the application operation load, you can reduce operation costs by scaling down.

Resizing of a Virtual Server

You can change the *Virtual Server Type* of a virtual server that has been created to a different type.

Important

- For Operation from the Service Portal

  Make sure that the virtual server to be resized is in an operating state (ACTIVE) and that all the applications have stopped, and then resize the virtual server.

The virtual server is stopped forcibly during the resizing processing and starts up automatically after resizing is completed.

- For Operation from the API

  Make sure that the virtual server to be resized is in a shut-down state (SHUTOFF), and then resize the virtual server.

  The virtual server does not start up automatically after resizing is completed. Start the virtual server manually.

Rollback of Virtual Server Resizing

You can rollback the resizing of the virtual server in some situations, such as if the target virtual server does not properly enter an ACTIVE state after it has been resized.

2.1.1.4 Operations on a Virtual Server

You can carry out the following operations on a virtual server that has been created in the system.

Startup/Termination of a Virtual Server

Start the created virtual server from a shut-down state (SHUTOFF). Or, shut down the server from an operating state (ACTIVE).


Important A virtual server that is shut down from the OS or terminated from the service portal/API will be subject to usage charges. After termination, servers that are used infrequently can be released in order to reduce costs.


Note A virtual server that is terminated from the service portal/API will be stopped forcibly, which is equivalent to a forced power shutdown. To shut down a virtual server normally, log in to the virtual server and carry out a shutdown operation.

Release/Restoration of a Virtual Server

In order to release the CPU and memory resources in use by the virtual server, release the virtual server. Virtual servers that have been released will enter a released state (SHELVED_OFFLOADED).


Tip You can carry out the release of a virtual server from both an operating state and from a terminated state.


Note You cannot carry out the following operations on a virtual server that has been released:

- Connection/disconnection of port
- Attachment/detachment of a block storage
- Changing of virtual server type
- Re-creation of virtual server
- Startup/termination of virtual server

In order to return a released server to a state in which it can be used normally, restore it.


Important When you restore a virtual server, it is restored to an operating (ACTIVE) state. Be aware that charges are applied for services such as the OS provision service and the software provision service.

Rebooting a Virtual Server

- Soft reboot (equivalent to the OS reboot command)
- Hard reboot (equivalent to the reset button)

Changing Virtual Server Settings

You can change the existing settings of a virtual server. You can make the following changes:

- Change of the virtual server name
- Change of the IP address

Note

You can change the IPV4 address only.

Attachment/Detachment of a Block Storage

Specify the device name of the existing block storage (example: /dev/vdb) and attach it. You can also detach a block storage that is no longer needed.

Port Connection/Disconnection

Ports can be added or removed on the virtual server.

2.1.1.5 Server Group Function

You can register multiple virtual servers together as one server group, and specify how the server group behaves as a policy.

Specify the behavior of the server group as an entity by specifying how the collection of servers is run on the physical host.

- Affinity

  The virtual servers that are registered in the server group for which the Affinity policy is specified are started on the same physical host when possible.

  This helps communication between virtual servers within the same server group become faster compared to when Anti-Affinity is specified.

- Anti-Affinity

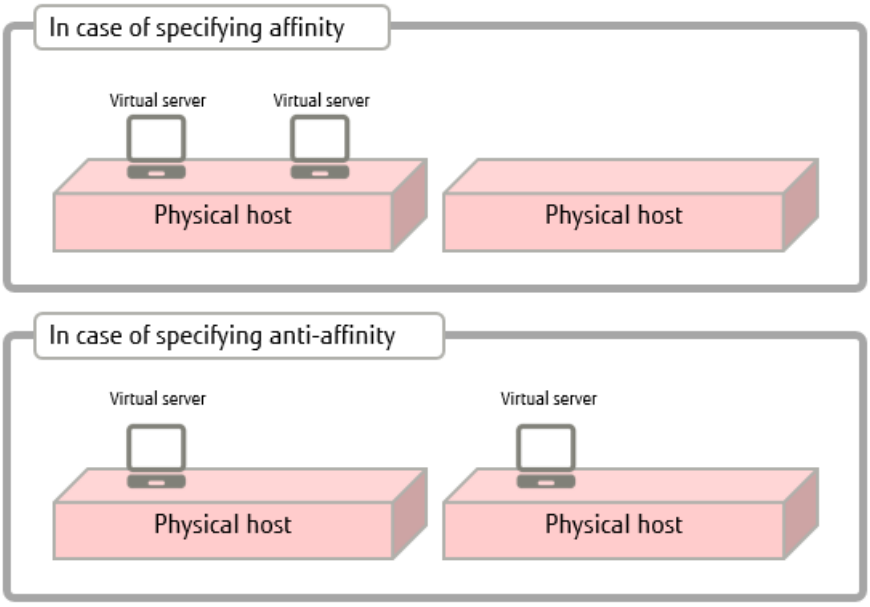
  The virtual servers registered in the server group for which the Anti-Affinity policy is specified are started on different physical hosts when possible.

  In this case, even if some physical hosts go down, virtual servers running on the other physical hosts are not affected. Therefore, in a scale out configuration, your business system keeps on running.

Specify the server group when you create the virtual server.

Tip

Figure 11: Operation of the Server Group Function



Note

Operation of the server group function is not guaranteed. Depending on the usage of K5 IaaS, you may experience the following:

- Even when you specify Affinity, some virtual servers may start on different physical hosts.
- Even when you specify Anti-Affinity, some virtual servers may start on the same physical host.

2.1.1.6 Logging in to a Virtual Server

This section explains how to log in through the network while the virtual server is in operation.

The method of logging in to the virtual server depends on the OS image that is in use.

Logging in to CentOS Virtual Server

To log in to a CentOS virtual server via SSH, use the registered key pair that you used when you created the virtual server.

The user ID for the Administrator is "k5user."

Tip

Logging in to Red Hat Enterprise Linux Virtual Server

To log in to a Red Hat Enterprise Linux virtual server via SSH, use the registered key pair that you used when you created the virtual server.

The user ID for the Administrator is "k5user."

Tip

Logging in to Ubuntu Virtual Server

To log in to an Ubuntu virtual server via SSH, use the registered key pair that you used when you created the virtual server.

Tip The user ID for the Administrator is "ubuntu."

Logging in to Windows Virtual Server

To log in to a Windows virtual server, use a remote desktop connection. Specify the private IP address of the target virtual server, and use a remote desktop connection to connect from the client PC.

Tip The user ID for the Administrator is "k5user," and the password is the password you obtained in *Administrator Password for a Virtual Server* on page 12 when you created the virtual server.

Important When you log in to Windows 2012 R2 for the first time, the inquiry message shown below appears on the right side of the screen. Be sure to select [Yes]. If you select [No], a remote desktop connection may not be possible.

```
Do you want to find PCs, devices, and content on this network, and
 automatically connect to devices like printers and TVs?

We recommend that you do this on your home network and work network.
```

2.1.1.7 Key Pair Management Function

You can create and register a key pair for logging in to the virtual server via SSH. You can also import a key pair that was created externally.

When you register the key pair, you can acquire the key file for SSH authentication (*.pem). You can log in to the virtual server easily by using the following procedure.

1. When you create the virtual server, specify the key pair that you have registered, and obtain the key file (*.pem).
2. On the SSH client software side, set the acquired key file (*.pem).
3. Log in to the virtual server via SSH connection.

Important Exercise appropriate caution when you manage the key file.

Creating and Importing a Key Pair

Specify the key pair name and create the key pair. You can also specify a public key that was created with ssh-keygen or other tools to register the key pair.

Note We recommend you create a key with a passphrase if you use an external tool to create the key pair.

Table 7: List of Key Pair Settings

Item	Description	Required
Key Pair Name	Specify the name of the key pair.	
Public Key String	Specify the public key string that you created with an external tool	

The information entered for the Public Key String is the information of img_rsa.pub, which is created in "Example of Creation of Key Pair with Passphrase"

Example of Creating a Key Pair with a Passphrase

Below is an example of using ssh-keygen to create a key pair with a passphrase.

```
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user1/.ssh/id_rsa): /tmp/img_rsa
 Enter passphrase (empty for no passphrase): Enter passphrase
Enter same passphrase again: Enter passphrase
Your identification has been saved in /tmp/img_rsa.
Your public key has been saved in /tmp/img_rsa.pub.
The key fingerprint is:
6e:d0:(omitted):c0:8b user1@LinuxImgDev
The key's randomart image is:
(omitted)
```

Deleting a Registered Key Pair

You can delete key pairs that are no longer needed.

2.1.1.8 Checking Console Log

A function that allows you to check the console output is provided, for the purpose of investigating trouble that occurs when you start the virtual server and such.


Tip

By specifying a number of lines of the log, you can acquire the specified number of lines of console log content, starting with the newest line.


Note

When a virtual server is released, the content of the console log up until that time is deleted and you can no longer view the content. In addition, you cannot view the console log in a released state (SHELVED_OFFLOADED).

2.1.2 Dedicated Virtual Server

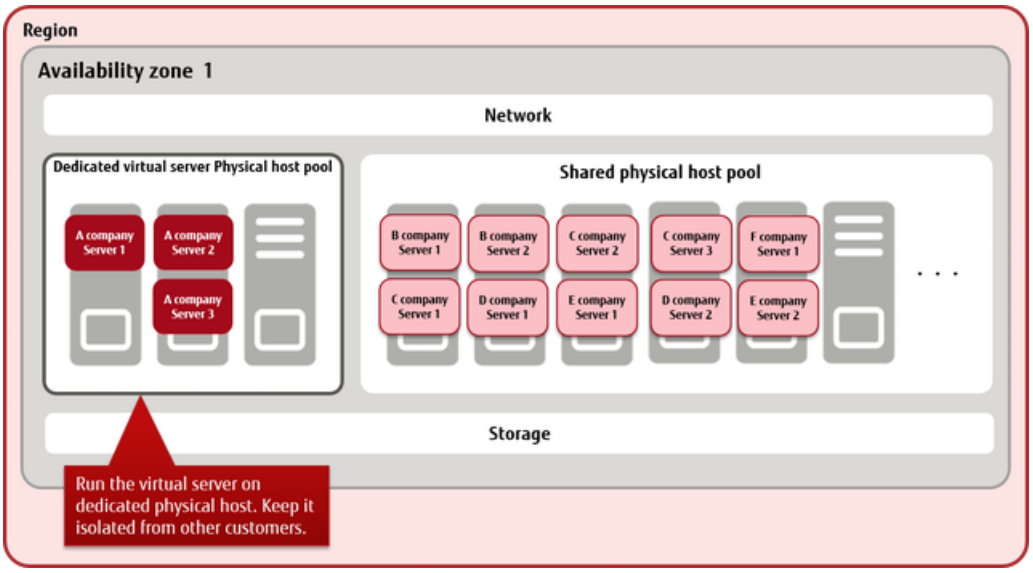
2.1.2.1 Dedicated Virtual Server

A pool for dedicated physical hosts is secured for each contract number (domain), and a function that can create a dedicated virtual server is provided.

Since virtual servers for another customer will not be created on the physical host that you have secured, this server can be used for environments that must be separate from other users (single tenant) for reasons such as compliance and license management.


Important

The storage and networks are shared.



Available Server Types for Dedicated Virtual Servers

The types of virtual servers that are available as dedicated virtual servers are the same as normal virtual servers.

Table 8: List of Provided Virtual Server Types (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
S-1	1	4
S-2	2	8
S-4	4	16
S-8	8	32
S-16	16	64
M-1	1	8
M-2	2	16
M-4	4	32
M-8	8	64
M-16	16	128
XM-4	4	128

Physical Host Pool Menu

- Basic Set: "2 server configuration"

  A physical host pool that includes a failover host is secured as the creation destination for the virtual server that is dedicated to the customer. You must apply for one Basic Set for each availability zone in which you will run a dedicated virtual server.
- Additional Servers

  Use additional servers when you want to increase the capacity of available dedicated virtual servers, such as when there is increased demand on the system. Physical hosts are added to the same pool where the Basic Set is currently used.

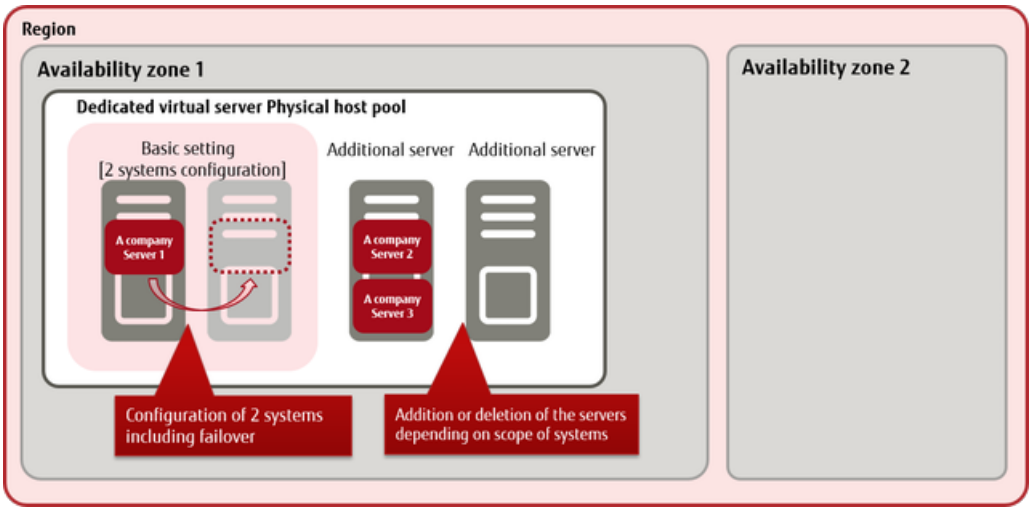
The following amounts of resources can be used by each physical host.

Tip

Number of Virtual CPUs	40
Memory	250 GB

Confirm the type of dedicated virtual server, and then estimate the number of dedicated virtual servers that can be created.

Figure 12: Using the Physical Host Pool Menu



Functions Included

When you create a virtual server, you have the option of creating it in a physical host pool that you have secured. Dedicated virtual servers that you create can be managed by project, in the same way as a normal virtual server.

Note

- You cannot specify a specific physical host in a physical host pool to create a virtual server.
- The physical host pool for a single contract number is shared between all projects.

Dedicated virtual servers that you have created have the same Compute function as normal virtual servers.

- Compute
  - Dedicated Virtual Server
    - Creating/Deleting a Dedicated Virtual Server
    - Provisioning Script Function
    - Scaling Up and Scaling Down of a Dedicated Virtual Server
    - Startup/Termination of a Dedicated Virtual Server
    - Release/Restoration of a Dedicated Virtual Server
    - Restarting a Dedicated Virtual Server
    - Server Group Function

      Note: You cannot use the Anti-Affinity policy.
    - Attachment/Detachment of a Block Storage
    - Port Connection/Disconnection
    - Key Pair Management Function
    - Checking Console Log

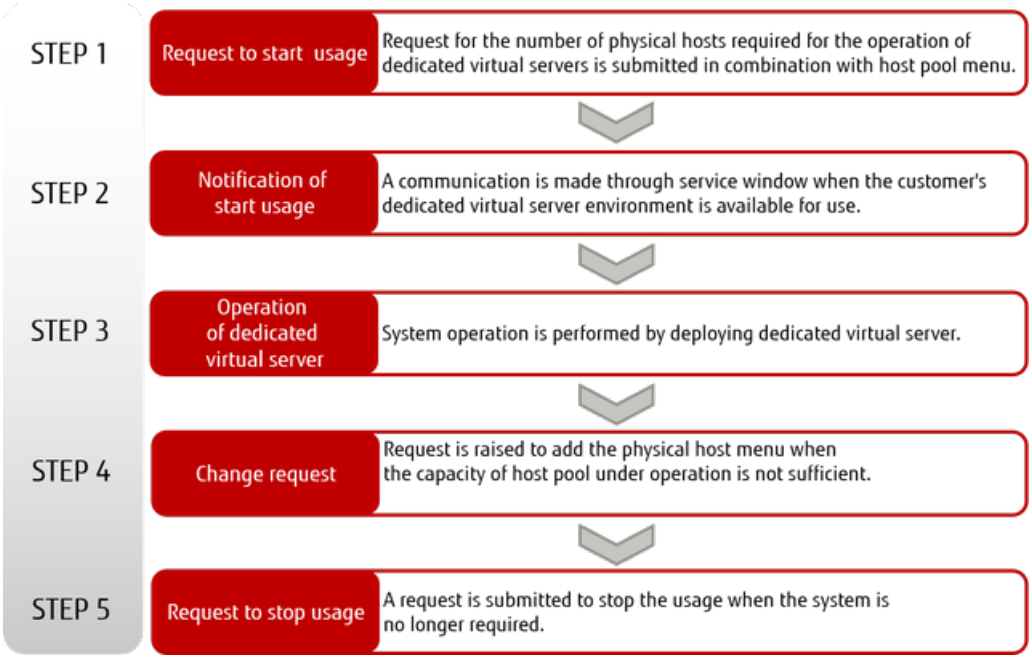
- OS Provision Service
- Software Support Service
- Auto-Scaling
- Image
- Virtual Server Import Service

For shared storage and networks, you can use the same functions as a normal virtual server.

- Storage
- Network

How to Use This Service

Figure 13: Procedure from Starting to Stopping a Dedicated Virtual Server



Points to Note

- A contract number (domain) can have only one physical host pool where dedicated virtual servers are created.
- Although the physical host is a dedicated machine, it is unlikely to improve the performance of any dedicated virtual servers that are created.
- Although the physical host is separate from other users, the network is shared. Therefore, separation in regards to security is not guaranteed. Use security groups and the firewall function to ensure security in the same way as you would with a normal virtual server.

2.1.3 OS Provision Service

2.1.3.1 OS Provision Service

The service provides an OS for the virtual server. We plan to continually expand the OS types, editions, and versions provided by K5 IaaS.

OS Provision Service

You can choose an OS for the virtual server from the following lineup. When you create the virtual server, select the OS image that you want to use.

Table 9: OS Environment Provided

OS Type	OS Provided
Windows	• Windows Server 2008 SE R2 SP1 64bit English Version • Windows Server 2008 EE R2 SP1 64bit English Version • Windows Server 2012 SE R2 64bit English Version • Windows Server 2012 SE 64bit English Version
Linux	• CentOS 6.5 64bit (English) • CentOS 7.2 64bit (English) • Red Hat Enterprise Linux 6.5 64bit (English) • Red Hat Enterprise Linux 7.2 64bit (English) • Ubuntu Server 14.04 LTS (English)

DNS Server Settings of the OS

To resolve Internet names from the OS, refer to *Common Network Services* on page 214 to set the name server information that corresponds to the region and availability zone in which the virtual server exists.

2.1.3.2 OS Patch/Update Settings

This section describes the settings required to apply patches and updates to the virtual server to be created.

Note Configure in advance the network settings (connection to external networks, security group settings and such) required to connect to the repository where patch files and updates are provided.

Red Hat Update Infrastructure Settings

When you use Red Hat Enterprise Linux, the following settings are required in order to use RHUI:

1. Transfer RHUI Agent to virtual server

   Table 10: List of the corresponding RHUI Agent module

OS Version	Name of module transfered
Red Hat Enterprise Linux 6.x	rhui-entitlement6-2.0-1.noarch.rpm
Red Hat Enterprise Linux 7.x	rhui-entitlement7-2.0-2.noarch.rpm

2. Install RHUI Agent on virtual server
3. Use yum to perform update

Note Allow the following in the security group settings:

- Egress: TCP/Port 53, UDP/Port 53, TCP/Port 80

2.1.3.3 Japanese Language Settings for Red Hat Enterprise Linux/CentOS (for version 6.x)

In order to create an image of the English Linux OS provided by the service and use it in Japanese, configuration of the following settings is required.

Supported OS:

- Red Hat Enterprise Linux 6.5 64bit (English)
- CentOS 6.5 64bit (English)

Log in to the virtual server that you want to use in Japanese and configure the following settings to use the English Linux OS in Japanese.

Time Zone Settings

Change the setting of the time zone to "Asia/Tokyo."

1. Change the time zone setting in /etc/sysconfig/clock as shown below.

```
ZONE="Asia/Tokyo"
```

2. Overwrite /etc/localtime with the following command:

```
# cp -f /usr/share/zoneinfo/Asia/Tokyo /etc/localtime
```

Checking the System Clock

Execute the following command and confirm that the setting of the system clock is set to "UTC."

```
# cat /etc/adjtime
0.000069 1423210340 0.000000
1423210340
UTC
```

Changing the Language

Change the language setting in /etc/sysconfig/i18n as shown below.

```
LANG="ja_JP.UTF8"
```

Changing the Keyboard Layout

Change /etc/sysconfig/keyboard as shown below.

```
KEYTABLE="jp106"
MODEL="jp106"
LAYOUT="jp"
KEYBOARDTYPE="pc"
```

Reflecting Changed Settings

When you have completed all of the changes, shut down the virtual server and make sure that it has entered SHUTOFF state before you start it.

Important Because settings may not be reflected if you restart, you must shut down the system entirely and then start it.

2.1.3.4 Japanese Language Settings for Red Hat Enterprise Linux/CentOS (for version 7.x)

In order to create an image of the English Linux OS provided by the service and use it in Japanese, configuration of the following settings is required.

Supported OS:

- Red Hat Enterprise Linux 7.2 64bit (English)
- CentOS 7.2 64bit (English)

Log in to the virtual server that you want to use in Japanese and configure the following settings to use the English Linux OS in Japanese.

Time Zone Settings

Change the setting of the time zone to "Asia/Tokyo."

1. Execute the following command.

```
# timedatectl set-timezone Asia/Tokyo
```

2. Checking with the following command:

```
# timedatectl status
      Local time: Mon 2016-08-01 18:57:37 JST
  Universal time: Mon 2016-08-01 09:57:37 UTC
        RTC time: Mon 2016-08-01 09:57:36
       Time zone: Asia/Tokyo (JST, +0900)
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: no
      DST active: n/a
```

Changing the Language

Execute the following command.

```
# localectl set-locale LANG=ja_JP.UTF-8
```

Changing the Keyboard Layout

Change /etc/sysconfig/keyboard as shown below.

1. Execute the following command.

```
# localectl set-keymap jp106
```

2. Checking with the following command:

```
# localectl status
   System Locale: LANG=ja_JP.UTF-8
       VC Keymap: jp106
      X11 Layout: jp
       X11 Model: jp106
```

Reflecting Changed Settings

When you have completed all of the changes, shut down the virtual server and make sure that it has entered SHUTOFF state before you start it.


Important Because settings may not be reflected if you restart, you must shut down the system entirely and then start it.

2.1.4 Software Provision Service

2.1.4.1 Software Provision Service

This service provides a virtual server with software installed.

Provided Software

Table 11: Software Provision Service

Software	Version Provided
Microsoft SQL Server	• Microsoft SQL Server 2014 SE 64bit English Version

Required Number of Licenses

Table 12: List of Required Number of Licenses by Virtual Server Type

Software	Name of Virtual Server Type	Required Number of Licenses
Microsoft SQL Server	S-1	1
	S-2	1
	S-4	1
	S-8	2
	S-16	4
	M-1	1
	M-2	1
	M-4	1
	M-8	2
	M-16	4
	XM-4	1

How to Use This Service

You can create a virtual server from one of the image types included in the software shown below:

Table 13: Software Provision Service, List of Images

Image Name	OS and Software
Windows Server 2012 R2 SE + SQL Server 2014 SE (English)	OS: Windows Server 2012 SE R2 64bit English Version Software: Microsoft SQL Server 2014 SE 64bit English Version

After creating a virtual server, refer to the following information for how to use the software:

Table 14: Software Provision Service Usage Guide

Software	Reference
Microsoft SQL Server	*SQL Server 2014 Standard Edition Usage Guide* on page 222

2.1.5 Software Support Service

2.1.5.1 Software Support Service

We offer software support for some of the software that is provided with a virtual server (including the OS).

This service allows you to change the support option for the OS or for the software that is used on the virtual server to meet your support requirements, after the virtual server has been created.

Software Whose Support Option You Can Change

- OS Provision Service

  Table 15: OS that Allow Changes to Support Options

OS Type	OS Provided
Windows	• Windows Server 2008 SE R2 SP1 64bit English Version • Windows Server 2008 EE R2 SP1 64bit English Version • Windows Server 2012 SE R2 64bit English Version • Windows Server 2012 SE 64bit English Version
Linux	• Red Hat Enterprise Linux 6.5 64bit English Version • Red Hat Enterprise Linux 7.2 64bit English Version

- Software Provision Service

  Table 16: Software that Allows Changes to Support Options

Software	Version Provided
Microsoft SQL Server	• Microsoft SQL Server 2014 SE 64bit English Version

Functions Included

- Support Option Change Function

  When a virtual server is created, the system default support option is configured for the software that is used on that virtual server.

  Table 17: System Default Support Option Overview (OS that Allow Changes to Support Options)

OS	Default Support Option
Windows Server 2008 SE R2 SP1 64bit English Version	No support
Windows Server 2008 EE R2 SP1 64bit English Version	No support
Windows Server 2012 SE R2 64bit English Version	No support

OS	Default Support Option
Windows Server 2012 SE 64bit English Version	No support
Red Hat Enterprise Linux 6.5 64bit English Version	24-hour support
Red Hat Enterprise Linux 7.2 64bit English Version	24-hour support

Table 18: System Default Support Option Overview (Software that Allows Changes to Support Options)

Software	Default Support Option
Microsoft SQL Server 2014 SE 64bit English Version	No support

Use the support option change function to change the support level for the software type.

Tip When changing the support level, you can select from among the different types of support provided for the same software.

Table 19: Changing Support Options, List of Support Levels (OS)

OS	Support Levels that Allow Changes
Windows Server 2008 SE R2 SP1 64bit English Version	• No support
Windows Server 2008 EE R2 SP1 64bit English Version	• No support
Windows Server 2012 SE R2 64bit English Version	• No support
Windows Server 2012 SE 64bit English Version	• No support
Red Hat Enterprise Linux 6.5 64bit English Version	• 24-hour support
Red Hat Enterprise Linux 7.2 64bit English Version	• 24-hour support

Table 20: Changing Support Options, List of Support Levels (Software)

Software	Support Levels that Allow Changes
Microsoft SQL Server 2014 SE 64bit English Version	• No support

Applicable Prices, Billing Start and Inquiry Start Timing

- Applicable prices

  The option with the higher usage charges is applied for the billing month when the software support option was changed.

- Start of the billing period

  Note: You can change the support option even if the virtual server has not been started. In this case, the billing period starts when you start the virtual server for the first time after applying the changes.

- Time required for the inquiry service to become available

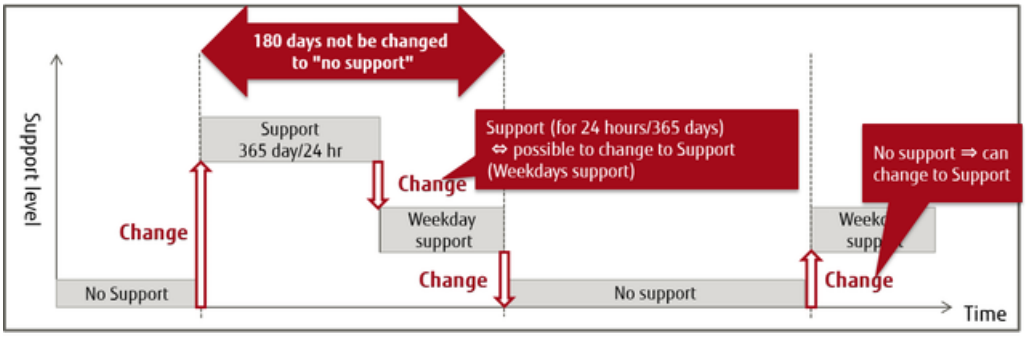
  If you change the settings to "Support Available," the inquiry service becomes available within five business days.

  Note: You can change the support option even if the virtual server has not been started. In this case, the inquiry service becomes available within five business days of when you start the virtual server for the first time after applying the changes.

Limitations Related to Changing Support Options

This section explains the limitations to note regarding software for which "No Support" is a support option.

Important: When you switch from "No Support" to "Support Available," you cannot switch back to "No Support" for 180 days starting from the day when the changes were applied.

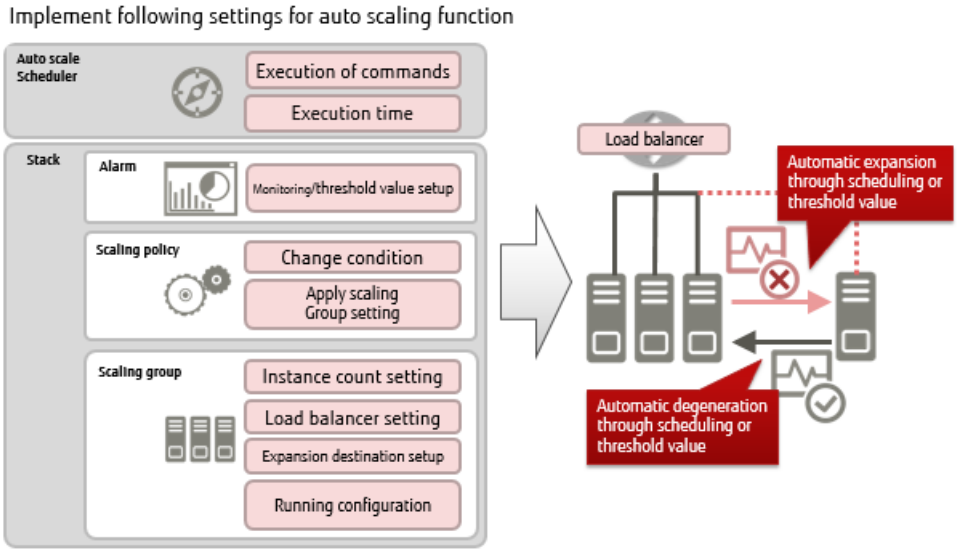


2.1.6 Auto-Scaling

2.1.6.1 Auto-Scaling Settings

You can set a scaling group that has specific conditions (such as the number of virtual servers) in the stack definition in order to automatically control the increase and decrease of resources.

Figure 14: Overview of Auto-Scaling



You can configure the auto-scaling function settings as follows.

Scaling Group Management Function

Set the following items to create scaling groups and register them in the stack. You can also configure settings for the *health check function*, which detects abnormality on scaled-out virtual servers and starts recovery automatically.

Table 21: List of Settings for Scaling Groups

Item	Description	Required
Cool down period (Cooldown)	Specify this setting, in seconds, to prevent the next scaling operation from taking place immediately after the previous scaling operation was completed	
Startup configuration name (LaunchConfiguration)	Specify the name of a startup configuration to start the virtual server	Yes
Load balancer name (LoadBalancerNames)	Specify as a list the names of the load balancers that are included in the scaling operation	
Maximum number (MaxSize)	Specify the maximum number of virtual servers to be scaled	Yes
Minimum number (MinSize)	Specify the minimum number of virtual servers to be scaled Tip This is the number of servers that are created initially when the stack is registered.	Yes

Item	Description	Required
Availability zone name (AvailabilityZones)	Specify the name of the availability zone where you intend to create the scaling group	Yes
Subnet ID list (VPCZoneIdentifier)	Specify as a list the subnet IDs that exist in the availability zone that you specified for the availability zone name	

Scaling Policy Settings

Specify the following items to set a scaling policy.

Table 22: List of Settings for Scaling Policies

Item	Description	Required
Scaling type (AdjustmentType)	Specify how to increase or decrease the number of virtual servers by selecting one of the following types • ChangeInCapacity Adds the specified number of virtual servers when the number is positive, and deletes the specified number of virtual servers when the number is negative • ExactCapacity Changes the number of virtual servers to the specified number • PercentChangeInCapacity Increases or decreases by the specified ratio (percentage), from 1 to 100	Yes
Scaling group name (AutoScalingGroupName)	Specify the name of the scaling group on which you intend to set the scaling policy	Yes
Cool down period (Cooldown)	Specify this setting, in seconds, to prevent the next scaling operation from taking place immediately after the previous scaling operation was completed	
Scaling value (ScalingAdjustment)	Specify the scaling adjustment value according to the type that you specify for the scaling type Example: When you set the scaling type as "ChangeInCapacity" and set the change value as "-1," a virtual server will be deleted when the policy is applied	Yes

Startup Configuration Settings

Define the settings for when a scaling policy is applied and the virtual servers that are added are actually started.

Only one port can be connected to the virtual servers in the scaling group.

Note

Table 23: List of Settings for Startup Configurations

Item	Description	Required
Image ID (ImageId)	Specify the ID or name of the image to be used on the virtual server to be started	Yes
Virtual server type (InstanceType)	Specify the type name (flavor name) of the virtual server to be started	Yes
Key name (KeyName)	Specify the name of the key pair that is set on the virtual server to be started	
Security group (SecurityGroups)	Specify as a list the security group names to be set on the virtual server to be started	
User data (UserData)	Specify the user data to be executed when a virtual server is started	
List of block storage device mapping settings (BlockDeviceMappingsV2)	Describe the *block device mapping setting* regarding block storage that is attached to the virtual server to be started	

Support of the Alarm Function

The alarm setting of the monitoring service specifies a scaling policy as an action to be taken when the value reaches the threshold. You can adjust auto-scaling according to the workload by setting the thresholds for alarms to call different scaling policies.


Tip

You can register multiple actions for one alarm. Notifications are available by email when scale out or scale in occurs.

Example of Setting Auto-Scaling

An example of a stack definition that describes conditions for auto-scaling is shown below. In this example, the conditions are set as described below.

- The following are defined for the scaling group:
  - Specification of a load balancer in order to distribute the load on the auto-scaled virtual servers (balance the traffic load to port 80 (HTTP))
  - Specification of the maximum number of virtual servers as three
  - Specification of the minimum number of virtual servers as two
  - Specification of the subnet to which auto-scaled virtual servers are connected
  - Specification of the startup configuration (specification of values by using variables that are declared in the parameters section)
- The following policies are defined as the scaling policies:
  - web_server_scaleout_policy: Specification of "ChangeInCapacity" for the scaling type, and setting of one (+1) for the number of virtual servers to be added when the alarm is raised
  - web_server_scalein_policy: Specification of "ChangeInCapacity" for the scaling type, and setting of one (-1) for the number of virtual servers to be deleted when the alarm is raised
- The following two alarms are defined as the alarms:
  - cpu_alarm_high: Application of web_server_scaleout_policy when a CPU usage rate of higher than 50% that continues for one minute or more is detected
  - cpu_alarm_low: Application of web_server_scalein_policy when a CPU usage rate of 15% or lower that continues for one minute or more is detected

Sample stack definition:

```
heat_template_version: 2013-05-23

description:
  Autoscaling sample template.

parameters:

  az:
    type: string
    default: jp-east-1a
  param_image_id:
    type: string
# ImageID of CentOS 6.5 64bit
    default: 46676b95-fc6a-4ad2-b6aa-320ab4288d6f
  param_flavor:
    type: string
    default: standard

  key_name:
    type: string
    description: SSH key to connect to the servers
    default: sample_keypair00
  autoscale_security_group:
    type: comma_delimited_list
    default: sample_SG00


resources:

  web_server_group:
    type: FCX::AutoScaling::AutoScalingGroup
    properties:
      AvailabilityZones: [{get_param: az}]
      LaunchConfigurationName: {get_resource: launch_config}
      MinSize: '2'
      MaxSize: '3'
# subnet ID for auto-scaling
      VPCZoneIdentifier: [38e6630f-3257-4ee8-a006-f6d57ceaa2c3]
      LoadBalancerNames:
      - {get_resource: fj_elb}

  launch_config:
    type: FCX::AutoScaling::LaunchConfiguration
    properties:
      ImageId: { get_param: param_image_id }
      InstanceType: { get_param: param_flavor }
      KeyName: {get_param: key_name}
      SecurityGroups: {get_param: autoscale_security_group}
      BlockDeviceMappingsV2: [{source_type: 'image', destination_type:
 'volume', boot_index: '0', device_name: '/dev/vda',  volume_size: '40',
 uuid: {get_param: param_image_id}, delete_on_termination: true}]

  fj_elb:
    type: FCX::ExpandableLoadBalancer::LoadBalancer
    properties:
# subnet ID for auto-scaling
      Subnets: [38e6630f-3257-4ee8-a006-f6d57ceaa2c3]
      Listeners:
      - {LoadBalancerPort: '80', InstancePort: '80',
        Protocol: 'HTTP', InstanceProtocol: 'HTTP' }
      HealthCheck: {Target: 'HTTP:80/healthcheck', HealthyThreshold: '3',
                    UnhealthyThreshold: '5', Interval: '30', Timeout: '5'}
      Version: 2014-09-30
      Scheme: internal
      LoadBalancerName: fjsampleELBaz1

  web_server_scaleout_policy:
    type: FCX::AutoScaling::ScalingPolicy
```

```
    properties:
      AdjustmentType: ChangeInCapacity
      AutoScalingGroupName: {get_resource: web_server_group}
      Cooldown: '60'
      ScalingAdjustment: '1'

  web_server_scalein_policy:
    type: FCX::AutoScaling::ScalingPolicy
    properties:
      AdjustmentType: ChangeInCapacity
      AutoScalingGroupName: {get_resource: web_server_group}
      Cooldown: '60'
      ScalingAdjustment: '-1'

  cpu_alarm_high:
    type: OS::Ceilometer::Alarm
    properties:
      description: Scale-out if the average CPU > 50% for 1 minute
      meter_name: fcx.compute.cpu_util
      statistic: avg
      period: '60'
      evaluation_periods: '1'
      threshold: '50'
      alarm_actions:
      - {get_attr: [web_server_scaleout_policy, AlarmUrl]}
      matching_metadata: {'metadata.user_metadata.groupname': {get_resource:
'web_server_group'}}
      comparison_operator: gt

  cpu_alarm_low:
    type: OS::Ceilometer::Alarm
    properties:
      description: Scale-in if the average CPU < 15% for 1 minute
      meter_name: fcx.compute.cpu_util
      statistic: avg
      period: '60'
      evaluation_periods: '1'
      threshold: '15'
      alarm_actions:
      - {get_attr: [web_server_scalein_policy, AlarmUrl]}
      matching_metadata: {'metadata.user_metadata.groupname': {get_resource:
'web_server_group'}}
      comparison_operator: lt
```

2.1.6.2 Health Check Function

Following auto-scaling, this function detects abnormality on the scaled-out virtual servers and starts recovery automatically.

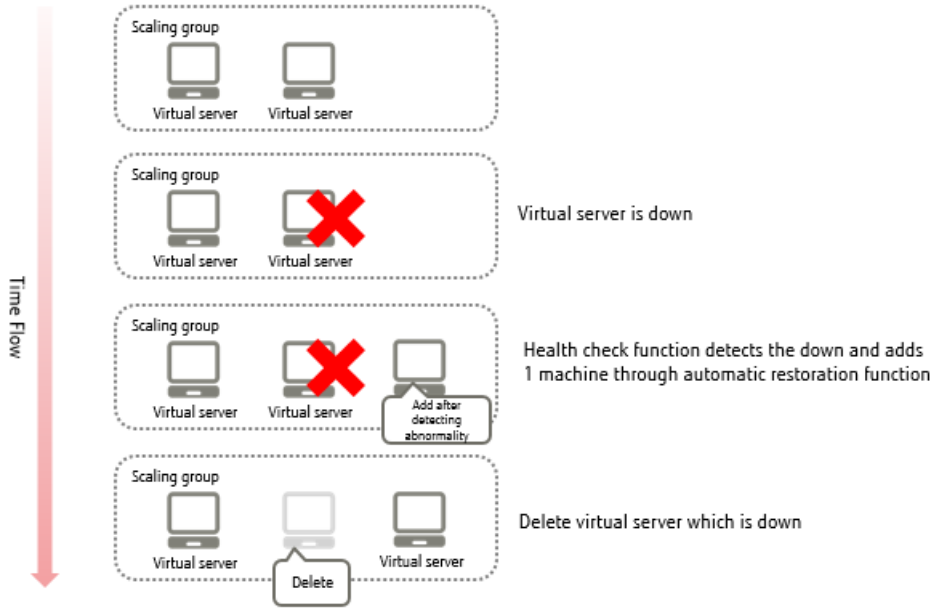
Functions Included

You can use the following functions for scaled-out virtual servers:

- Health check function, for scaled-out virtual servers

- Auto recovery function, for virtual servers where abnormality was detected by the health check function

  Figure 15: Operation of the Auto Recovery Function on a Virtual Server Where Abnormality Was Detected by the Health Check Function



Auto Recovery Function for a Virtual Server Where Abnormality Was Detected by the Health Check Function

To use this function, add the following items to the appropriate categories of the settings for auto-scaling:

- Settings for the health check function for scaling groups

  Table 24: List of Scaling Group Settings Regarding the Health Check Function

Item	Description	Required
Cool down period (Cooldown)	Specify this setting, in seconds, to prevent the next scaling operation from taking place immediately after the previous scaling operation was completed (*Formula for Estimating Cool Down Period after Auto-Scaling* on page 221) Important When you use this function in conjunction with auto-scaling based on the monitoring of thresholds, such as CPU usage rate, specify this field instead of specifying the cool down period in the scaling policies.	
Maximum number (MaxSize)	Specify the maximum number of virtual servers to be scaled Tip When you use this function, we recommend that you specify a value which is the minimum number plus 1 or more. Note When the maximum number of virtual servers have been created and abnormality is detected on a virtual server, the addition of virtual	Yes

Item	Description	Required
	servers is not carried out, and only the deletion of virtual servers is carried out.	
Minimum number (MinSize)	Specify the minimum number of virtual servers to be scaled  Tip This is the number of servers that are created initially when the stack is registered.	Yes
Health check type (HealthCheckType)	Supports only "ELB." When you specify the load balancer name and this parameter, the auto recovery function for virtual servers where abnormality was detected by the health check function is enabled.	
Time to wait before starting health check (HealthCheckGracePeriod)	Specify this setting, in seconds, to wait for a period after scaled-out virtual servers are started before starting the health check	

- Settings for scaling policies

Table 25: List of Scaling Policy Settings Regarding the Health Check Function

Item	Description	Required
Scaling type (AdjustmentType)	Specify "ChangeInCapacity"	Yes
Cool down period (Cooldown)	Specify this setting, in seconds, to prevent the next scaling operation from taking place immediately after the previous scaling operation was completed (*Formula for Estimating Cool Down Period after Auto-Scaling* on page 221)	
Scaling value (ScalingAdjustment)	Specify the scaling adjustment value  Note Specify a value which is lower than the maximum number that is set for the scaling group, and within the range of 1 to 5.	Yes

- Settings for alarms

Table 26: List of Alarm Settings Regarding the Health Check Function

Item	Description	Required
Action (alarm_actions)	Specify the URL of the action required in order to delete the virtual server that is experiencing abnormality	
Comparison operator (comparison_operator)	Specify comparison operators that are used with threshold values • "le": Less than or equal • "ge": Greater than or equal • "eq": Equal to • "lt": Less than • "gt": Greater than	

Item	Description	Required
	• "ne": Not equal	
Number of times that constitutes alarm status (evaluation_periods)	Specify the number of times the threshold condition must be reached in order to be considered to be in alarm status	
Meta data search condition (matching_metadata)	Specify "{'resource_id': <load balancer name>}"	
Meter name (meter_name)	Specify "fcx.loadbalancing.instance.unhealthy"	Yes
Period that constitutes alarm status (period)	Specify how long of a period (sec) the threshold must be exceeded in order to be considered to be in alarm status	
Statistic type (statistic)	Specify "min" to count the virtual servers that are experiencing abnormality	
Threshold (threshold)	Specify the threshold for the number of virtual servers that are experiencing abnormality. Specify the same value as the scaling adjustment value (ScalingAdjustment) that you specified in the scaling policy settings. If you specify two or more, auto recovery will not be performed until the number of servers experiencing abnormality reaches or exceeds the number.	Yes
Repeat actions (repeat_actions)	Specify "true" to use the health check function	

Note

The number of virtual servers that will be added after execution of the auto recovery function is determined based on the scaling policy that is set for the scaling group that is using the health check function. When auto recovery is performed, the number of virtual servers is determined according to the following formula:

```
(Number of virtual servers running in the scaling group before auto
 recovery is performed) + (number of virtual servers that will be
 added according to the setting in the scaling policy) - (number of
 virtual servers which were determined to be experiencing abnormality
 by the health check)
```

Note

As a result of deleting virtual servers where an abnormality was detected, the number of virtual servers may fall below the minimum number of virtual servers that is set in the scaling group. In this case, virtual servers will be added automatically until the number of virtual servers reaches the minimum number required.

2.1.6.3 Auto-Scaling Scheduler Function

With this function you can control the execution of scale out by specifying the date and time for execution. You can use the schedule function to automate scaling out for a predictable increase of workload, such as the busy season of your business.

This function provides the method to execute the REST API at the specified time.

Tip

You can realize the operation of an increased number of virtual servers in the busy season by describing the REST API to control the scaling policy in order to increase the number.

Registering a Schedule

Set the following items to register a schedule.

Table 27: List of Settings for a Schedule

Item	Description	Required
Schedule name	From 1 to 64 alphanumeric characters can be used. Important The name must be unique among all projects in the same region.	Yes
HTTP methods	Specify the HTTP methods for the REST API that is to be executed. Only the POST method can be specified	Yes
URL	Specify the URL for the signal to be the target of the schedule.	Yes
Date and time to execute	Specify the date and time at which to execute the REST API	Yes
Project ID	Specify ID of the project in which the schedule is to be executed	Yes

Note The format for the URL for the signal is as follows:

```
http://<orchestration API end point>/v1/<project ID>/stacks/<stack
 name>/<stack ID>/resources/<scaling policy name>/signal
```

Note Specify the execution date and time in the five fields of the cron-command-compliant format that is shown below. (Fields are separated by single-byte spaces)

```
minute hour dom month dow
```

Table 28: Description of Each Field and Values That Can Be Specified

Field	Values That Can Be Specified
Minute	From 0 to 59, * specifies every minute
Hour	From 0 to 23, * specifies every hour
Day of Month	From 1 to 31, * specifies every day
Month	From 1 to 12, or from jan to dec, * specifies every month
Day of Week	From 0 to 7 (0 and 7 specify Sunday) or from sun to sat, * specifies all days

Important Confirm that a valid trust token exists, on which the user to whom you delegate the execution of schedules, the trusted user (orchestration user), the project ID, and the role (System Owner role) match. Check the trust token by using the following API, which is explained in the section about IDs and access management in API Reference Manual.

1. Check the trust token (list)

Confirm that a trust token that meets the following conditions exists.

Table 29: Conditions for Confirming Existence of Trust Token

Item	Value
trustor_user_id	uuid of the user to whom you delegate the task
expires_at	null
trustee_user_id	1f708e1376784e529a7b09eb5ff1a5fc
project_id	uuid of the project where the stack exists

2. Confirm the role on the trust token

Table 30: Conditions for Confirming Role on Trust Token

Item	Value
trust_id	uuid of the trust token that meets the conditions above
role_id	0739580a550d4a0f9c78f45a9f038c05

Deleting a Schedule

You can delete a schedule that is already registered.

2.1.7 Image

2.1.7.1 Managing Virtual Server Images

Create and manage images of created virtual servers.

Creating an Image

You can create virtual server images of virtual servers that you have created.


Note

First, you must shut down the virtual server of which you will create an image.


Note

For additional storage, relocate a storage volume by detaching and reattaching it, or use a function such as the snapshot function to duplicate the storage volume.


Warning

Perform the following steps before creating an image of a virtual server whose OS is CentOS, Ubuntu, or Red Hat Enterprise Linux. If the following settings remain in the image, network communication with the virtual server created from that image will not be possible.

1. Disable write_net_rules

```
/lib/udev/rules.d/75-persistent-net-generator.rules
```

Comment out (add a # to the beginning of the line) the following line in the above file.

```
DRIVERS=="?*", IMPORT{program}="write_net_rules"
```

2. Delete /etc/udev/rules.d/70-persistent-net.rules

```
rm -f /etc/udev/rules.d/70-persistent-net.rules
```

Warning

Perform the *procedure to run Sysprep on Windows OS* before you create an image of a virtual server whose OS is Windows.

Table 31: Creating an Image (List of Items That Can Be Set)

Item	Description	Required
Image Name	Specify a name that identifies the image	
Disk Format	Specify "raw"	
Container Format	Specify "bare"	
Force Option	Specify "true"	

Acquiring/Updating Image Metadata

You can check and edit metadata that is assigned to virtual server images that have been created.

Table 32: Modifying Image Metadata (List of Items That Can Be Set)

Item	Description	Required
Image Name	Specify a name that identifies the image	
Metadata	Specify the metadata for the image in Key-Value format	

Deleting a Image

Delete images that have been registered.

2.1.7.2 Sharing Virtual Server Images

Virtual server images from the created virtual servers are shared between different projects.

Functions Included

The following operations are available for virtual server images that have been created.

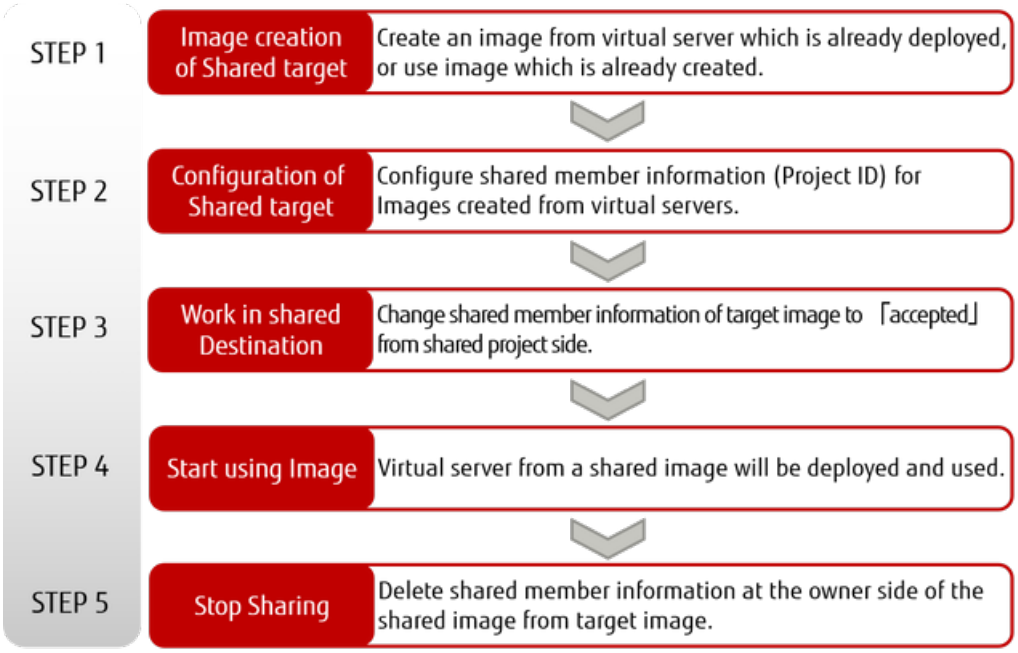
- Creating shared member information
- Modifying shared member information
- Deleting shared member information

Tip

Set the visibility for a virtual server image to be shared to "private."

How to Use This Service

Figure 16: Procedure from Starting to Stopping the Sharing of a Virtual Server Image



Points to Note

- When stopping the sharing of a virtual server image, be sure to delete the shared member information from the target image.

2.1.7.3 Procedure to Run Sysprep on Windows OS

In order to create an image of your Windows virtual server by using the image archiving service, you must run Sysprep on the Windows virtual server of which you intend to create an image. The procedure is shown below for reference.

About this task

For details on Sysprep, refer to the Microsoft TechNet website (*https://technet.microsoft.com/en-us/*), and be sure you fully understand Sysprep before you actually run it.

Warning Fujitsu does not take responsibility for any problems that are caused by running Sysprep. The customer takes full responsibility for carrying out this procedure.

Tip We recommend that you take snapshots or create backups of system block storage before you start the procedure to run Sysprep.

Procedure

1. Taking a Snapshot

   Take a snapshot of the system storage using the snapshot function.

   Tip Perform the subsequent procedures on Windows OS.

2. Allowing remote access to the computer

   Remote access to the computer is allowed by default. If remote access is not allowed, change the setting to allow it by following the procedure below.

   - For Windows Server 2012 SE

From the Start menu, click [Control Panel] > [System and Security] > [Allow remote access], and then select [Allow remote connections to this computer (L)] in the dialog box.

- For Windows Server 2008 SE or EE

  From the Start menu, click [Control Panel] > [System and Security] > [Allow remote access], and then select [Allow connections from computers running any version of Remote Desktop (less secure) (L)] or [Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure) (N)] in the dialog box.

3. Editing of the sysprep response file

   Edit the sysprep response file as necessary. The sysprep response file is stored in the following location on the virtual server:

   - For Windows Server 2012 SE

     C:\Windows\System32\Sysprep\ans_w2k12.xml
   - For Windows Server 2008 SE

     C:\Windows\System32\Sysprep\ans_w2k8_se.xml
   - For Windows Server 2008 EE

     C:\Windows\System32\Sysprep\ans_w2k8_ee.xml

4. Deleting the log file

   Delete the Cloudbase-init log file. You can find the path to the Cloudbase-init log file at the following locations on a Windows OS:

   - Settings for the log file in cloudbase-init-unattend

     <Location where Cloudbase-init is intalled>\conf\cloudbase-init-unattend.conf

     - Location where the log exists: logdir in the [DEFAULT] section
     - Log file: logfile in the [DEFAULT] section

     
     Tip

     Normally, the path to the log file is as follows:

     C:\Program Files (x86)\Cloudbase Solutions\Cloudbase-Init\log\cloudbase-init-unattend.log

   - Settings for the log file in cloudbase-init

     <Location where Cloudbase-init is installed>\conf\cloudbase-init.conf

     - Location where the log exists: logdir in the [DEFAULT] section
     - Log file: logfile in the [DEFAULT] section

     
     Tip

     Normally, the path to the log file is as follows:

     C:\Program Files (x86)\Cloudbase Solutions\Cloudbase-Init\log\cloudbase-init.log

5. Deleting the registry information

   Delete the Cloudbase-init registry information. Delete the following path by using the registry editor:

   - For 64-bit Windows OS

     HKEY_LOCAL_MACHINE\Software\Wow6432Node\Cloudbase Solutions\Cloudbase-Init

6. Starting the command prompt

   - For Windows Server 2012 SE

On the desktop screen, right-click the [Windows] logo button and click [Command Prompt (Admin)].

- For Windows Server 2008 SE or EE

  1. Click the [Start] button.
  2. Click [All Programs] > [Accessories].
  3. Right-click [Command Prompt] and click [Run as administrator].

7. Moving the current directory

   Execute the following command to move the current directory:

   ```
   cd C:\Windows\System32\sysprep\
   ```

8. Running of sysprep

   Run the following batch file:

   ```
   vsysprep.bat
   ```

Results

The virtual server will be shut down automatically after a few minutes. Make sure that the status of the virtual server is "SHUTOFF" before you create an image.

After creating an image, follow the procedure below on the virtual server:

1. Restoring a snapshot

   Restore the snapshot of the system storage using the snapshot function.

2. Starting virtual servers

   Start the virtual server.

2.1.8 Virtual Server Import Service

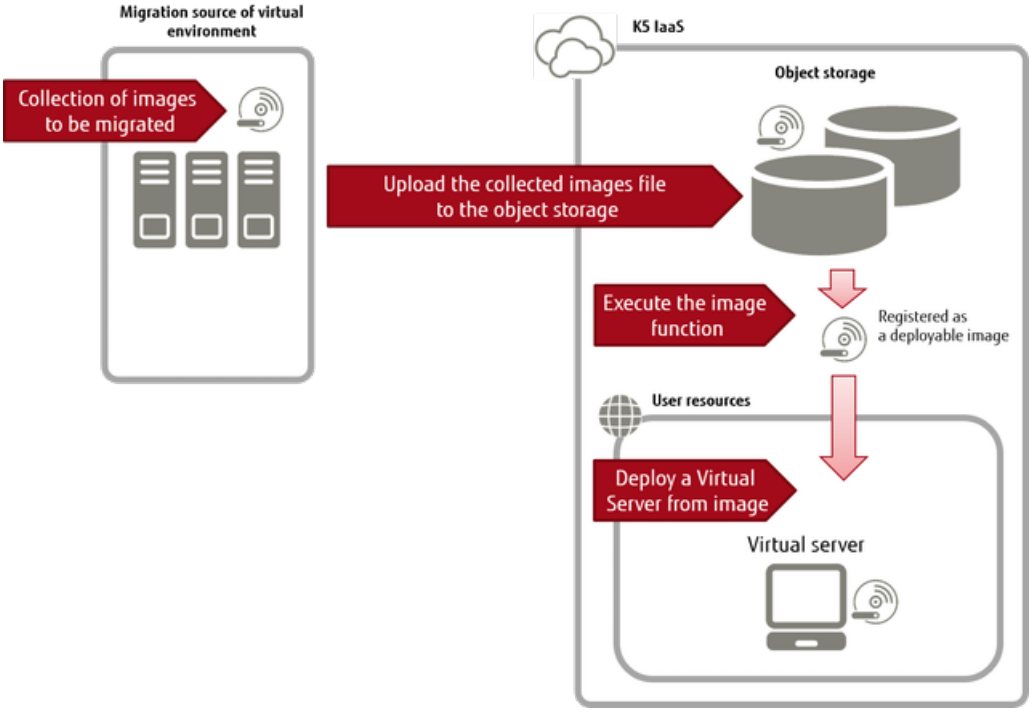
2.1.8.1 Overview of Functions

2.1.8.1.1 Virtual Server Import Service

This service is used to migrate a virtual server running on your on-premises virtual environment to K5 IaaS. This function allows you to register image files that you have captured as image files that can be used in K5 IaaS.

A diagram that shows how this service is used is shown below.

Figure 17: Using the Virtual Server Import Service



Supported Migration Source Virtual Environments

A list of supported migration source virtual environments is shown below.

Table 33: List of Migration Source Virtual Environments

Virtual Environment	Product and Version
VMware	• ESX/ESXi 6.0 5.5 5.1 5.0 • vCenter Server 6.0 5.5 5.1 5.0
FUJITSU Software ServerView Resource Orchestrator[1]	• ServerView Resource Orchestrator v3.1 v3.2

Note

BIOS startup is supported in any virtual environment. UEFI startup is not supported.

Supported Migration Source Guest OS

A list of supported migration source guest OS is shown below.

Table 34: List of Migration Source Guest OS

OS Type	Supported OS
Windows	• Windows Server 2008 SE R2 64bit (English Version) • Windows Server 2008 EE R2 64bit (English Version) • Windows Server 2012 SE 64bit (English Version) • Windows Server 2012 SE R2 64bit (English Version)

[1] Hypervisors are supported for VMware only.

OS Type	Supported OS
Linux	• CentOS 6.5 64bit • Ubuntu 14.04 LTS 64bit

Limitations on Migration Source Virtual Server Configurations

- Disk Configuration

  Only system storage that is on the startup disk can be imported. Additional storage cannot be imported.
- Network Interface

  At least one network interface must be defined.

Handling of Licenses

The handling of licenses by type of imported OS is shown below.

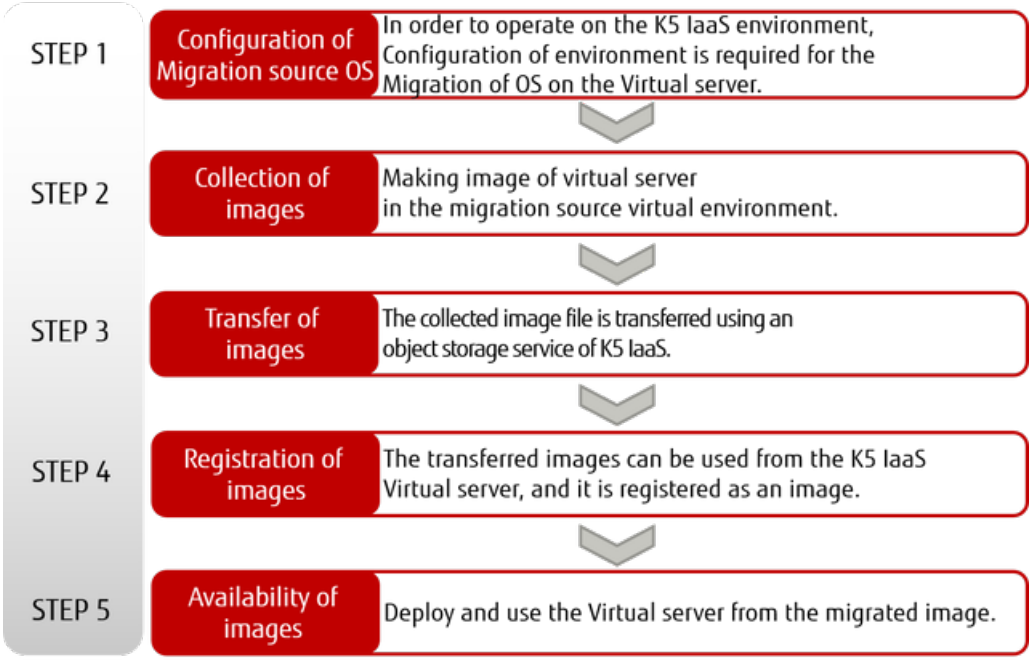
Table 35: Handling of Licenses by Type of Imported OS

Type of Imported OS	Handling of License
Windows	When you import a virtual server, the license is automatically changed to an SPLA license. After importing, perform KMS activation.
Linux	• CentOS The started virtual server is shown in the usage details as "OS Provision Service, CentOS." • Ubuntu The started virtual server is shown in the usage details as "OS Provision Service, Ubuntu."

How to Use This Service

Perform the following operations to import the image on the migration source virtual server to K5 IaaS.

Figure 18: How to Use the Virtual Server Import Service



2.1.8.2 Procedure on the Migration Source Virtual Environment

2.1.8.2.1 Migrating an Image of Windows Server OS

The following explains the steps required for migrating an image to a K5 IaaS environment when the OS of the virtual server that is operating in the virtual environment is Windows Server.

Before you begin

The procedure explained below applies when the OS that you are migrating is one of the following versions:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

About this task

Perform the following steps in the virtual environment and on the OS of the virtual server from which you are migrating the image.

Important

- Use the console of the virtual environment for operation. Do not connect from outside, such as by using remote desktop, because doing so affects the network settings.

  Example: Start and operate the virtual machine console from VMware vSphere Client.
- Be sure to make a backup before you change the settings of the virtual environment from which you are migrating so that you can restore it.

Procedure

1. Uninstallation of VMware Tools

If VMware Tools is installed on the virtual server that you intend to migrate, uninstall it. For the uninstallation procedure, refer to the VMware Tools manuals.

2. Enabling of remote desktop
   Enable remote desktop in order to connect to the virtual server by using remote desktop after the image is migrated to the K5 IaaS environment. For the procedure to enable the setting, check topics related to the Remote Desktop settings in Windows Help and Support.
   After enabling the setting, confirm that you can log in to the server by using remote desktop.

3. Setting of network (DHCP connection)
   Start [Network connection] from the desktop and check the DHCP settings.

   Note: When the settings are configured so that DHCP is not used (the fixed IP address is used), the settings are changed after importing the image so that DHCP is used.

4. Disabling of the firewall function
   Open the [Windows Firewall] settings from Control Panel, and disable the firewall.

   Note: If a third-party firewall product is installed, disable the firewall according to the procedure in the product manual.

5. Downloading of agent software
   Download the installation module for the agent software from the portal site. After the download finishes, transfer it to a directory on the virtual server.

6. Installing of agent software
   Install the agent software according to the procedure that is described in *Installing Agent Software for Migration* on page 47.

2.1.8.2.2 Installing Agent Software for Migration

Install the agent software that automatically configures the settings required in order for the OS which you are migrating to operate on K5 IaaS. The software also sets up the related software automatically.

Before you begin

- Confirm that the steps that are described in *Migrating an Image of Windows Server OS* on page 46 have been completed.
- Download the installation package (TransportAgent.msi) from the distribution site.

About this task

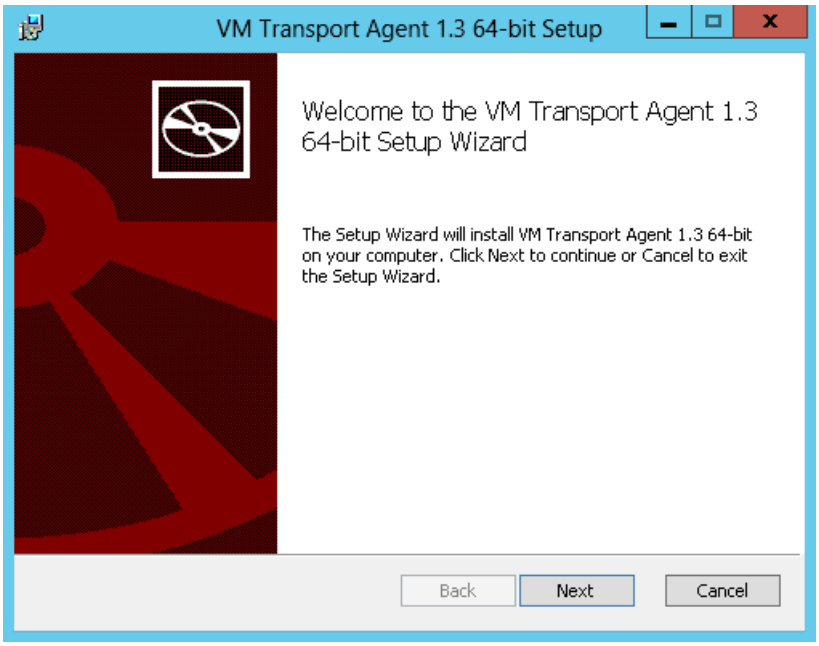
Install the software according to the procedure described below when the OS that you are migrating is one of the following:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

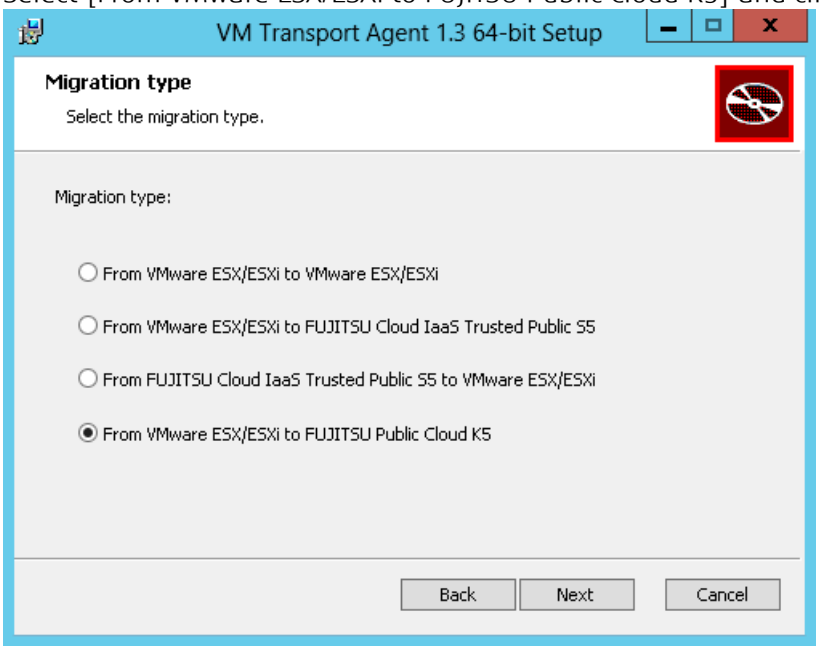
Procedure

1. Installation of VM Transport Agent
   Execute TransportAgent.msi.

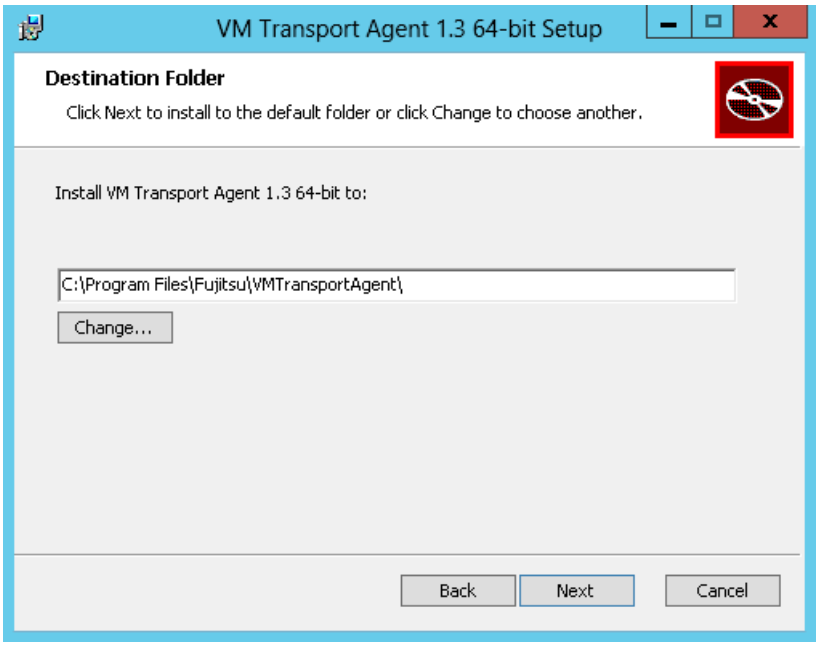
2. Starting of an installation
   When the setup wizard appears, click the [Next] button.



3. Selection of the combination of migration source and destination
   Select [From VMware ESX/ESXi to FUJITSU Public Cloud K5] and click the [Next] button.



4. Selection of the installation destination for the agent software
   Click the [Change] button to select the installation destination, and then click the [Next] button.

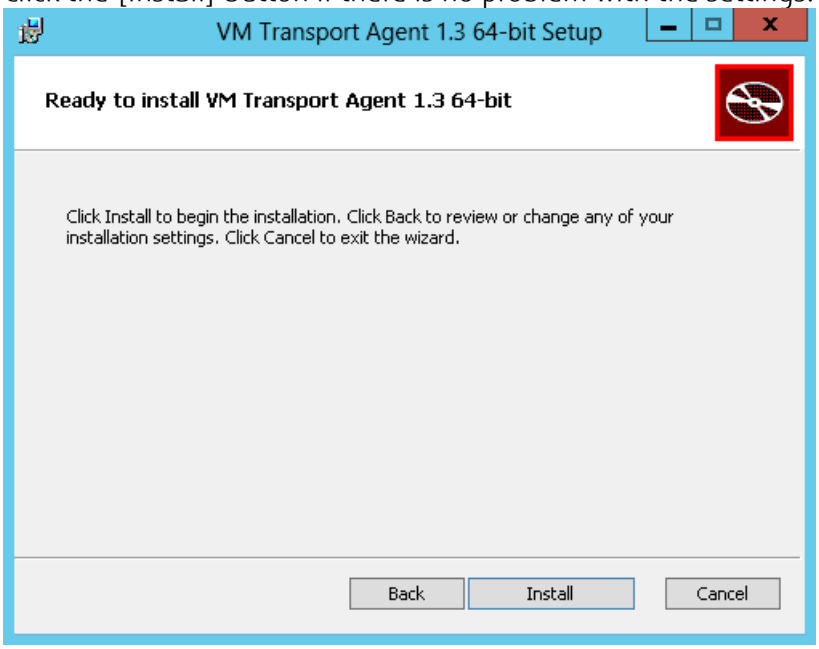


Tip

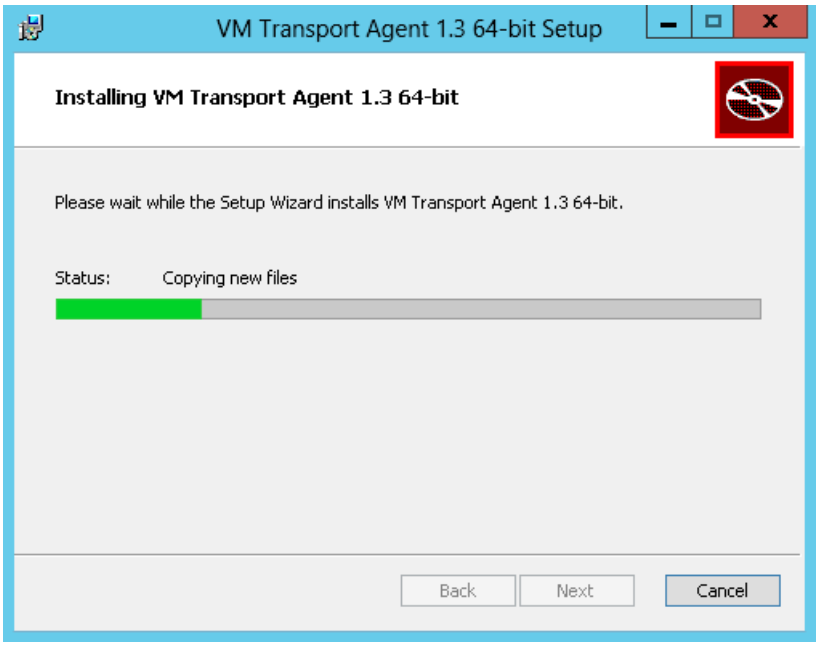
The default installation destination is as shown below. If you do not need to change it, click the [Next] button.

```
C:\Program Files\Fujitsu\VMTransportAgent
```

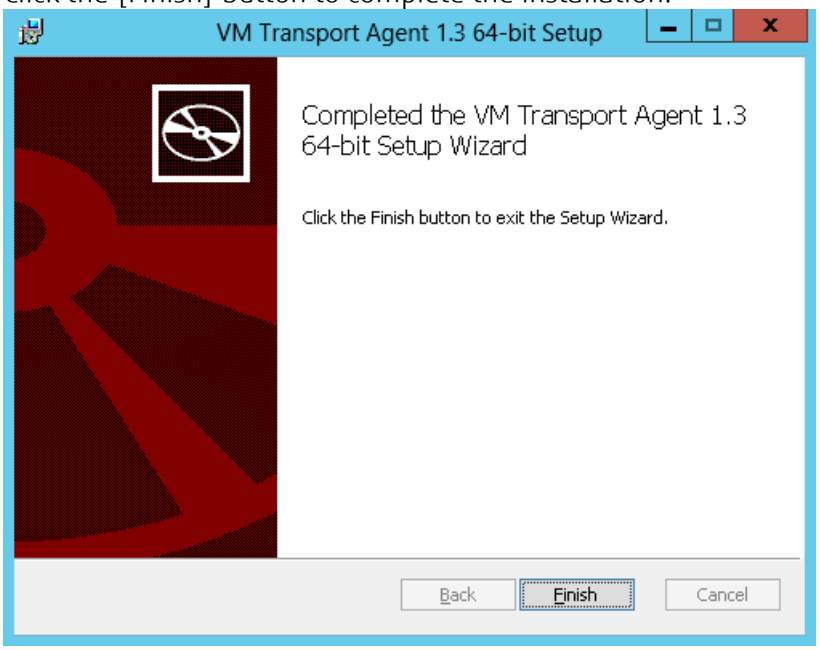
5. Checking of the final confirmation screen
   Click the [Install] button if there is no problem with the settings.



The screen that shows the progress appears. Wait a while for the installation to be completed.



6. Checking of the completion screen
   Click the [Finish] button to complete the installation.



2.1.8.2.3 Migrating an Image of CentOS

The following explains the steps required for migrating an image to a K5 IaaS environment when the OS of the virtual server that is operating in the migration source virtual environment is CentOS.

About this task

Perform the following steps in the virtual environment and on the OS of the virtual server from which you are migrating the image.

Important

- Use the console of the virtual environment for operation. Do not connect from outside, such as by using remote desktop, because doing so affects the network settings.

  Example: Start and operate the virtual machine console from VMware vSphere Client.

- Be sure to make a backup before you change the settings of the virtual environment from which you are migrating so that you can restore it.

Procedure

1. Uninstallation of VMware Tools
   If VMware Tools is installed on the virtual server that you intend to migrate, uninstall it.

```
# vmware-uninstall-tools.pl
```

2. Installation of an SSH server
   Install an SSH server by following the procedure below.

```
# yum install openssh-server
# chkconfig sshd on
# /etc/init.d/sshd restart
```

3. Installation of cloud-init
   Install cloud-init by following the procedure below.
   1. Installation of cloud-init

```
# yum install http://download.fedoraproject.org/pub/epel/6/x86_64/epel-
release-6-8.noarch.rpm
# yum -y install cloud-init.noarch cloud-utils-gworpart
# yum -y install dracut-modules-growroot
```

   2. Editing of cloud-init configuration file "/etc/cloud/cloud.cfg"
      An example configuration is shown below.

```
# cat /etc/cloud/cloud.cfg
users:
 - default

disable_root: 1
ssh_pwauth: 1

locale_configfile: /etc/sysconfig/i18n
mount_default_fields: [~, ~, 'auto', 'defaults,nofail', '0', '2' ]
resize_rootfs_tmp: /dev
ssh_deletekeys: 0
ssh_genkeytypes: ~
syslog_fix_perms: ~
hostname: localhost.localdomain
manage_etc_hosts: cloud-init_host
user: vmimport

cloud_init_modules:
 - migrator
 - bootcmd
 - write-files
<--omitted-->
system_info:
  default_user:
    name: centos
    lock_passwd: true
    gecos: Cloud User
    groups: [wheel, adm]
    sudo: ["ALL=(ALL) NOPASSWD:ALL"]
    shell: /bin/bash
  distro: rhel
  paths:
    cloud_dir: /var/lib/cloud
    templates_dir: /etc/cloud/templates
  ssh_svcname: sshd
# vim:syntax=yaml
```

Example of setting the host:

- hostname: <host name>
- manage_etc_hosts: cloud-init_host

Example of specifying a general user name that connects via SSH:

- user: <user name>

Important The user password that you specified for cloud-init and the created key pair are set for this user when you create a virtual server.

4. Setting of the output destination of the boot log
   Change the setting so that the Kernel can write the boot logs to the ttyS0 device.
   1. Save /boot/grub.grub.conf.
      ```
      # cp -p /boot/grub/grub.conf /root/grub.conf.bak
      ```
   2. Edit /boot/grub/grub.conf and add the definition that enables the Kernel to write boot logs to the ttyS0 device to grub.
      ```
      # vi /boot/grub/grub.conf
      ```
      Add or change the serial definition as shown below:
      ```
      (Before) kernel /vmlinuz<string omitted> rhgb quiet
      (After) kernel /vmlinuz<string omitted> console=tty0
       console=ttyS0,115200n8
      ```
5. Setting of network (DHCP connection)

   Tip To connect a virtual server via a network using DHCP after importing the image, configure the settings shown below. When the fixed IP address is set, the same IP address is used for startup after importing the image.

   1. Enable NetworkManager.
      ```
      # yum -y install NetworkManager
      # chkconfig NetworkManager on
      # /etc/rc.d/init.d/NetworkManager start
      ```
   2. Check the setting of /etc/sysconfig/network-scripts/ifcfg-<network interface name>.
      ```
      BOOTPROTO=dhcp
      ```
   3. Restart the network.
      ```
      # /etc/rc.d/init.d/NetworkManager restart
      ```
6. Deletion of the MAC address
   1. Save the configuration file. If no configuration file exists, this operation is not required.
      ```
      # cp /etc/udev/rules.d/70-persistent-net.rules \
      /etc/udev/rules.d/70-persistent-net.rules.bak
      # cp /lib/udev/rules.d/75-persistent-net-generator.rules \
      /lib/udev/rules.d/75-persistent-net-generator.rules.bak
      ```
   2. Delete the MAC address information.
      ```
      # rm /etc/udev/rules.d/70-persistent-net.rules
      # rm /lib/udev/rules.d/75-persistent-net-generator.rules
      # touch /etc/udev/rules.d/70-persistent-net.rules
      # touch /lib/udev/rules.d/75-persistent-net-generator.rules
      ```
   3. Delete the MAC address information (the line that starts with "HWADDR=") from /etc/sysconfig/network-scripts/ifcfg-<network interface name>.
   4. Restart the OS.
      ```
      # reboot
      ```

7. Disabling of the firewall
   Disable the iptables service and the ipchains service.

```
# service ipchains stop
# service iptables stop
# chkconfig ipchains off
# chkconfig iptables off
```

2.1.8.2.4 Migrating an Image of Ubuntu

The following explains the steps required for migrating an image to a K5 IaaS environment when the OS of the virtual server that is operating in the migration source virtual environment is Ubuntu.

About this task

Perform the following steps in the virtual environment and on the OS of the virtual server from which you are migrating the image.

Important

- Use the console of the virtual environment for operation. Do not connect from outside, such as by using remote desktop, because doing so affects the network settings.
  Example: Start and operate the virtual machine console from VMware vSphere Client.
- Be sure to make a backup before you change the settings of the virtual environment from which you are migrating so that you can restore it.

Procedure

1. Uninstallation of VMware Tools
   If VMware Tools is installed on the virtual server that you intend to migrate, uninstall it.

```
# vmware-uninstall-tools.pl
```

2. Installation of an SSH server
   Install an SSH server by following the procedure below.

```
# apt-get install openssh-server
```

   Tip
   Configure the SSH service settings as necessary.

3. Installation of cloud-init
   Install cloud-init by following the procedure below.
   1. Installation of cloud-init

```
# apt-get install cloud-init
# dpkg-reconfigure cloud-init
```

   2. Editing of cloud-init configuration file "/etc/cloud/cloud.cfg"
      An example configuration is shown below.

```
# cat /etc/cloud/cloud.cfg
users:
 - default

disable_root: 1
ssh_pwauth: 1

locale_configfile: /etc/sysconfig/i18n
mount_default_fields: [~, ~, 'auto', 'defaults,nofail', '0', '2' ]
resize_rootfs_tmp: /dev
ssh_deletekeys: 0
```

```
ssh_genkeytypes: ~
syslog_fix_perms: ~
hostname: localhost.localdomain
manage_etc_hosts: cloud-init_host
user: vmimport

cloud_init_modules:
 - migrator
 - bootcmd
 - write-files
<--omitted-->
system_info:
  default_user:
    name: centos
    lock_passwd: true
    gecos: Cloud User
    groups: [wheel, adm]
    sudo: ["ALL=(ALL) NOPASSWD:ALL"]
    shell: /bin/bash
  distro: rhel
  paths:
    cloud_dir: /var/lib/cloud
    templates_dir: /etc/cloud/templates
  ssh_svcname: sshd
# vim:syntax=yaml
```

Example of setting the host:

- hostname: <host name>
- manage_etc_hosts: cloud-init_host

Example of specifying a general user name that connects via SSH:

- user: <user name>

Important The user password that you specified for cloud-init and the created key pair are set for this user when you create a virtual server.

4. Setting of the output destination of the boot log
   Change the setting so that the Kernel can write the boot logs to the ttyS0 device.
   1. Save /etc/default/grub and add the definition that enables the Kernel to write boot logs to the ttyS0 device to grub.

      ```
      # cp -p /etc/default/grub /root/grub.bak
      # vi /etc/default/grub
      ```

      Add the following settings to grub:

      ```
      GRUB_CMDLINE_LINUX_DEFAULT=console=tty0 console=ttyS0,115200
      GRUB_TERMINAL=console
      ```

   2. Execute the following command to apply the settings:

      ```
      # update-grub
      ```

5. Setting of network (DHCP connection)

Tip To connect a virtual server via a network using DHCP after importing the image, configure the settings shown below. When the fixed IP address is set, the same IP address is used for startup after importing the image.

Using the network interface definition defined in /etc/network/interfaces, configure the settings so that the DHCP connection is used.

```
# vim /etc/network/interfaces
```

An example of setting eth0 is as follows:

```
auto eth0
```

```
iface eth0 inet dhcp
```

6. Deletion of the MAC address
   1. Save the configuration file. If no configuration file exists, this operation is not required.

```
# cp /etc/udev/rules.d/70-persistent-net.rules \
/etc/udev/rules.d/70-persistent-net.rules.bak
# cp /lib/udev/rules.d/75-persistent-net-generator.rules \
/lib/udev/rules.d/75-persistent-net-generator.rules.bak
```

   2. Delete the MAC address information.

```
# rm /etc/udev/rules.d/70-persistent-net.rules
# rm /lib/udev/rules.d/75-persistent-net-generator.rules
# touch /etc/udev/rules.d/70-persistent-net.rules
# touch /lib/udev/rules.d/75-persistent-net-generator.rules
```

7. Disabling of the firewall
   1. Install iptables-persistent with the following command:

```
# apt-get install iptables-persistent
```

   2. Initialize the iptables settings and make the settings persistent.

```
# iptables -F
# /etc/init.d/iptables-persistent save
```

2.1.8.2.5 Capturing Images of a Virtual Server

You can capture virtual server images in ovf-format from the migration source environment.

About this task

For the procedure to capture images in ovf-format, refer to the manuals for the migration source environment.

Example: Taking an image by using VMware vSphere Client

1. Select the VM of which you intend to capture an image.
2. Select [File] > [Export] > [Export OVF Template] from the menu.
3. Specify the export destination directory and press the [OK] button to capture an image.

2.1.8.3 Procedure on the K5 IaaS Environment

2.1.8.3.1 Transferring Images

Register images that you have captured in the migration source virtual environment as K5 IaaS images by using the object storage service.

Before you begin

In order to use the object storage service, you need a user who can create and delete containers or objects.

About this task

Create a container to store images using the object storage service, and then upload the image files that you have taken.

Note: When the size of the image files is 5 GB or less, you can perform a batch upload. When the size is greater than 5 GB, you must divide and upload them separately.

Warning: Be aware that usage charges for the amount that has been uploaded are applied from the point when the upload to object storage started.

2.1.8.3.2 Virtual Server Image Import Function

This function allows you to register image files stored in object storage as K5 IaaS virtual server images so that they are available to create servers.

Virtual Server Image Registration Function

To request the registration of a virtual server image, specify the following information.

Table 36: Registering a Virtual Server Image (List of Items)

Item	Description	Required
Image Name	Specify an image name to identify the image in the image archiving service.	Yes
Image File Storage Location	Specify part of the object storage URL where you uploaded the virtual server image as a source, in the following format: "/v1/AUTH_<Project ID>/<Container Name>/<Object Name>"	Yes
Checksum Value	Specify the SHA1 checksum value if you choose to verify the source virtual server image file. If you do not specify this value, the system does not carry out the checksum verification.	
Image ID	Specify the uuid for the image to be registered.	Yes
Minimum Memory Space	Specify the minimum memory space (MB) required in order to use the image.	
Minimum Disk Space	Specify the minimum disk space (GB) required in order to use the image.	
Metadata for the Image	Specify the metadata (Key-Value) for the image.	
Image Conversion Flag	Specify "true" • For Windows images The drivers that are necessary for operation after the transition are embedded, and the conversion from the "vmdk" format to the "raw" format is performed. • For Linux images The conversion from the "vmdk" format to the "raw" format only is performed.	Yes
OS Type	Specify one of the following OS types for the source virtual server image: • win2008R2SE: Windows Server 2008 R2 SE • win2008R2EE: Windows Server 2008 R2 EE • win2012SE: Windows Server 2012 SE • win2012R2SE: Windows Server 2012 R2 SE • centos: CentOS • ubuntu: Ubuntu	Yes
User Name	Specify the name of the user who imports the image.	Yes
Password	Specify the password (a Base64-encoded character string) for the user who imports the image.	Yes

Item	Description	Required
Domain Name	Specify the name of the domain to which the user who imports the image belongs.	Yes

Acquiring the Registration Status List for Virtual Server Images

You can acquire a list of the image registration processes in progress within a domain. The results are listed starting with the most recent requests to the system. You can also acquire basic status information for each registration process.

- succeeded

  This status indicates that the image was registered successfully.
- failed

  This status indicates that the image registration process failed.
- processing

  This status indicates that the image registration process is in progress.
- queued

  This status indicates that the image registration request is waiting for the process to begin.

Virtual Server Image Registration Status

You can acquire the following detailed information regarding the operation status for one virtual server image registration process:

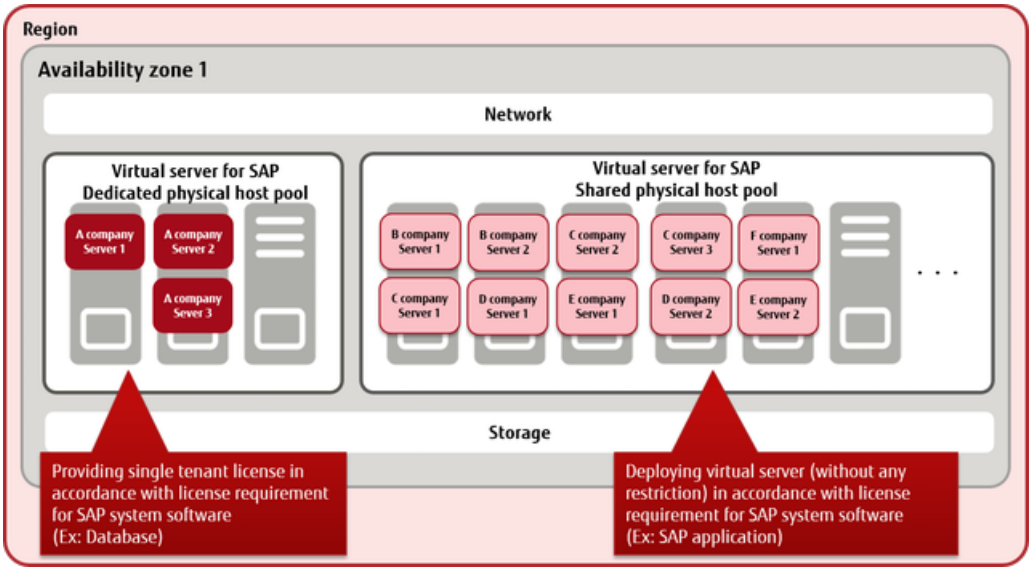
- Status information of the registration process
- Progress rate (from 0 to 100%)
- Settings you configured when registering the image

2.2 Services for SAP

2.2.1 Virtual Server for SAP

2.2.1.1 Virtual Server for SAP

Virtual servers can be created for SAP applications as virtual environments supported by SAP.



Functions Included

- Compute
  - Enabling/disabling of an environment

    Specify a project and availability zone, and set whether to enable the virtual server for SAP environment.

    Note: If you disable this environment, you must delete all created virtual servers for SAP, images, and network resources in the project.
  - A virtual server for SAP
    - Creating/deleting a virtual server for SAP
    - Startup/termination of a virtual server for SAP
    - Restarting a virtual server for SAP
    - Acquiring information for a virtual server for SAP
  - OS provision service

    You can use the images provided in *List of Available OS* to create a virtual server for SAP.

    You can use Windows Server Update Services and Windows Activation (KMS), which are common network services.
  - Software support service

    The available functions and charge systems comply with [Compute] > [Standard Services] > [Software Support Services].
  - Auto recovery of a virtual server

Note: You cannot select whether to enable or disable the auto recovery function. (Always enabled)

- Image management

  You can create private images from an existing virtual server for SAP and delete private images that have been created.

  Tip: A private image that has been created can be used only in the activity zone in which it was created.

  You can choose to disclose a created private image either within the project or within the domain.

- Storage
  - System storage

    System storage is provided as a system region for starting the OS. The size of system storage is fixed according to the OS image available in the OS provision service.

    Table 37: List of System Storage Sizes

OS Type	OS Provided	Size
Windows	Windows Server 2012 SE R2 64bit English Version	80 GB
	Windows Server 2008 SE R2 SP1 64bit English Version	80 GB

  - Additional storage

    Additional storage is provided for data archiving.

    Table 38: List of Limiting Values Related to Additional Storage

Item	Limiting Values
Size of Additional Storage	0.1 - 2,048 GB
Number of Storage Systems	1 - 55

  - Snapshot function

    You can take, restore, and delete snapshots for existing virtual servers for SAP.

    Note: If you delete a virtual server for SAP in which snapshots are taken, the snapshots will also be deleted.

    Table 39: List of Limiting Values Related to Snapshots

Item	Limiting Values
Number of Snapshots Taken	Maximum 10 generations

- Network
  - Network resource management

    For virtual networks and subnets that have been created, you can assign and release network resources for the virtual server for the SAP environment.

Tip You can use private IP addresses and gateway IP addresses by assigning network resources.

- Adding/deleting ports

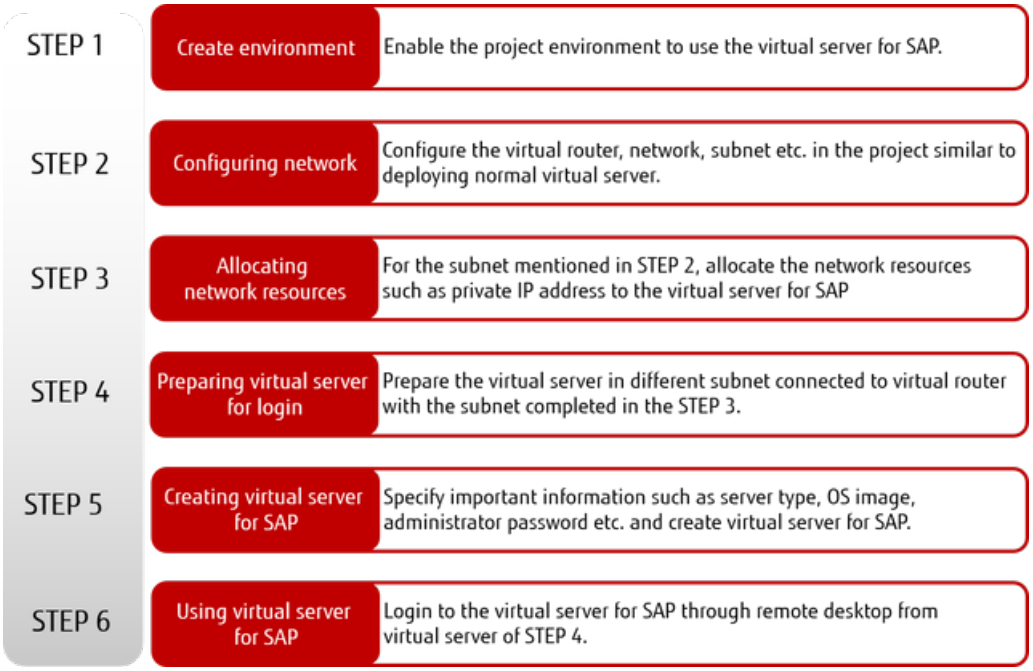
Note
- If you add or delete ports, also modify the network adapter settings on the OS as appropriate.
- You cannot use security group functions.

Table 40: List of Limiting Values Related to Adding a Port

Item	Limiting Values
Number of Ports that Can Be Added	1 - 9

How to Use This Service

Figure 19: How to Use a Virtual Server for SAP



Points to Note

- An auto-scaling function is not provided.
- A virtual server import function is not provided.
- You cannot assign a global IP address to a virtual server for SAP. Use the service via a normal virtual server.
- Only a virtual server for SAP can be created in a subnet that has had its settings modified for use with a virtual server for SAP.
- A virtual server for SAP that has been created cannot be targeted for a load balancer to distribute the load.
- This server cannot be created with a template.
- If a physical host in a data center experiences an abnormality, the virtual server for SAP running on the target host is automatically migrated. During this migration, access to the target virtual server and business applications will be temporarily suspended.

2.2.1.2 Preparing the Virtual Server for SAP Environment

To start operations on a virtual server for SAP, you must prepare a connection with the existing virtual resource environment.

Before creating a virtual server for SAP, make the preparations as shown below.

Enabling of an Environment

Enable an environment for a project in which you want to use a virtual server for SAP.

Table 41: Enabling of an Environment (List of Items That Can Be Set)

Item	Description	Required
Project ID	Specify the existing project ID	Yes
Availability Zone Name	Specify the name of the availability zone where the environment will be enabled Tip If this setting is omitted, all the availability zone names will be set.	

Note Do not enable and disable the same project at the same time.

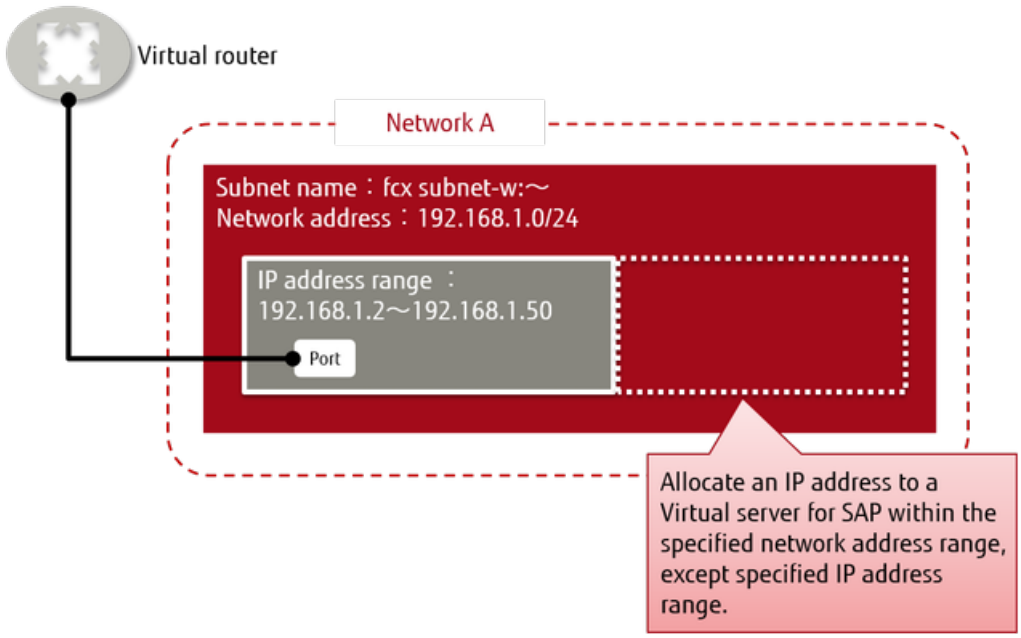
Building a Virtual Network

To connect the environment for a virtual server for SAP with an existing virtual resource environment, create the following virtual network resources:

- Virtual router
- Virtual network and a subnet that belongs to the virtual network

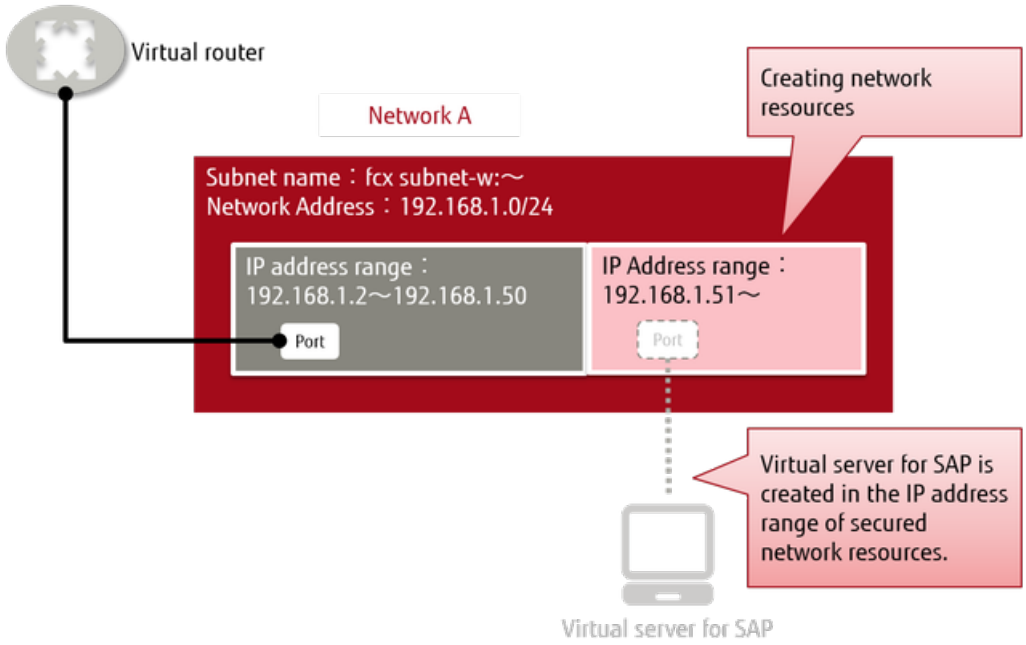
Important The subnet that will be created for a virtual server for SAP must meet the following conditions:

- No normal virtual servers are connected
- The subnet name starts with the prefix "fcx_subnet-w:"
- The CIDR range specified as network addresses is larger than the specification of the IP address range (secure a network resource range described later)



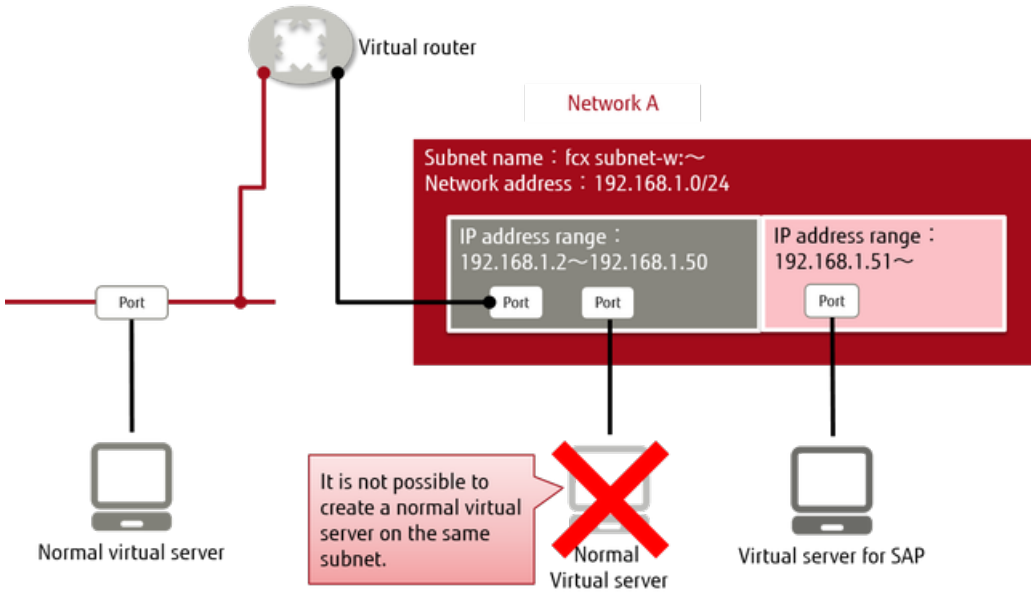
Creating a Network Resource

Create a network resource by assigning the subnet that has been created for the virtual server for SAP environment.



Preparing a Virtual Server Used for Logging In

When network resources are assigned to the subnet created for the virtual server for SAP environment, you cannot create normal virtual servers on the same subnet. Therefore, prepare a different network and a subnet, and connect to them via a virtual router, as shown below.



2.2.1.3 Creating/Deleting a Virtual Server for SAP

You can create a virtual server for SAP according to the requirements and purposes of the SAP applications by selecting from several types. You can also delete virtual servers for SAP that are in use at any time if they are no longer needed.

Creating a Virtual Server for SAP

You can create a virtual server for SAP from one of the image types explained below.

- Standard

  Image provided in *Virtual Server for SAP (List of Available OS)*
- Created by the user

  Image prepared through *management of the virtual server image*

To create a virtual server for SAP, specify the following items.

Tip The virtual server enters a "shut-down" state immediately after it is created. Start the virtual server for SAP as necessary.

Table 42: Creating a Virtual Server for SAP (List of Items That Can Be Set)

Item	Description	Required
Server Name	Specify the name of the virtual server for SAP. The characters that you specify must meet the following specifications: • Use an alphanumeric character as the first character • Use alphanumeric characters, hyphens (-), underscores (_), and periods (.) • Specify at least 1 character, and no more than 64 characters	Yes
Server Type Name	Specify the type name from available server types	Yes
Image Name	Use either of the following image names: • Image provided in the list of available OS • Private image that has been created	Yes

Item	Description	Required
Port Identification Number	Specify a number that identifies the port that will be assigned to the virtual server for SAP. The number that you specify must meet the following specifications: • Enter "0" when you create a virtual server • Enter a number in the range from 0 to 9 • Enter a sequence number, which must be an integer that starts with 0	Yes
Network Resource ID	Specify the ID of the created network resource	Yes
IP Address	Specify an IP address that will be assigned to a virtual server for SAP. You can specify an IP address in either of the following two ways: • Directly specify one in xxx.xxx.xxx.xxx format • Automatic (The system automatically assigns one from the IP address range specified for the network resource.)	
Computer Name	Specify the name of the computer The characters that you specify must meet the following specifications: • Use alphanumeric characters and hyphens (-) • Specify at least 1 character, and no more than 15 characters • You cannot specify numeric characters only  Tip If this setting is omitted, the server name will be applied.	
Administrator Password	Specify the password for the OS Administrator The characters that you specify must meet the following specifications: • Use alphanumeric characters and single-byte symbols • Specify at least 1 character, and no more than 128 characters	Yes
Port Identification Number for which the DNS Server Is Configured	Specify a port identification number for which the DNS server information is configured	Yes
IP Address of the DNS Server	When the OS is Windows, set the IP address specified as the DNS server address of the network adapter  Note If this setting is omitted, the IP address of the DNS server will not be set.	
Availability Zone Name	Specify the name of the availability zone where the virtual server for SAP will be created  Tip If this setting is omitted, the default availability zone will be used as the creation destination.	
Creation in the Dedicated Area	Specify "true" to create a virtual server for SAP in the dedicated area	

Item	Description	Required
	Note To specify "true," you must submit an application to the service provider.	

Deleting a Virtual Server for SAP

Delete a virtual server for SAP that is no longer needed.

Note Stop (turn off) the virtual server for SAP before deleting it.

Available Server Types

A list of virtual server types that can be used with virtual servers for SAP is shown below:

Table 43: List of Types of Virtual Server for SAP (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
WS-4	4	16
WS-8	8	32
WS-16	16	64

Tip The performance for each virtual CPU is equal to 2.6 GHz.

List of Available OS

Table 44: List of Available OS of Virtual Server for SAP

OS Type	OS Provided
Windows	• Windows Server 2012 SE R2 64bit English Version • Windows Server 2008 SE R2 SP1 64bit English Version

2.2.1.4 Operations on a Virtual Server for SAP

You can carry out the following operations on a virtual server for SAP that has been created in the SAP on Windows environment.

Startup/Termination of a Virtual Server for SAP

Start a created virtual server for SAP from a shut-down state or shut down a server from an operating state. As a shut-down method, you can select either [Shut down forcibly] or [Do not shut down forcibly].

Note OS waiting does not occur during startup of virtual servers.

Restarting a Virtual Server for SAP

Restart a running virtual server for SAP. As a restart method, you can select either [Restart forcibly] or [Do not restart forcibly].

Acquiring Information of Virtual Server for SAP

You can obtain detailed information of a created virtual server for SAP. In addition to the items specified when a server is created, you can obtain the following information:

Table 45: Virtual Server for SAP (List of Items That Can Be Acquired)

Item	Description
Resource ID	You can obtain the resource ID of the target virtual server for SAP
Power Status	You can obtain the power status information of the virtual server for SAP. The status is indicated by one of the following character strings: • on • off • unknown
Snapshot Generations	You can obtain the number of snapshot generations taken for the virtual server for SAP
Snapshot Date and Time	You can obtain the date and time of when snapshots were taken for the virtual server for SAP
Snapshot ID	You can obtain the ID of the snapshots taken for the virtual server for SAP
Storage Name	You can obtain the name of the storage system attached to the virtual server for SAP
Storage ID	You can obtain the ID of the storage system attached to the virtual server for SAP
Storage Capacity	You can obtain the capacity (in GB) of the storage system attached to the virtual server for SAP
Device Path	You can obtain the path or identifier of the device connected to the storage system
MAC Address	You can obtain the MAC address of the network interface connected to the virtual server for SAP
Status	You can obtain the status information of the virtual server for SAP. The status is indicated by one of the following character strings: • normal • warning • stop • error • fatal • unknown

Attaching Additional Storage

To attach additional storage, specify the following items:

Table 46: Attaching Additional Storage (List of Items That Can Be Set)

Item	Description	Required
Index Number	Specify the number of the additional storage system. The number that you specify must meet the following specifications: • Enter an integer from 1 to 55 • Enter a sequence number, which must start with 1	
Size	Specify the storage size. The value that you specify must meet the following specifications: • Specify in the range from 0.1 to 2048 • You can specify a number with up to one decimal place • Specify a value in GB Note: You can specify a value in an increment of 0.1 GB, but the size may not be recognized as specified, depending on the OS specifications.	Yes

Deleting Additional Storage

When additional storage is no longer necessary, delete it on a virtual server for SAP.

Note: Stop (turn off) the virtual server for SAP before deleting the target.

Tip: The index number of a storage system that is not deleted remains the same.

Adding a Port

To add a port, specify the following items.

Note: To add a port, you must delete all the snapshots taken on the target virtual server for SAP.

Tip: When a port is added successfully, the system assigns the smallest unused number equal to or above 0 to the port as its identification number.

Table 47: Adding a Port (List of Items That Can Be Set)

Item	Description	Required
Type	Specify "nic"	Yes
Network Resource ID	Specify the ID of the network resource to which the port will be connected	Yes
IP Address	Specify an IP address that will be assigned to the port If this setting is omitted, an IP address is automatically assigned from the IP address	

Item	Description	Required
	Tip range available to the network resource that will be connected.	

Deleting a Port

Delete a port that is no longer necessary by specifying the port identification number.

Note To delete a port, you must delete all the snapshots taken on the target virtual server for SAP.

Table 48: Deleting a Port (List of Items That Can Be Set)

Item	Description	Required
Type	Specify "nic"	Yes
Port Identification Number	Specify the identification number of the port that will be deleted	Yes

Tip The identification number of a port that is not deleted remains the same.

Creation of a snapshot

To take a snapshot, specify the following items on a created virtual server for SAP.

Tip Snapshots are taken on a per-virtual server basis.

Note You can take snapshots while a virtual server for SAP is running, but doing so may affect normal operation of the virtual server for SAP. We recommend that you take snapshots after a virtual server for SAP is stopped.

Table 49: Taking a Snapshot (List of Items That Can Be Set)

Item	Description	Required
Type	Specify "snapshot"	Yes
Resource ID of Virtual Server for SAP	Specify the resource ID of the target virtual server for SAP of which you want to take a snapshot	Yes

Deleting a Snapshot

Delete a snapshot that is no longer necessary.

Table 50: Deleting a Snapshot (List of Items That Can Be Set)

Item	Description	Required
Type	Specify "snapshot"	Yes
Resource ID of Snapshot	Specify the resource ID of the snapshot that will be deleted	Yes

Restoring from a Snapshot

Restore a virtual server for SAP from a snapshot.

Restoration is carried out on a per-virtual server basis.

Tip

Table 51: Restoring from a Snapshot (List of Items That Can Be Set)

Item	Description	Required
Resource ID of Snapshot	Specify the resource ID of the snapshot that will be restored	Yes

2.2.1.5 Managing Virtual Server for SAP Images

You can create private images in an existing virtual server for SAP, and delete private images that have been created.

Private images that have been created can be shared within a contract number (domain) or within a project and used for creation of a new virtual server for SAP.

Creating a Private Image

To create a private image from the virtual server for SAP that was created, specify the following items.

Table 52: Creating a Private Image (List of Items That Can Be Set)

Item	Description	Required
Name	Specify a name for the private image. The characters that you specify must meet the following specifications: • Specify 32 characters or less using alphanumeric characters and underscores (_) • Use an alphabetic character as the first character • The name must be unique within the project	Yes
Type	Specify "cloning"	Yes
Resource ID of Virtual Server for SAP	Specify the resource ID of the target virtual server for SAP for which you want to create a private image	Yes
Comment	Specify a comment character string to be set to the private image. The characters that you specify must meet the following specifications: • Specify double-byte and single-byte characters other than percent signs (%), backslashes (\), double quotation marks ("), and newline characters • Specify at least 1 character, and no more than 96 characters	

Note

- As a target for which you want to create a private image, specify a virtual server for SAP that has started up before.
- When creating a private image, stop the target virtual server for SAP in advance.

Deleting a Private Image that Has Been Created

Delete a private image that is no longer needed by specifying its name.

Changing the Disclosure Range of a Created Private Image

You can change the disclosure range of a private image that has been created to either of the following:

- domain: Within a contract number (domain)
- private: Only within this project

Tip

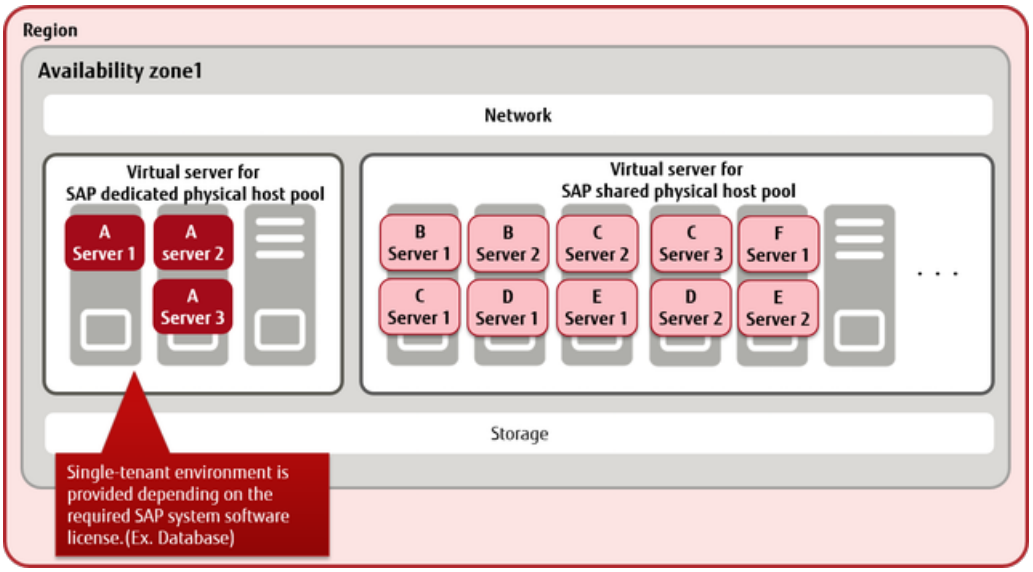
The conditions for changing the disclosure range are as follows:

- The private image of this project is disclosed in the contract number (domain)
- The private image is disclosed only within the project

2.2.2 Dedicated Virtual Server for SAP

2.2.2.1 Dedicated Virtual Server for SAP

A pool for dedicated physical hosts is secured for each contract number (domain), and a function that can create a dedicated virtual server for SAP is provided.



This server can be used for environments that must be separate from other users (single tenant), as required in the license for SAP system software.

Important

Networks and storage are shared in a virtual server for SAP environment.

Available Server Types for Dedicated Virtual Servers for SAP

The types of virtual servers for SAP that are available as dedicated virtual servers are the same as normal virtual servers for SAP.

Table 53: List of Types of Virtual Server for SAP (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
WS-4	4	16

Type Name	Number of Virtual CPUs	Memory (GB)
WS-8	8	32
WS-16	16	64

Physical Host Pool Menu

- Basic Set: "2 server configuration"

  A physical host pool that includes a failover host is secured as the creation destination for the virtual server for SAP that is dedicated to the customer. You must apply for one Basic Set for each availability zone in which you will run a dedicated virtual server for SAP.
- Additional Servers

  Use additional servers when you want to increase the capacity of available dedicated virtual servers for SAP, such as when there is increased demand on the system. Physical hosts are added to the same pool where the Basic Set is currently used.

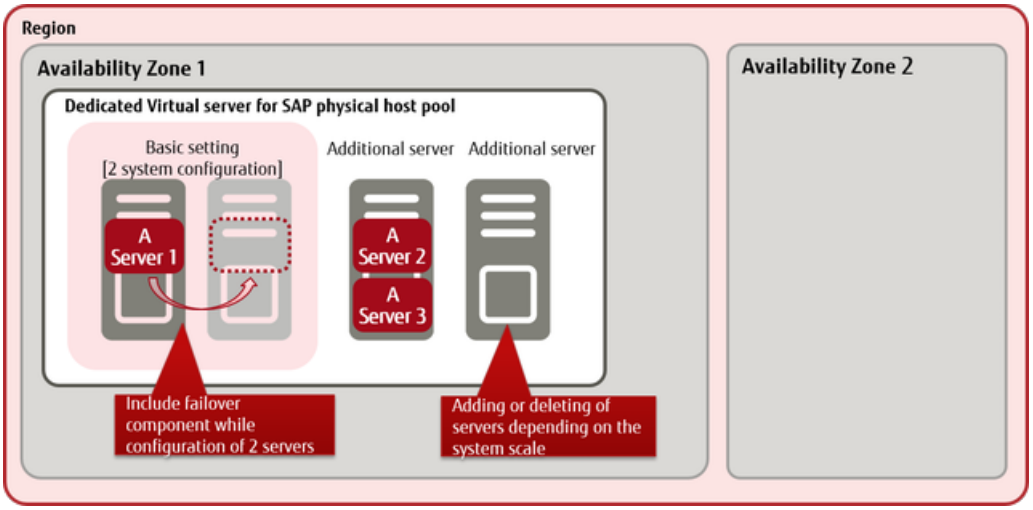
Tip

The following amounts of resources can be used by each physical host.

Number of Virtual CPUs	42
Memory	245 GB

Confirm the type of dedicated virtual server for SAP, and then estimate the number of dedicated virtual servers that can be created.

Figure 20: Using the Physical Host Pool Menu



Functions Included

When you create a virtual server for SAP, you have the option of creating it in a physical host pool that you have secured. Dedicated virtual servers for SAP that you create can be managed by project, in the same way as a normal virtual server for SAP.

Note

- You cannot specify a specific physical host in a pool to create a virtual server.
- The physical host pool for a single contract number is shared between all projects.

Dedicated virtual servers for SAP that you have created have the same Compute function as normal virtual servers for SAP.

- Compute

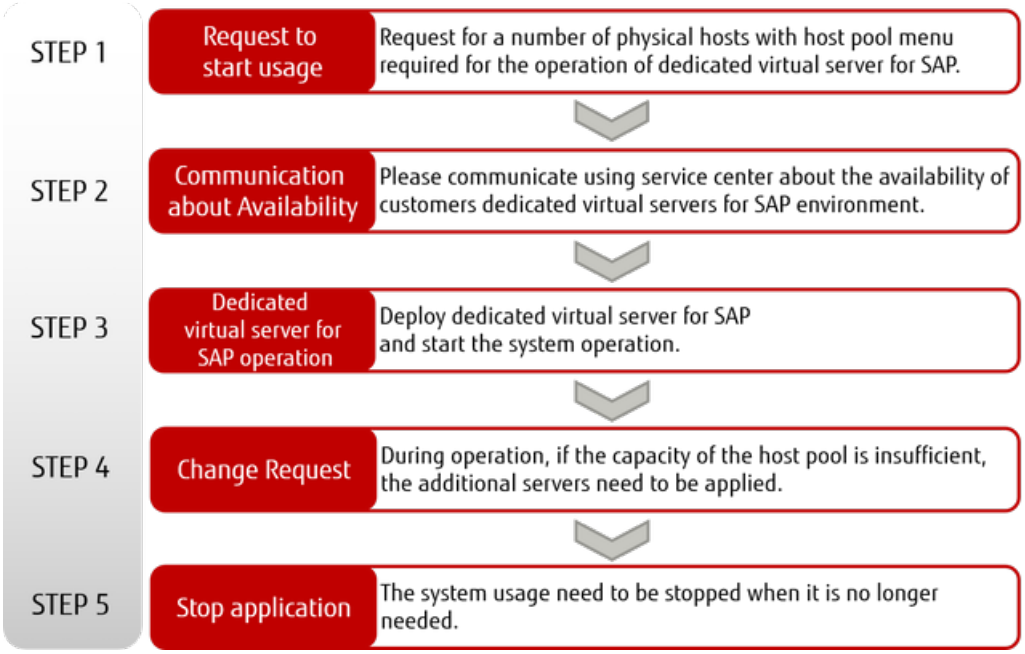
- Enabling/disabling of an Environment
- Dedicated virtual server for SAP
  - Creating/deleting a dedicated virtual server for SAP
  - Startup/termination of a dedicated virtual server for SAP
  - Restarting a dedicated virtual server for SAP
  - Acquiring information for a dedicated virtual server for SAP
- OS Provision Service
- Software Support Service
- Auto recovery of a virtual server
- Image management

For shared storage and networks, you can use the same functions as a normal virtual server for SAP.

- Storage
- Network

How to Use This Service

Figure 21: How to Use a Dedicated Virtual Server for SAP



Points to Note

- A contract number (domain) can have only one physical host pool where dedicated virtual servers for SAP are created.
- Although the physical host is a dedicated machine, it is unlikely to improve the performance of any dedicated virtual servers for SAP that are to be created.
- Although the physical host is separate from other users, security is not guaranteed because the network is shared. Use the firewall function to ensure security.

Part 3: Storage

Topics:

With physical storage separated by virtualization technology, K5 IaaS provides a virtual infrastructure that is accessible via the Internet.

3.1 Block Storage

3.1.1 System Storage

When you create a virtual server, select a bootable block storage source as system storage.

Select from the following sources:

- Image

  Create block storage from an image (such as an OS image provided by Fujitsu or an image created by the user from a virtual server) and attach it to the virtual server.

  Table 54: OS Image and System Storage Size

OS	Size of System Storage Specified
Windows 2008 R2 SP1	80 GB
Windows 2012 R2	80 GB
Windows 2012	80 GB
CentOS 6.5	30 GB
CentOS 7.2	30 GB
Red Hat Enterprise Linux 6.5	40 GB
Red Hat Enterprise Linux 7.2	40 GB
Ubuntu 14.04 LTS	Specify 3 GB or more

  Note: When you create a virtual server, specify whether to retain the system storage of the server upon deletion.

- Existing block storage

  Attach existing bootable block storage to create a virtual server. When you create block storage, you can select disk performance from the following:

  - Standard (type M1)

  Table 55: List of Disk Types

Type	Purpose
Standard	Use this in the following cases: • When you deploy application data that requires frequent file access (reading and writing) • When you handle a lot of large data files

- Snapshot of existing block storage

  Create a snapshot from existing bootable block storage, and attach the snapshot to create a virtual server.

Block Device Mapping Settings

To attach block storage to a virtual server, you must configure the block device mapping settings. Create new block storage from the specified resource, and attach it as a boot device for the virtual server. Then start the block storage.

Table 56: List of Items That Can Be Set for Device Mapping Settings

Item	Description	Required
Device Name	Specify a device name in "/dev/vd*" format, where * is a character string that is valid as a device name. Example: /dev/vda Note: If "/dev/vda" is assigned to storage other than the system storage, such as when adding storage, you cannot appropriately make a template using Template Builder. We recommend that you specify "/dev/vda" as the device name for system storage.	Yes
Source Type	Specify one of the following: • Image (image) • Existing block storage (volume) • Snapshot of existing block storage (snapshot)	Yes
Connected to	You can specify "volume" only.	Yes
Boot Sequence	Specify the order in which the devices start. To set up the block storage as a boot disk, specify 0.	Yes
Resource ID	Specify the ID of the resource selected in [Source Type].	Yes
Block Storage Size	Specify the size of the block storage that you want to create. Note: The notes for each source type specified are as follows: • When you have specified "image": Make sure that you specify a valid size. • When you have specified "volume": The same block storage size as the source is used. Even if you specify a value, it is ignored. • When you have specified "snapshot": If you omit this field, the size will be the same as the snapshot source block storage.	
Delete Flag	Specify whether block storage that is created when the system is scaled out or when a stack is created will be deleted when the system is scaled in or when the stack is deleted. Specify "true" to delete storage. Note: Even if you specify "true," block storage is not deleted if a snapshot has been taken of it.	

3.1.2 Additional Storage

When you need additional disk space, you can create new block storage and attach it to the virtual server as additional storage.

When you create block storage, you can select disk performance from the following:

- Standard (type M1)

Tip If you detach the additional storage before deleting a virtual server, you can reuse the data in the storage.

Table 57: List of Disk Types

Type	Purpose
Standard	Use this in the following cases: • When you deploy application data that requires frequent file access (reading and writing) • When you handle a lot of large data files

Limiting Values

Table 58: List of Limiting Values Related to Block Storage

Item	Limiting Values
Size of Additional Storage	1 GB or more (specified in GB)
Number of Storage Systems	50 per project per availability zone Note The total number of additional storage systems and additional ports must be within 26 for a single virtual server.
Storage Capacity (total for a project)	5,000 GB per project per availability zone
Number of Snapshots Taken	100 per project per availability zone

3.2 Snapshot

3.2.1 Snapshot Function

Create a snapshot of the block storage currently in use. You can use this function for both system storage and additional storage.

The following functions are provided:

Taking a Snapshot

Take a snapshot of the block storage currently in use on a virtual server. The virtual server can be either running or stopped.

Note

We do not guarantee operation using a snapshot that was taken while the virtual server was online. To ensure that a snapshot serves as backup data, you must take the snapshot while the virtual server is stopped.

Deleting a Snapshot

Specify snapshot data that is no longer needed and delete it.

Restoring from a Snapshot

Attach and reuse snapshot data when you create a virtual server.

Note

To reuse it for system storage, the block storage that you use as the snapshot source must be bootable.

3.3 Object Storage

3.3.1 Object Storage

This is online storage space for dividing the data to be stored into objects (their contents and metadata) and saving the data. Object storage is also referred to as object-based storage.

This service allows you to create containers or register objects on end points that exist in each region in order to store binary data in object storage.

The data saved in each region is distributed among multiple availability zones for storage. This is to ensure that even if one availability zone stops, you can still retrieve data from other availability zones.

3.3.2 Creating/Deleting a Container

Create or delete a container (storage space) for storing objects.

Creating a Container

Specify a region to create a container. Also, specify the items listed below to create a container.

Note

Since containers do not have a layered structure, all the containers are created in a parallel structure.

- *Access Policy Settings* on page 79
- Synchronization Settings
- *Versioning* on page 80
- *Custom Metadata Management* on page 80

Deleting a Container

Delete a container.

Important

Containers with objects cannot be deleted.

Limiting Values

Table 59: List of Limiting Values Related to Object Storage

Item	Limiting Values
Number of Objects per User	Unlimited
Number of Objects per Container	Unlimited
Length of Object Name	1,024 bytes or less
Size of Object that Can Be Uploaded	0 - 5 GB
Length of Object Metadata Name	128 bytes or less
Length of Object Metadata	2,048 bytes or less
Number of Containers per User	Unlimited
Length of Container Name	256 bytes or less

Item	Limiting Values
Uniqueness of Container Name	Unique name in a project
Length of Container Metadata Name	128 bytes or less
Length of Container Metadata	2,048 bytes or less

3.3.3 Container Management

Change the settings of an existing container.

The items that you can change are as follows:

- *Access Policy Settings* on page 79
- Synchronization settings
- *Versioning* on page 80
- Addition of custom metadata

3.3.4 Access Policy Settings

Set access permissions for a container and control the access to the registered objects.

The access policy is based on the following two types of information:

- Policy settings for each user and project

  Table 60: Values that Can Be Specified for Each User and Project

Setting Target	Description Method	Configurable Access Permissions
Project	<Project Name>	• Read permission • Write permission
User	<Project Name>:<User Name>	• Read permission • Write permission

- Policy settings based on the HTTP referer header

  Table 61: Values that Can Be Specified Based on the HTTP Referer Header

Setting Target	Description Method	Configurable Access Permissions
Host	• When permitted .r:<Host Name> • When forbidden .r:-<Host Name>	• Permission to retrieve the object list • Reading permitted without a token • Reading not permitted • Writing not permitted
Domain	• When permitted .r:<Domain Name>, or .r:*.<Domain Name>	• Permission to retrieve the object list • Reading permitted without a token

Setting Target	Description Method	Configurable Access Permissions
	• When forbidden .r:-<Domain Name>, or .r:-*.<Domain Name>	• Reading not permitted • Writing not permitted
All access	• When permitted .r:*	• Permission to retrieve the object list • Reading permitted without a token • Reading not permitted • Writing not permitted

3.3.5 Versioning

If you set a versioning container for the old objects to the existing container, the versioning process for all the objects registered to that container will always be carried out automatically.

When objects are registered to the container targeted for the versioning process, the old objects are renamed according to specific naming conventions and moved to the versioning container. If you delete the most recent object, the preceding object is moved from the versioning container to the original container. The object name is then changed to the original object name.

Starting the Versioning Process

First, create a versioning container. Next, set the versioning container to the container where you want to carry out the versioning process.

Stopping the Versioning Process

Delete the versioning container settings from the container where the versioning process is taking place.

Note

Stopping the versioning process will not delete the versioning container.

Retrieving Objects from Previous Versions

Retrieve objects directly from the versioning container. The objects moved to the versioning container are stored according to the naming conventions described below:

```
[Object Name Length][Object Name]/[Time Stamp]
```

Note

- The object name length contains a zero-padded three-character string in hexadecimal form.
- The time stamp indicates the creation time of the most recent object.

3.3.6 Custom Metadata Management

Users can set or change metadata freely according to the purpose of its use for the container or for the objects used in the object storage service.

Use an HTTP header in the custom metadata settings.

Setting/Changing Metadata

Name and set the metadata for the container or objects you want to use. To change metadata that has already been set, specify an existing metadata name to overwrite it.

- Setting the metadata for the container

  Use the format below to set the metadata.

  ```
  X-Container-Meta-{Metadata Name}: {Metadata Value}
  ```

- Setting the metadata for the objects

  Use the format below to set the metadata.

  ```
  X-Object-Meta-{Metadata Name}: {Metadata Value}
  ```


Note

Object metadata is set anew and the existing metadata is discarded. To keep the existing metadata, the user needs to set it again.

Deleting Metadata

Delete existing metadata. To delete the metadata, enter an empty character string for the existing metadata or use the format below.

- Deleting the metadata of the container

  ```
  X-Remove-Container-Meta-{Metadata Name}: {Metadata Value}
  ```


Tip

When you use the "X-Remove-" format, the specified metadata value is ignored.

3.3.7 Registering/Deleting an Object

This function allows you to specify a created container to store data. When storing data, you can add metadata and handle the data and metadata together as one object.


Important

To store an object, you need to create a container first. You cannot register the object alone.

Registering an Object

Specify data on the local drive, and store it in the container as an object. When registering an object, configure the following items.

Table 62: List of Object Settings

Item	Description	Required
Delete at / Delete after	Select one of the following conditions: • Delete the created objects after a certain period of time • Delete the objects on a specific date and at a specific time	
Custom Metadata	Specify metadata in the formats described in *Custom Metadata Management* on page 80.	

Deleting an Object

Delete objects stored in a container.

Limiting Values

Table 63: List of Limiting Values Related to Object Storage

Item	Limiting Values
Number of Objects per User	Unlimited
Number of Objects per Container	Unlimited
Length of Object Name	1,024 bytes or less
Size of Object that Can Be Uploaded	0 - 5 GB
Length of Object Metadata Name	128 bytes or less
Length of Object Metadata	2,048 bytes or less
Number of Containers per User	Unlimited
Length of Container Name	256 bytes or less
Uniqueness of Container Name	Unique name in a project
Length of Container Metadata Name	128 bytes or less
Length of Container Metadata	2,048 bytes or less

3.3.8 Object Management

This function allows you to retrieve data from an existing object, copy the object, and change the registration information.

Retrieving an Object

Specify an existing object to download the data.

Copying an Object

Specify an existing object to create a copy. New objects are created in the same container.

Changing the Registration Information

Specify an existing object to change the settings.

Table 64: List of Object Settings

Item	Description	Required
Delete at / Delete after	Select one of the following conditions: • Delete the created objects after a certain period of time • Delete the objects on a specific date and at a specific time	

Item	Description	Required
Custom Metadata	Specify metadata in the formats described in *Custom Metadata Management* on page 80.	

3.4 Network Attached Storage (NAS)

3.4.1 NAS Software Image

This function provides the virtual server image that can be created as network attached storage (NAS).

The provided virtual server image and template are as follows:

- Virtual server image with NAS server (GlusterFS) software installed

  Table 65: NAS Software Image Information

Image Name	FJK5-NAS-Vxx Tip "xx" represents the version of the image. This may be updated.
Image OS	CentOS 6.5 64bit (English)

- A template for creating the NAS software image in the user environment

Use the resources described above to build NAS in the user environment.

Important
- The NAS built in the user environment must be operated/maintained by the customer. No support service is provided for the NAS server created with this function.
- Before application, carefully examine the capacity, performance, and maintenance of the function.

3.4.2 How to Use NAS Software Image

This section explains how to configure the settings that are required in order to create an NAS software image in the customer's environment and make it available.

Before you begin

In order to create and use the NAS in your user environment, you must create the following resources within the project to which the user belongs in advance:

- Network and subnet
- Virtual router that connects to the above network

  Note Configure the routing, security group, firewall and other settings correctly so that communication is possible between the subnets in which the NAS server was created.

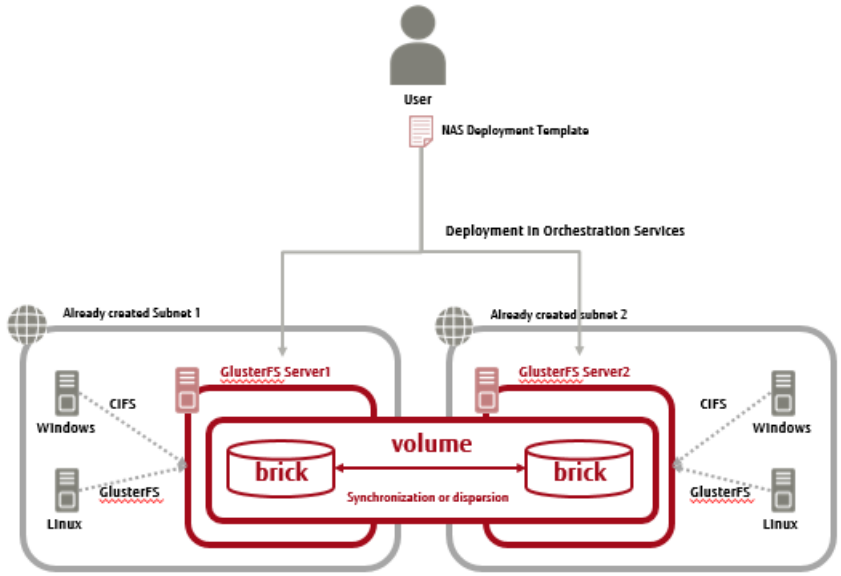
- SSH key pair to be set for the virtual server
- Network connector and connector endpoint

  Tip Required only in configuration across the availability zones.

About this task

This section describes the procedure for the creation of the NAS image using the template provided by the orchestration service and configuring it to be accessed as NAS. The structure of the system that is created is as shown in the figure below.

Figure 22: Creation of a NAS Image by Using the Template



Procedure

1. Prepare the NAS creation template file "glusterfs_nas_YYYYMMDD.yaml."

   Tip: Obtain the NAS creation template file "glusterfs_nas_YYYYMMDD.yaml" from the service provider.

2. Specify the contents of the NAS creation template file for the template parameter for the stack creation function provided by the orchestration service.

   Tip: If the NAS creation template can be accessed by URL, you can specify the URL for the template_url parameter.

   The parameters below are set for the template. Specify the values for the parameters according to the environment in use.

   Table 66: List of NAS Creation Template Parameters

Parameter	Contents Specified (Value)
nas1_name	Virtual server name of GlusterFS Server1
nas1_keypair_name	Key pair name of GlusterFS Server1
nas1_network	Creation destination network ID for GlusterFS Server1
nas1_subnet	Creation destination subnet ID for GlusterFS Server1
nas1_subnet_cidr	Range of addresses of the above subnet (in CIDR notation)
nas1_availability_zone	Creation destination availability zone name of GlusterFS Server1
nas2_name	Virtual server name of GlusterFS Server2
nas2_keypair_name	Key pair name of GlusterFS Server2

Parameter	Contents Specified (Value)
nas2_network	Creation destination network ID for GlusterFS Server2
nas2_subnet	Creation destination subnet ID for GlusterFS Server2
nas2_subnet_cidr	Range of addresses of the above subnet (in CIDR notation)
nas2_availability_zone	Creation destination availability zone name of GlusterFS Server2
flavor	Server type in use by GlusterFS Server1/2
storage_size	Size of the block storage (brick) to be attached to GlusterFS Server1/2  Tip The size that you specify here will be used as the volume for the NAS.  Important As additional storage of the size specified here is attached to both GlusterFS Server1/2, the storage charges are doubled.
storage_type	Selection for a type of block storage • Standard (type M1)
client_cidr	Specify in CIDR notation the network address of the subnet where the client to be permitted access to the NAS is created.  Tip With the NAS creation template, create a security group to be permitted to connect from the network address specified for this parameter and set it on GluesterFS Server1/2.

3. Create a stack.
Wait for creation to be complete, while checking the progress of creation of the stack. When creation of the stack is complete, information such as that below can be referred to as fields that are output.

```
GlusterFS Commands:
  description: gluster Command
  value: |
    * Display the status of peers.
      gluster peer status

    * Display information about all volumes, or the specified volume.
      gluster volume info vol01
      gluster volume status vol01

    * Start the specified volume.
      gluster volume start vol01

    * Stop the specified volume.
      gluster volume stop vol01

    * GlusterFS service Logs and locations
      glusterd: /var/log/glusterfs/etc-glusterfs-glusterd.vol.log
      bricks  : /var/log/glusterfs/bricks/bricks-vol01.log

    more information see http://gluster.readthedocs.org/en/latest/

mount:
  description: How to mount
```

```
    value: |
      * glusterfs
        mount -t glusterfs IPADDRESS:/vol01 /mnt/MOUNTDIR
      * cifs
        \\IPADDRESS\Share
```

Results

The NAS you created is now in operation.

Note

Do not create multiple NAS servers in the same project using the NAS creation template file. When you need to create multiple NAS servers in the same project, make corrections so that different names are used for the host names (nas1, nas2) set in the template file.

```
... (omitted)
                echo '$NAS1_IP_ADDR nas1' >> /etc/hosts
                echo '$NAS2_IP_ADDR nas2' >> /etc/hosts
... (omitted)
```

What to do next

To access the NAS server, you must perform either of the following on the client:

- Installation and setup of GlusterFS client
- Setup of sharing in Windows

Note

Do not access the NAS server using NFS protocol.

- For Linux OS

Note

Use GlusterFS client version 3.6.X (X represents 2 or later). When you upgraded the NAS server version, also upgrade the client version.

A user with administrator (root) privileges must perform the following operations:

1. If glusterfs is installed, uninstall glusterfs.

   ```
   # yum remove glusterfs-server
   # yum remove glusterfs-client
   ```

2. If the glusterfs repository exists in the yum repository, delete it.

   How to check: Execute "yum repolist all" to check whether the glusterfs repository exists.

   How to delete: Delete the file in which the glusterfs repository is set from the /etc/yum.repos.d directory or move to a different directory.

3. Register the repository.

   ```
   # wget http://download.gluster.org/pub/gluster/glusterfs/3.6/3.6.2/
   EPEL.repo/glusterfs-epel.repo -P /etc/yum.repos.d
   # yum clean all
   # yum search glusterfs
   # yum -y install glusterfs-client
   ```

4. Add the following settings to /etc/hosts:

   ```
   IPADDRESS nas1
   IPADDRESS nas2
   ```

   In "IPADDRESS," specify the private IP address of nas1/nas2 server. Check the private IP address in the portal screen or the API execution results.

5. Create the directory to be used for mount destination.

   ```
   # mkdir /mnt/MOUNTDIR
   ```

   In "MOUNTDIR," specify a directory.

6. Mount the NAS server.

```
# mount -t glusterfs IPADDRESS:/vol01 /mnt/MOUNTDIR
```

Note

To the -t option of the mount command, specify "glusterfs." Do not specify "cifs."

7. For details about other additional settings such as security, refer to the GlusterFS website[2].

- For Windows

  A user with administrator (Administrator) privileges must perform the following operations:

  1. From the Start menu, click [All Programs] > [Accessories] > [Run] and enter the following string in the [Open] box to connect.

     ```
     \\IPADDRESS\Share
     ```

     In "IPADDRESS," specify the private IP address of nas1/nas2 server. Check the private IP address in the portal screen or the API execution results.
  2. For details about other additional settings such as security, refer to the Samba website[3].

[2] *https://gluster.readthedocs.org/en/latest/Administrator%20Guide/Setting%20Up%20Clients/*
[3] *https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/install.html#id2553683*

Part 4: Network

Topics:

With a physical network separated by virtualization technology, K5 IaaS provides a virtual infrastructure that is accessible via the Internet.

4.1 Virtual Network

4.1.1 Network Management

Network management allows you to create or delete networks in a project in order to create resources such as virtual servers.

You can create multiple networks in a project.

Creating a Network

To create a network, specify the following items.

Table 67: List of Network Settings

Item	Description	Required
Network Name	Specify a name to identify the network.	
Availability Zone Name at Creation Destination	Specify the name of the availability zone where the network will be created. If this setting is omitted, the default availability zone will be used.	

Note To communicate with an external network, you must create a virtual router and connect it to the internal network.

To create resources such as virtual servers, create a subnet on the network you created.

Deleting a Network

Delete a network that is no longer needed.

Important If there are virtual servers or a virtual router to which a user is connected on the network to be deleted, you must disconnect the virtual resources from them before deleting the network.

4.1.2 Subnet Management

Subnet functions include the management of private IP addresses for resources that are connected to a network and the automatic setting of an IP address with DHCP.

Creating a Subnet

You can set the following items on a network to create a subnet.

Table 68: List of Subnet Settings

Item	Description	Required
Subnet Name	Specify a name to identify the subnet.	
Network ID	Specify the ID of the network to which the subnet will belong.	Yes
IP Version	Specify IPv4.	Yes

Item	Description	Required
Network Address	Specify an address from within the following ranges of private IP addresses, in CIDR notation. • Class A: 10.0.0.0 - 10.255.255.255 • Class B: 172.16.0.0 - 172.31.255.255 • Class C: 192.168.0.0 - 192.168.255.255	Yes
IP Address Range	Specify a starting address and an ending address for the IP address range to be assigned within a network.	
Gateway Address	Specify a gateway IP address.	
Enable/Disable DHCP Auto Allocation	Specify true or false.	
Availability Zone Name	Specify the availability zone where the subnet will be created. If this setting is omitted, the default availability zone will be used.	

Tip In order to communicate with a DNS server, you must allow outbound communication to the Internet. Check the settings of the *security group functions* or *firewall service*, and configure them to allow communication to the DNS server. (Protocol: TCP/UDP, Port No.: 53)

Deleting a Subnet

Delete a subnet that is no longer needed.

Note If a resource connected to the subnet is currently using an IP address, you will not be able to delete the subnet.

4.1.3 Security Group Functions

Security group functions allow you to define and configure groups of rule settings in order to perform packet filtering on ports that are connected to virtual servers.

You can set multiple rules in a security group. Packets that match one of the rules in a security group that is set on a port are allowed, and all other packets are blocked. (whitelist method, OR condition)

Note You cannot set a security group on a port of a virtual router or a DHCP server.

Creating a Security Group

The *default security group*, which automatically blocks communication, is set on the port. Create a security group and configure rules that allow communication as necessary.

To create a security group, specify the following items.

Table 69: List of Security Group Settings

Item	Description	Required
Security Group Name	Specify a name that identifies the security group.	
Description	Enter a description of the security group to be created.	

Item	Description	Required
Availability Zone Name	Specify the availability zone where the security group will be created. If this setting is omitted, the default availability zone will be used.	

Default Rules

The default rules when a security group is created are shown below.

Table 70: Default Rules When a Security Group Is Created

Direction	Communication Partner	Protocol	IP Version
Outbound (Egress)	All	All	IPv4
Inbound (Ingress)	Own security group	All	IPv4

Creating a Rule

Rules for performing packet filtering consist of the following items. You can register multiple rules in a single security group.


Tip For communication between virtual servers where both can use the security group functions, in general we recommend using the security group ID to specify the communication partner.

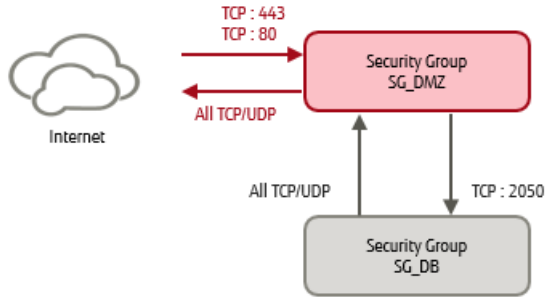
To create a rule, specify the following items.

Table 71: List of Security Group Rule Settings

Item	Description	Required
Security Group ID	Specify the ID of the security group in which you will register the rule.	Yes
Communication Direction	Specify either inbound (Ingress) or outbound (Egress).	Yes
IP Version	Specify IPv4.	
Communication Partner	For inbound, specify the sender. For outbound, specify the destination. Use either of the following: • IP address in CIDR notation • Security group  Note Specifying a security group is equivalent to specifying the IP addresses for all ports where that security group is set.	
Protocol Information	Specify one of the following: • tcp • udp • icmp	Yes
Starting Port No.	Specify the starting port number that is appropriate for the protocol information.	

Item	Description	Required
	Tip If you want to use a single port, specify the same value for the starting port number and the ending port number. Warning If you specify 0 for the starting port number, communication will be allowed on all ports. Therefore, do not specify 0.	
Ending Port No.	Specify the ending port number that is appropriate for the protocol information.	
Availability Zone Name	Specify the availability zone where rules will be created. If this setting is omitted, the default availability zone will be used.	

Figure 23: Example of Configuring Security Group Rules



Default Security Group

If you omit security group settings when creating a port, the default security group created in the project will be set automatically.

Tip The security group name for the default security group is "default."

The initial rule settings for the default security group are shown below.

Tip You can add rules to the default security group.

Table 72: Default Security Group Rules

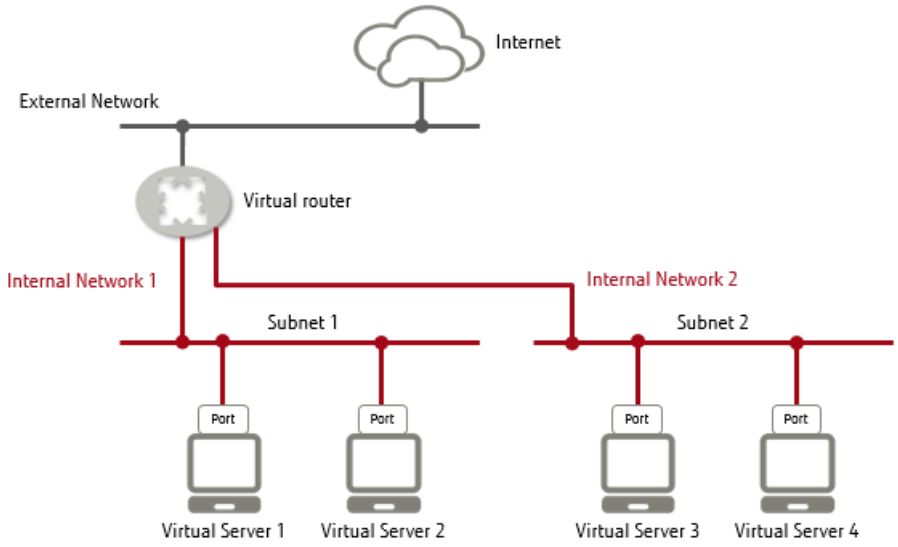
Direction	Communication Partner	Protocol	IP Version
Egress	All	All	IPv4
Ingress	Own security group	All	IPv4

4.1.4 Virtual Router Function

The virtual router function is used to connect an external network to an internal network, or to connect multiple internal networks to each other.

The relationship between networks and a virtual router is shown in the following figure.

Figure 24: Relationship between External/Internal Networks and a Virtual Router



Creating a Virtual Router

To create a virtual router, specify the following items:

Warning: Do not specify an external network when creating a virtual router. If you do, your Internet connection will not function normally. In order to specify an external network, use the function for modifying the information of a virtual router after it has been created.

Table 73: List of Virtual Router Settings

Item	Description	Required
Virtual Router Name	Specify a name to identify the virtual router.	
Availability Zone Name	Specify the availability zone where the virtual router will be created. If this setting is omitted, the default availability zone will be used.	

Modifying the Virtual Router Information

You can modify the setting information for an existing virtual router. To connect the virtual router to an external network, use this function to set the external network.

Table 74: Modifying the Virtual Router Information (List of Items That Can Be Set)

Item	Description	Required
Virtual Router Name	Specify the name of the virtual router for which you want to change the settings.	
External Network ID	Specify the ID for the external network.	

Item	Description	Required
	Tip You can confirm the ID in the list of subnet IDs.	

Managing the Connection between a Virtual Router and a Network

Use the following operation to add a new subnet connection to an existing virtual router.

1. Create a port on the subnet for which you want to add a connection.
2. Add the created port to the virtual router as an interface.

Tip A routing table is set automatically so that subnets connected to the same virtual router can communicate via the virtual router.

Important If the virtual router is hierarchically structured, the user should set the routing table on the virtual router so that communication can take place normally.

Deleting a Virtual Router

Delete a virtual router that is no longer needed.

Important If a subnet is connected to a virtual router, you cannot delete the virtual router. You must first disconnect from all subnets.

NAT Functions

You can use the following NAT functions on a virtual router.

- SNAT

  Communication from an internal network to an external network. The sender global IP address used for SNAT is unique to each virtual router connected to an external network and is not shared with any virtual routers of other projects.
- DNAT

  Communication from an external network to an internal network

If a global IP address has been assigned to the port on a resource, address translation will be performed between the global IP address and private IP addresses.

Inter-Project Network Connection Function

You can connect networks via a virtual router between different projects in the same contract number (domain). To the virtual router in your project, set the information of a port existing in another project to be connected to, as shown below.

Table 75: Inter-Project Network Connection (List of Items That Can Be Set)

Item	Description	Required
Port ID	Specify the ID of a port that exists in a project different from the project to which the virtual router belongs.	Yes

Disconnection of Inter-Project Network Connection

To disconnect the inter-project network connection, delete the information of the port (belonging to another project) that is already connected to the virtual router.

Table 76: Disconnection of Inter-Project Network Connection (List of Items That Can Be Set)

Item	Description	Required
Port ID	Specify the port ID from which the inter-project network connection will be disconnected.	Yes

4.2 Port Addition Service

4.2.1 Port Management

This function allows you to create and manage ports (network interfaces) to associate with IP addresses in order to connect resources such as virtual servers to a network.

If you specify only a subnet when creating the following resources, the system will automatically create and assign ports.

- Virtual server

  Note: If you want to create a port by specifying an IP address rather than using automatic allocation with DHCP, first create a port at that IP address in advance, and then assign it to a virtual server.

  Tip: You can add multiple ports to a virtual server.

- Virtual router

  Note: Ports are assigned automatically only if they are created on the default gateway (x.x.x.1). To add a virtual router to a network to which a virtual router is already connected at the address x.x.x.1, you must configure the port manually.

Creating a Port

Create a port to specify and assign an IP address that is not used in a subnet, or to add a new port to a resource.

Note: When you create a new port, you can assign an IP address. If you change the IP address, you must re-create the port.

Table 77: Creating a Port (List of Items That Can Be Set)

Item	Description	Required
Network ID	Specify the ID of the network to which the port will be connected.	Yes
Port Name	Specify a name to identify the port.	
Owner Device ID	Specify the resource ID that owns the port to be created.	
MAC Address	If you explicitly specify a MAC address, the system will assign that MAC address to the port.	
Private IP Address	If you explicitly specify an IP address, the system will assign that IP address to the port. If this setting is omitted, an address from within the range of addresses on the network specified by the network ID will be assigned. Note: If you specify an IP address that is already in use, creation of the port will fail.	

Item	Description	Required
List of Allowed Address Pairs	Out of the communications blocked by the filtering rule against IP spoofing[4], specify the senders to be explicitly allowed, using a list of combination of MAC address and IP address.  Tip When running a program such as PRIMECLUSTER on a virtual server, allow the combination of MAC address and IP address of the sender that requires communication, using this parameter.  Warning You cannot use this function to run Windows NLB. Doing so may affect the underlying K5 IaaS network.	
List of Security Group IDs	Specify as a list the security groups to be applied to the port.	
Network ID	Specify the ID of the network to which the port will be connected.	
Availability Zone Name	Specify the availability zone where the port will be created. If this setting is omitted, the default availability zone will be used.	

[4] The filter that is automatically set is designed to block communications except those from the ports with the combinations of MAC and IP address assigned to the virtual server. Using this filter prevents spoofing with a forged sender IP address or MAC address.

4.3 Global IP Service

4.3.1 Global IP Address Service

You can acquire or release a global IP address that is used to access virtual resources via the Internet. The global IP address that you obtain is assigned to virtual resources and used as a floating IP address.

Acquiring a Global IP Address

Specify the port of the assignment destination and obtain the global IP address.

Table 78: List of Global IP Address Settings

Item	Description	Required
External Network ID	Specify the external network ID issued by the system Tip You can confirm the ID in the list of subnet IDs.	Yes
Port ID	Specify the port to which the global IP address is to be assigned	Yes
Private IP Address	Specify the private IP address to be replaced with the global IP address	
Project ID	Specify the ID of the project for which the global IP address is to be obtained	
Availability Zone Name	Specify the availability zone for which the global IP address is to be obtained. If omitted, a global IP address is obtained for the default availability zone	

Note The global IP address is automatically assigned from the pool of addresses provided by this service. You cannot, for example, specify a range within which to assign the global IP address, or specify and obtain a global IP address of your choice.

Changing the Assignment of a Global IP Address

You can specify an existing global IP address and change the assigned port.

Table 79: List of Changeable Fields for Global IP Address

Item	Description	Required
Port ID	Specify the new port to which to assign the global IP address	Yes
Private IP Address	Specify the private IP address that is to be replaced with the global IP address	

Releasing a Global IP Address

You can release a global IP address that you have obtained that is no longer needed.

Warning

After the specified period has lapsed, global IP addresses that have been released might be acquired and reused by other users of the service via global IP address acquisition. Prior to releasing the global IP address, take measures such as erasing the DNS registration in order to prevent communication involving the IP address from unintentionally taking place.

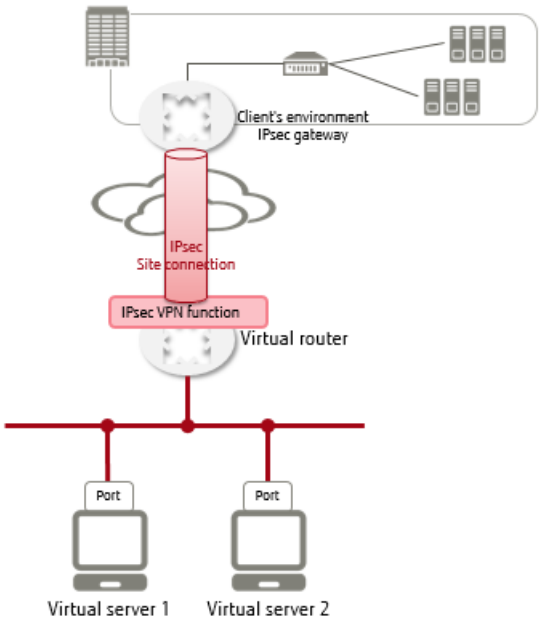
4.4 VPN (IPsec VPN)

4.4.1 IPsec VPN Function

The IPsec VPN gateway function allows you to connect to on-premises environments or to systems between regions.

If you add the IPsec VPN function to a virtual router, you can connect to a peer IPsec VPN gateway.

Figure 25: Network Connections Using the IPsec VPN Function



Note

Communication is possible through an IPsec VPN tunnel between a single subnet connected directly to a virtual router and a single subnet connected to the peer gateway.

Note

You can create multiple IPsec VPN tunnels on a single virtual router.

Settings

Table 80: Settings Related to VPN Connections

Item	Supported Methods
Authentication Method	Pre-shared key method
Action When Dead Peer Is Detected	hold, clear, restart, restart by peer
DPD Interval	1 second or more
DPD Timeout	A value larger than the DPD interval
Initiator Mode	bi-directional, response-only

Settings Related to Supported Encryption Methods

Table 81: IKE Policy

Item	Supported Methods
Authorization Algorithm	sha1
Encryption Algorithm	AES-128, AES-192, AES-256
IKE version	V1
Life Time	60 - 86400 (seconds)
PFS	group2, 5, 14
Key Exchange Mode	main

Table 82: IPsec Policy

Item	Supported Methods
Authorization Algorithm	sha1
Capsule Mode	tunnel
Encryption Algorithm	AES-128, AES-192, AES-256
Life Time	60 - 86400 (seconds)
PFS	group 2, 5, 14
Transformation Protocol	esp

Points to Note

When the IPsec VPN function is enabled, the communication shown below is allowed regardless of the firewall rule that is set on the virtual router.

Table 83: List of Allowed Communication Rules

Protocol	Port No.	Description
UDP	500	Internet Security Association and Key Management Protocol (ISAKMP)

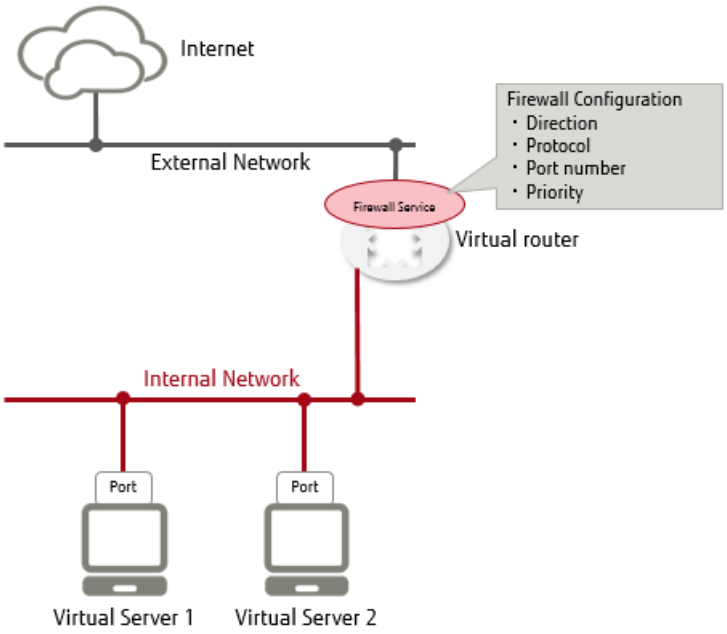
4.5 Firewall

4.5.1 Firewall Service

While a security group sets packet filters on virtual servers, the firewall service sets packet filters on the virtual router.

You can set this service on the virtual router connected to an external network as shown in the following figure.

Figure 26: Using the Firewall Service



Firewall service settings consist of the following elements and are configured with the information for filtering that is shown below, in the order they are listed. You must associate the firewall with a virtual router in order to perform filtering.

1. Create firewall rules
2. Register a collection of rules to create a firewall policy
3. Specify a policy to create a firewall, and associate it with a virtual router

Creating/Changing a Firewall Rule

Specify the following items to create or change firewall rules.

Table 84: List of Firewall Rule Settings

Item	Description	Required
Rule Name	Specify a name for the rule.	
Description	Enter a description.	
Priority	Specify the order in which policy rules are applied. Inspections are performed in ascending order from the smallest value.	
Enable/Disable Rule	Specify whether to enable or disable the rule.	

Item	Description	Required
Protocol	Specify one of the following protocols: • tcp • udp • icmp	
IP Version	Specify IPv4.	
Source IP Address	Specify the IP address of the sender (can be specified in CIDR notation).	
Source Port Number	Specify the port number of the sender targeted for communication (a range can be specified in a:b format).	
Destination IP Address	Specify the IP address of the destination (can be specified in CIDR notation).	
Destination Port Number	Specify the port number of the destination targeted for communication (a range can be specified in a:b format).	
Actions	Specify "Allow" or "Deny."	
Availability Zone Name	Specify the availability zone where rules will be created. If this setting is omitted, the default availability zone will be used.	

Creating/Modifying a Firewall Policy

Define a list of multiple firewall rules as a firewall policy. The traffic is inspected according to the rules in the list, in order of priority, to control whether communication is allowed or not.


Tip

The "DENY ALL" rule is automatically added to the end of the policy. Therefore, traffic that does not meet the definition for any of the Allow rules is blocked by default. (This is the whitelist method.)

The "DENY ALL" rule that is added automatically is an implicit rule, and does not appear in the policy.

Specify the following items to create or modify a firewall policy.

Table 85: List of Firewall Policy Settings

Item	Description	Required
Policy Name	Specify a name for the policy.	
Description	Enter a description.	
List of Firewall Rules	Specify as a list the firewall rules that have been created. Traffic is inspected according to the list of rules specified here, in order from the top of the list.	
Availability Zone Name	Specify the availability zone where policies will be created. If this setting is omitted, the default availability zone will be used.	

Creating/Modifying a Firewall

Create or modify a firewall on a virtual router by specifying a firewall policy in which rules have been registered.

Table 86: List of Firewall Settings

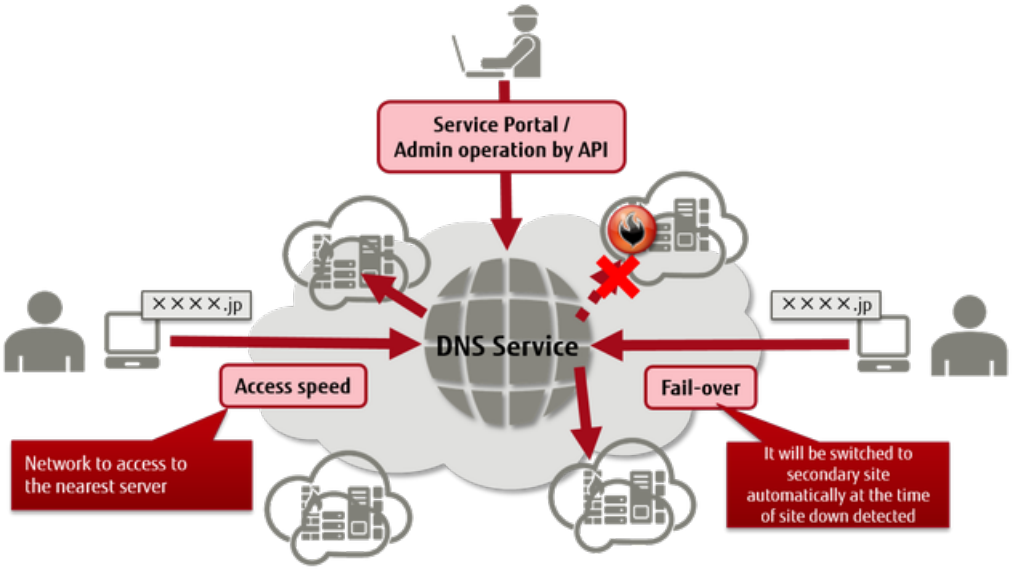
Item	Description	Required
Firewall Name	Specify a name for the firewall.	
Description	Enter a description.	
Firewall Policy ID	Specify the ID of a firewall policy that has been created.	
Virtual Router ID	Specify the virtual router ID to which the firewall policy will be applied. Important If this setting is omitted, the specified policy will be applied to all virtual routers in the availability zone.	
Availability Zone Name	Specify the availability zone where the firewall will be created. If this setting is omitted, the default availability zone will be used.	

4.6 DNS Service

4.6.1 DNS Service

The DNS service provides an environment for running zone management and record management operations on a DNS content server via Service Portal or an API. You can develop a system that interacts with multiple regions, without the need to build your own DNS server.

Figure 27: Overall Layout of the Functions Provided by the DNS Service



Functions Included

- DNS Zone Management Functions
- Record Management Functions
- Failover Function
- Latency-Based Routing Function
- Weighted Round Robin Function

Points to Note

- You cannot use a Whois publishing proxy for a domain.
- SOA records cannot be set.
- You cannot set an NS record for the root domain.
- You cannot set an alias for A or AAAA records.
- Dynamic IP record settings (Dynamic DNS) are not supported.
- The zone transfer function is not supported.
- DNSSEC is not supported.

4.6.2 DNS Zone Management Functions

Create zones, delete zones, and view the information of zones within the domains that are currently managed.

Creating a Zone

Create a zone. When you create a zone, an authentication code is required to confirm ownership of the domain.

Important

Select a domain from *Domains That Can Be Registered in a Zone* on page 216.

Note

For domains managed by other companies, authentication is required to create a zone again.

Acquiring Zone Information

Specify a zone name (zone ID) to view the zone information. You can acquire the zone information and the name server information.

Acquiring Zone Information in Bulk

View zone information in bulk.

Table 87: Acquiring Zone Information in Bulk (List of Items That Can Be Set)

Item	Description	Required
Starting Zone ID	Specify a zone ID to serve as the top of the list of zone information to be viewed. If this setting is omitted, acquisition will start from the beginning of the zone information.	
Number Acquired	Specify the maximum number of zone information items to acquire. If this setting is omitted, 100 is set.	

Deleting a Zone

Specify a zone that is no longer needed and delete it.

Important

When a zone is deleted, all of the records that are set for that zone are also deleted. Deleted zone information cannot be viewed or restored.

Note

The domain still exists after a zone is deleted.

Limiting Values

Table 88: List of Limiting Values Related to DNS Zone Management

Item	Limiting Values
Number of DNS Zones Registered	100 per domain
Time To Live (TTL) for Cache that Can Be Specified	60 - 86,400 seconds
Maximum Number of Records for Bulk Acquisition of Zone Information	100 records

4.6.3 Record Management Functions

Create, modify, and delete DNS records, and view the information contained in these records.

Creating/Modifying/Deleting a Record

You can create, modify, and delete the following types of records. You can execute the same request on multiple records at the same time.

- NS
- A
- AAAA
- CNAME
- MX
- TXT
- LBR (latency-based routing)


Note

Record operations are not executed immediately. They are executed when the status information included in the response changes to "INSYNC".

Limiting Values

Table 89: List of Limiting Values Related to DNS Record Management

Item	Limiting Values
Number of Records that Can Be Specified	10,000 per zone
Supported Record Type	A, AAAA, CNAME, MX, NS, TXT
Record Type with Wildcard Support	A, AAAA, MX, CNAME, TXT

Table 90: List of Limiting Values for DNS Record Entries

Record Type	Item	Limitations
A	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Available character type: Alphanumeric characters and dots (.) Must be a valid IPv4 address
	Memo	Length: 255 characters or less Available character type: Double-byte characters
	Weight	0 - 100 Available character type: Numeric characters
	Health Check IP Address	Length: 1 - 32 characters

Record Type	Item	Limitations
		Alphanumeric characters and dots (.)
	Health Check Port Number	Length: 1 - 5 characters Available character type: Numeric characters
	Health Check Host Name	Length: 0 - 255 characters Available character type: Single-byte characters
	Health Check Path	Available character type: Single-byte characters
AAAA	Record Name	Length: 1 - 63 characters Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Alphanumeric characters and dots (.) Must be a valid IPv6 address
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
	Weight	0 - 100 Available character type: Numeric characters
	Health Check IP Address	Length: 1 - 32 characters Available character type: Alphanumeric characters and dots (.)
	Health Check Port Number	Length: 1 - 5 characters Available character type: Numeric characters
	Health Check Host Name	Length: 1 - 255 characters Available character type: Single-byte characters
	Health Check Path	Available character type: Single-byte characters
CNAME	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)
	Memo	Length: 1 - 255 characters

Record Type	Item	Limitations
		Available character type: Double-byte characters
MX	Record Name	Length: 1 - 63 characters Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)
	Priority	Character type: Numeric characters, 0 - 64,000
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
TXT	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Alphanumeric characters, single-byte spaces, and single-byte symbols other than double quotation marks (")
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
NS	Record Name	Character type: Alphanumeric characters, dots (.), and hyphens (-)
	TTL	60 - 86,400 seconds
	Value	Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
LBR	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), and hyphens (-)
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters

Points to Note

- You cannot set more than one record of the same record type and with the same value for the same host name.
- You cannot set CNAME and other records for the same host name at the same time.
- You cannot set LBR and other records for the same host name at the same time.
- The following DNS records cannot be set:
  - Records that are not in FQDN format
  - Records with a dot (.) or hyphen (-) at the beginning or end of the record name
- SOA record settings cannot be changed.
- You cannot set an NS record for the root domain.
- Dynamic IP record settings (Dynamic DNS) are not supported.
- DNSSEC is not supported.

4.6.4 Failover Function

When the health check function is used on an end point that can be set by the user, the normal record information is returned if the health check is successful. However, if the health check indicates abnormality, the record information on the standby side is returned and traffic to the server where abnormality occurred is blocked.

Table 91: Failover Settings

Item	Description
Primary	Specify only a single record. You cannot specify multiple records.
Secondary	You can specify multiple records.

Note

Only A and AAAA records can be used.

Table 92: Health Check Destination Settings

Item	Description
Protocol	Select HTTP, HTTPS, or TCP.
IP Address	The values entered for the IP address are shown. This item can be changed.
Port No.	80 is shown for HTTP, 443 is shown for HTTPS. This item can be changed.
Host Name	Displayed when HTTP or HTTPS is selected for the protocol. Enter the host information from the HTTP header.
Path	Displayed when HTTP or HTTPS is selected for the protocol. Enter the path section of the URL targeted for health check.
URL	A URL that consists of the IP address, port number, and path is displayed when HTTP or

Item	Description
	HTTPS is selected for the protocol. This cannot be changed.

Health Check Rules

Note

- The individual health checks that are specified for each record are run.
- Health check is performed at 5-minute intervals. Until the first health check is performed immediately after record registration, both primary and secondary records are returned as a valid record.
- When a failover occurs, a host swithes over to the other host that that has the same Name tag and same Type tag in the group.
- If multiple records are specified for [Secondary], priority is given to the record that was registered first.
- The status for records that have been set is Enabled if there is a response from the DNS, and Standby if there is no response.
- If an abnormality is detected by a health check both in primary and secondary records, the primary record is returned.

Points to Note

- When you use a failover, 60 seconds is recommended for TTL for records.

4.6.5 Latency-Based Routing Function

This function allows the system to connect to the closest server by returning the record information that is set for that area, based on the access source information for the DNS server.

Table 93: Latency-Based Routing Settings

Item		Description
Record Name		Enter the host name of the server at the access destination.
Value	Default Host	Specify the value to return if there is access from somewhere other than the specified area. Select a value from an A or AAAA record that is registered in the same zone.
	Area	Specify the closest area.
	Host	Specify the value to return if there is access from the specified area. Select a value from an A or AAAA record that is registered in the same zone.

Points to Note

- If the client accesses the server via a DNS cache server or resolver, the IP address of the DNS cache server or resolver is used as the IP address of the source.

4.6.6 Weighted Round Robin Function

This function provides uneven round robin distribution by using hit counts according to the weight value for each record. This allows greater flexibility in access dispersion.

Table 94: Weighted Round Robin Settings

Item	Description
Weight Value	Specify the hit rate (from 0 to 100) for each record. The hit rate for a record will fluctuate according to the weight value that is specified.
Target	Distribution is performed on the hosts that have the same Name tag and same Type tag in the group.

Note

This function can be used only for A or AAAA records.

Points to Note

- If there are no records with a weight of 100, a target record might not be returned during name resolution.
- If the weight is set to 0, the hit rate will also be 0 and therefore no value is returned.
- During normal record registration, if records are registered with the same host and same record type, a weight of 100 is applied.

4.7 Load Balancer

4.7.1 Load Balancer Service

Create a load balancer within a network to distribute traffic to your virtual servers.

The load balancer service provides the following functions.

Creating a Load Balancer

Create a load balancer by configuring the following settings according to how you will use load distribution. When a load balancer is created, a unique FQDN will be assigned. Use this FQDN to ensure continuous operation that is unaffected by increases or decreases in the number of servers targeted for load distribution.

Tip If you register multiple subnets with different availability zones on the load balancer, the load will be distributed across the availability zones.

Table 95: Load Balancer (List of Items That Can Be Set)

Item	Description	Required
Load Balancer Name	Specify a name to identify the load balancer Note The name must be unique within the project.	Yes
Load Balancer Type	Specify one of the following types, according to the purpose: • public: Load distribution of traffic from the Internet • internal: Load distribution within a private network only	Yes
List of *Load Distribution Condition Settings* on page 115	Specify load distribution conditions regarding what traffic to distribute. You can specify multiple conditions as a list.	
List of Security Groups	Specify as a list the security group IDs that are set on the load balancer.	
List of Subnets	Specify the IDs of the subnets to which the virtual server targeted for load distribution is connected, as a list. Important To distribute the load of traffic from the Internet, the virtual router that the subnet is connected to must be connected to an external network.	Yes
Grade	Specify one of the following levels of performance for the load balancer: • Standard: Standard performance • Middle: Intermediate performance • High: High performance	

Operations on a Load Balancer

- *Adding/Deleting a Target for Load Distribution* on page 117
- *Multi-Availability Zone Distribution* on page 118
- *Monitoring for Abnormality on a Load Distribution Target* on page 118

Deleting a Load Balancer

Specify and delete an existing load balancer.

Security

If you create a load balancer that can communicate via the Internet, the front end will be public on the Internet. To prevent attacks via the Internet, create the necessary security group and configure it on the load balancer in advance.

Limiting Values

Table 96: List of Limiting Values Related to the Load Balancer Service

Item	Limiting Values
Load Balancer Name	• Length: 1 - 30 characters • Available character type: Alphanumeric characters and hyphens (-)
Number of Load Balancers Created	20 per project
Maximum Number of Connections	32,768 per subnet

4.7.2 Load Distribution Condition Settings

Set the traffic conditions for load distribution when creating a load balancer or for an existing load balancer.

To set the traffic conditions for load distribution, use a "listener" to determine how the traffic that has reached the front-end port communicates with the back-end port.

Creating/Modifying a Listener

When creating a load balancer, configure the following settings to create a listener. You can also specify the name of an existing load balancer to create a new listener or modify an existing one.

You can specify an SSL certificate for a listener, to terminate HTTPS communication.

Note To use an SSL certificate, you must use the *key management function* to register the certificate in advance.

Table 97: List of Listener Settings

Item	Description	Required
Protocol	Specify the front-end and back-end communication protocols. Note Only the following combinations can be specified: • HTTP - HTTP	Yes

Item	Description	Required
	• HTTPS - HTTP • HTTPS - HTTPS • TCP - TCP • SSL - TCP • SSL - SSL	
Front-end Port No.	Specify the front-end port number (1 - 65535).	Yes
Back-end Port No.	Specify the TCP port number (1 - 65535) for the virtual server at the distribution destination.	Yes
SSL Certificate ID	Specify the ID of the server certificate registered using the key management function. Important Only one server certificate can be specified for each listener. If you set a different server certificate than the one that has been specified for a given port, the certificate that was set most recently is enabled.	

Managing Listener Policies

You can register, modify, and delete the policies that are applied to a listener. The following types of policies can be applied:

- Session persistence policy

  If this policy is specified, cookie information that identifies the virtual server that is targeted for load distribution is embedded in the response packet. When this cookie information is sent in a request from the client, the load balancer distributes the load to the virtual server to which the first access was allocated.

  Note This policy can be applied only if an HTTP/HTTPS listener is specified.

  Specify the following settings to register the session persistence policy:

  Table 98: List of Settings for the Session Persistence Policy

Item	Description	Required
Load Balancer Name	Specify the name of the load balancer to set for the session persistence policy.	Yes
Policy Name	Specify a name for the session persistence policy to be created. Note The name must be unique in the load balancer.	Yes
Session Persistence Period	Specify the maximum amount of time in seconds (1 - 2,147,483,647) for a session for session persistence using cookies.	

- Sorry page redirect policy

Set the redirect information to be used if abnormality is detected on the virtual server targeted for load distribution during a health check and there is no other virtual server that is available for load distribution.

This policy can be applied only if an HTTP/HTTPS listener is specified.

Note

Specify the following settings to register the sorry page redirect policy:

Table 99: List of Settings for the Sorry Page Redirect Policy

Item	Description	Required
Load Balancer Name	Specify the name of the load balancer for which to set the redirect policy.	Yes
Redirect Policy Name	Specify a name for the policy to be created.  The name must be unique in the load balancer. Note	Yes
Redirect Destination URI	Specify the URI for the redirect destination.  This is set as the Location information for redirect responses. Tip	Yes

4.7.3 Adding/Deleting a Target for Load Distribution

Add or delete a virtual server to target for load distribution in order to distribute the load of the traffic that has reached the load balancer.

The load distribution algorithm for virtual servers is the "less connections" algorithm.

Important

Adding a Virtual Server to Target for Load Distribution

Add a virtual server to target for load distribution. You can specify multiple virtual servers and register them all at once.

Before you add a virtual server to target for load distribution, the virtual server must be in an operating state.

Important

If you change the IP address of a virtual server that has already been registered, load distribution will not be performed for the new IP address. Register the server again to include it as a target for load distribution.

Warning

Deleting a Virtual Server Targeted for Load Distribution

Delete a virtual server that has been set as a target for load distribution. You can specify multiple virtual servers and delete them all at once.

Before you delete a virtual server that is targeted for load distribution, the virtual server must be in a stopped state.

Important

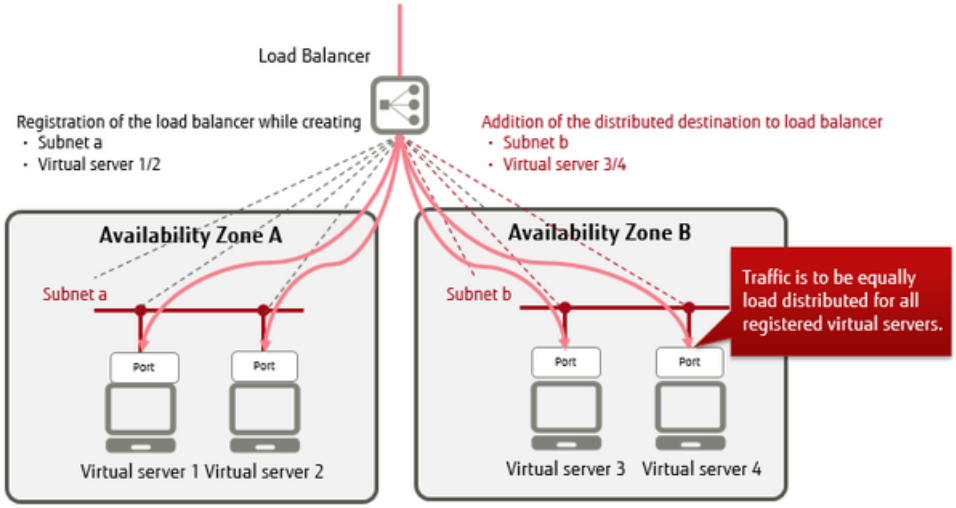
4.7.4 Multi-Availability Zone Distribution

If you register multiple subnets on a single load balancer, the load can be distributed across the availability zones.

If you specify multiple subnets with different availability zones on a load balancer, the traffic will be allocated across the availability zones.

In this case, because the load balancer is a single point of failure, you can connect multiple load balancers with a higher-level DNS service to improve distribution performance and availability.

Figure 28: Load Distribution when Connecting Multiple Availability Zones



4.7.5 Monitoring for Abnormality on a Load Distribution Target

Set the conditions for performing a health check on the virtual server targeted for load distribution.

Setting Health Check Conditions for Virtual Servers Targeted for Load Distribution

Configure the following settings as the conditions for checking whether a virtual server targeted for load distribution responds normally.

Table 100: List of Health Check Condition Settings

Item	Description	Required
Method	Select the method for monitoring the virtual server targeted for load distribution. Use the following format: "protcol:port[url]" • protocol: Specify either TCP or HTTP • port: Specify a port from 1 to 65535 • url: Specify the URL path (optional)	Yes
Interval (seconds)	Specify the interval for performing health checks, in seconds (1 - 2,147,483,647).	Yes

Item	Description	Required
Timeout (seconds)	Specify the time to wait for a response to a health check before a timeout occurs, in seconds (1 - 2,147,483,647).  Important Specify a value that is lower than the value for [Interval (seconds)].	Yes
Consecutive Detection of Abnormality Threshold (number of times)	Specify the number of consecutive health check failures that constitute occurrence of a failure on a target virtual server, and thus warrants exclusion of the virtual server as a target for load distribution (1 - 2,147,483,647).	Yes
Consecutive Detection of Normality Threshold (number of times)	Specify the number of consecutive health check successes that constitute the recovery of a target virtual server and thus warrants inclusion of the virtual server as a target for load distribution (1 - 2,147,483,647).	Yes

4.8 Network Connector

4.8.1 Network Connector Service

While virtual routers connect to networks that exist within the availability zone, the network connector service provides the function to connect to networks that exist outside the availability zone.

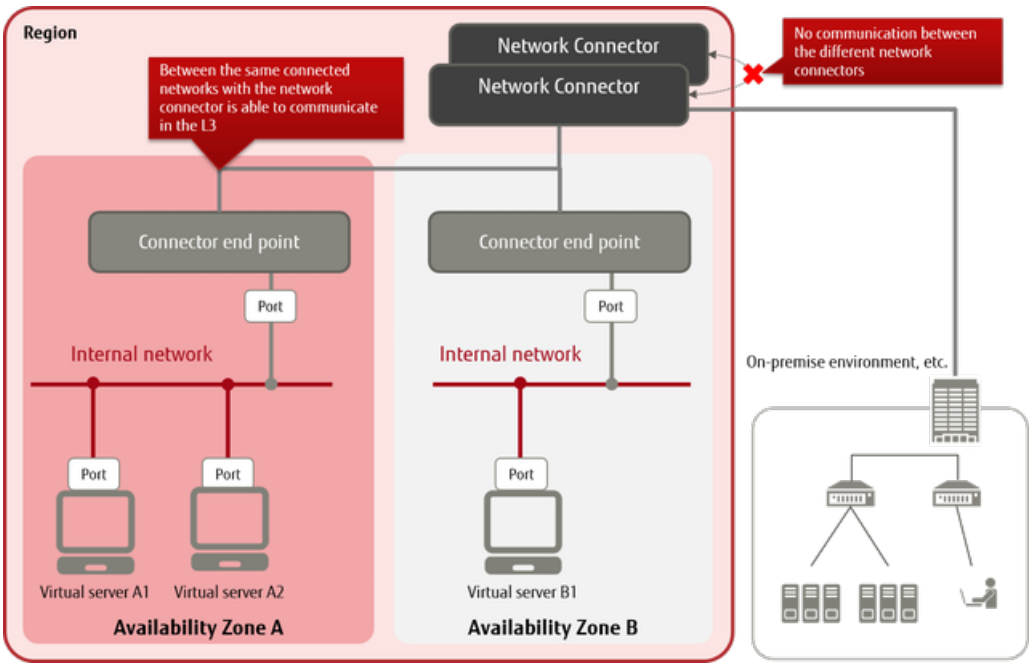
In order to achieve network communication between availability zones, create and connect network connectors and connector endpoints.

The network connector service is used to provide the following connection services:

- Intranet connections
- Hosting connections

Important In order to use the network connector service to connect to an external network, settings must be configured on the center side in advance. Contact the service provider for assistance.

Figure 29: Using the Network Connector Service



The following functions are provided in the network connector service.

Acquiring the Network Connector Pool Information

When creating a network connector, you can view the network connector pool information provided by the system in advance.

Creating a Network Connector

Set the following items to create a network connector.

Table 101: Creating a Network Connector (List of Items That Can Be Set)

Item	Description	Required
Network Connector Name	Specify a name that uniquely identifies the network connector.	Yes
Network Connector Pool ID	Specify the ID of the network connector pool in which the network connector will be created.	
Project ID	Specify the ID of your project.	

Viewing the Network Connector Information

You can view a list of created network connectors and their settings.

Modifying a Network Connector

Specify the ID of a network connector that has been created to modify its settings.

Table 102: Modifying a Network Connector (List of Items That Can Be Set)

Item	Description	Required
Network Connector Name	Specify a name that uniquely identifies the network connector.	

Deleting a Network Connector

Specify a network connector that is no longer needed and delete it.

Creating a Connector Endpoint

Set the following items to create a connector endpoint.

Table 103: Creating a Connector Endpoint (List of Items That Can Be Set)

Item	Description	Required
Connector Endpoint Name	Specify a name to uniquely identify the connector endpoint.	Yes
Network Connector ID	Specify the ID of the network connector that contains the connector endpoint that you want to use for intercommunication.	Yes
Type	Specify a type according to the network that you will connect to the connector endpoint. The user must specify "availability_zone." • availability_zone: When connecting to a K5 IaaS network	Yes
Creation Destination Information	Specify the following values according to the type specified above.	Yes

Item	Description	Required
	• For "availability_zone": Specify the name of the availability zone where the network to which the connector endpoint connects exists.	
Project ID	Specify the ID of your project.	

Viewing the Connector Endpoint Information

You can view a list of created connector endpoints and their settings.

Modifying a Connector Endpoint

Specify the ID of a connector endpoint that has been created to change its settings.

Table 104: Modifying a Connector Endpoint (List of Items That Can Be Set)

Item	Description	Required
Connector Endpoint Name	Specify the name that uniquely identifies the connector endpoint.	

Deleting a Connector Endpoint

Delete a connector endpoint that is no longer needed by specifying the ID.

Connecting a Connector Endpoint to a Network

Specify the ID of an existing connector endpoint to connect to a network.

- If the connector endpoint type is "availability_zone"

  Specify the ID of a port on the subnet that you want to connect to the connector endpoint.

  Note

  You must create the network, subnet, and port to be connected in advance.

Viewing the Connection Information for a Connector Endpoint and Network

Specify the ID of an existing connector endpoint to view the information for the network interface to which it is connected.

Releasing a Network Connection from a Connector Endpoint

Specify the ID of an existing connector endpoint to release its network connection.

- If the connector endpoint type is "availability_zone"

  View the connection information for the connector endpoint, and specify the IDs of ports that are no longer needed to delete them.

Part 5: Database

Topics:

K5 IaaS provides virtual servers equipped with the relational database function. By accessing this platform via the Internet, the user can set up and operate a relational database.

5.1 Overview of Functions

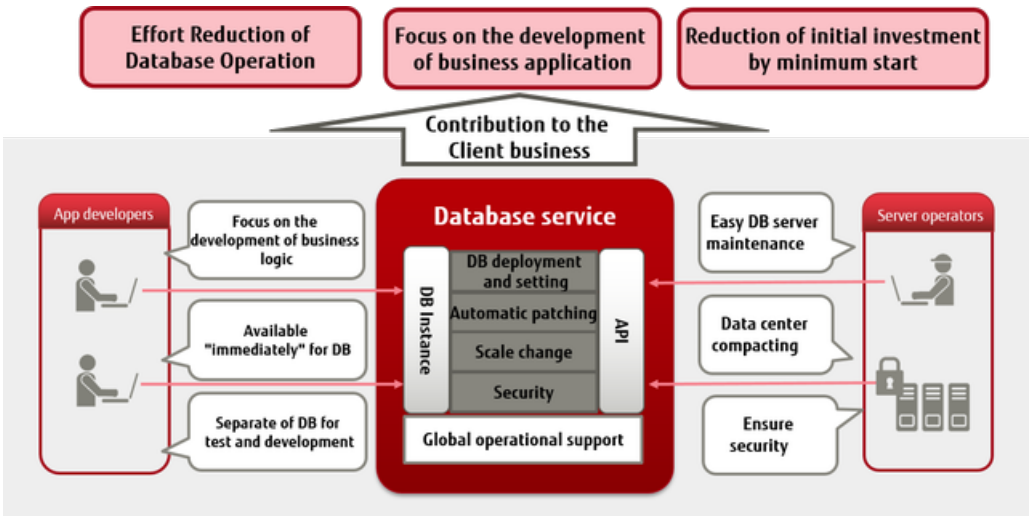
5.1.1 Database as a Service

Database as a Service facilitates setup and operations (such as scaling or backup) of cloud-based relational databases. Database as a Service reduces the burden on customers through use of an active-standby configuration that is constructed in environments that are physically separated, and automatic backups to cloud storage.

Benefits for Users

Users can utilize this service only when needed, and can use the database environment immediately whenever it is needed. In addition, users can leave the time-consuming operations to the side that provides the services, so that users can focus on developing business applications.

Figure 30: Value Provided By Database as a Service



Available Database Engines

Shown below is the compatibility information from the application perspective regarding database engines that are provided by this service. Users can use this service with applications intended for the products of the version levels included in the following table.

Table 105: Compatibility Information for Database Engines

Product Name	Compatible Versions and Levels	Remarks
Symfoware Server Enterprise Edition	V12.1	The same SQL can be used
PostgreSQL	9.2.4	The same SQL can be used

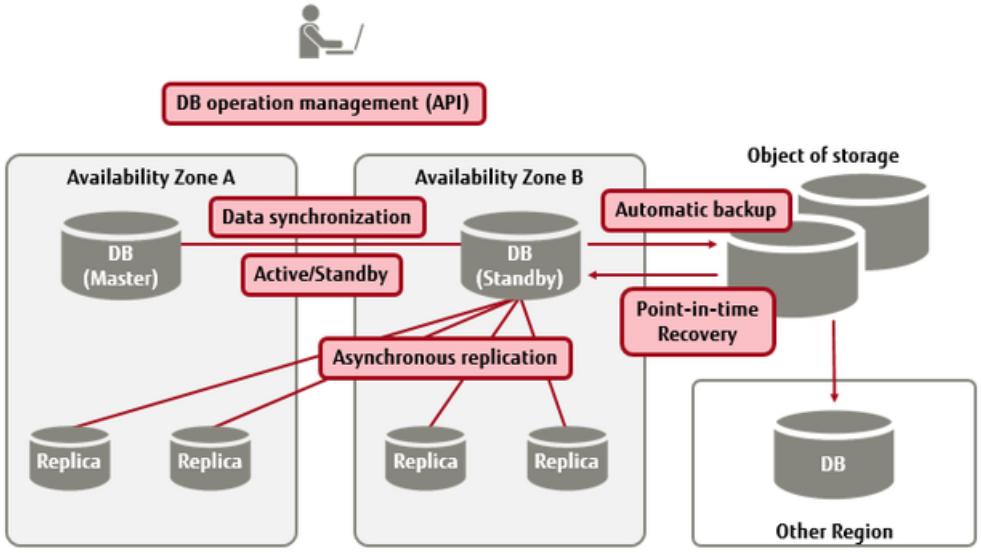
5.2 Building a Database

5.2.1 Creating a Virtual Database Server

In order to use a relational database environment, create virtual database servers. You can select the virtual database servers to create from various types according to the level of performance that is required, and you can configure settings such as automatic backups, as well.

Functions to enhance the performance, availability, and reliability are provided based on the virtual database servers that are created.

Figure 31: Overall Layout of Database as a Service



Virtual Database Server Settings

Configure the virtual database servers to be created.

- Specification of the virtual database server name
- Selection of the virtual database server type

Table 106: List of Provided Virtual Server Types (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
S-1	1	4
S-2	2	8
S-4	4	16
S-8	8	32
S-16	16	64
M-1	1	8
M-2	2	16
M-4	4	32
M-8	8	64

Type Name	Number of Virtual CPUs	Memory (GB)
M-16	16	128
XM-4	4	128

- Specification of the name of the availability zone where the server will be created
- Specification of the *DB subnet group*
- Specification of the *DB parameter group*

Data Area Settings

Specify the disk capacity and disk type that is used for the data area. Select the disk capacity from 10 GB to 10 TB, and the disk type from the following types.

Table 107: List of Disk Types

Type	Purpose
Standard	Use this in the following cases: • When you deploy application data that requires frequent file access (reading and writing) • When you handle a lot of large data files

Automatic Backup Settings

Configure automatic backup settings to perform a daily full backup of data and configuration files on the DB server. Items that you can specify are as follows.

Table 108: Settings for Automatic Backup

Item	Description
Backup time	Specify a specific time as the start time of the backup (specify the time in UTC)
Backup retention period	Specify in the range from 0 to 10 (days). If you specify 0, automatic backup will not be performed.

Automatic Maintenance Settings

You can set maintenance (such as security updates, or application of software patches) to be performed automatically every week. You can also select whether or not to perform automatic maintenance.

Items that you can specify are as follows.

Table 109: Settings for Automatic Maintenance

Item	Description
Maintenance time	Specify a specific time as the start time of maintenance (specify the time in UTC)
Automatic maintenance	Specify whether or not to perform automatic maintenance

Automatic Minor Version Upgrade Settings

Specify enable (true) or disable (false) to specify whether to perform version upgrade automatically when a minor version upgrade of the database engine is released.

Access Control

The *security group function* controls access to virtual database servers.

Database Settings

Configure settings for the database management master user, character codes, and other settings.

Table 110: Database Settings

Item	Description
Master user name	Specify the database management user name
Master user password	Specify the password for the database management user
List of users for database connections	Specify as a list the user name, password, and the name of the database to which the user can connect
Character code	Specify the character code that is used in the database

Points to Note

- Because virtual database servers are managed by the system, you cannot log in to virtual database servers by using SSH or remote desktop.

5.2.2 DB Subnet Groups

Create the network information that is used to create and control database instances as a DB subnet group. In order to ensure the availability of databases, register two or more subnets that exist in different availability zones.

Note

You must create a subnet before you can register it in the DB subnet group.

Creating a DB Subnet Group

Create a DB subnet group by specifying the parameters as shown below.

Table 111: Creating a DB Subnet Group (List of Items That Can Be Set)

Item	Description	Required
DB subnet group ID	Specify a DB subnet group ID. The characters that you specify must meet the following specifications: • Use alphanumeric characters and hyphens • Use an alphabetic character as the first character • You cannot use a hyphen as the last character • You cannot use two or more consecutive hyphens	

Item	Description	Required
	• Specify at least 1 character, and no more than 63 characters Note If you omit the ID, random characters will be set.	
DB subnet group name	Specify a name to identify the DB subnet group. The characters that you specify must meet the following specifications: • Use alphanumeric characters and hyphens • Use an alphabetic character as the first character • You cannot use a hyphen as the last character • You cannot use two or more consecutive hyphens • Specify at least 1 character, and no more than 255 characters	Yes
Subnet list	Specify as a list the subnets to register in the DB subnet group Note The specification of subnets must meet the following conditions: • Two or more subnets are specified • Each subnet that you specify belongs to a different availability zone	Yes
Description	Specify a description for the DB subnet group	

Acquiring the DB Subnet Group List

Acquire a list of the DB subnet groups in the project.

Checking the DB Subnet Group Information

Check the information of the DB subnet group, such as which subnets are registered, by specifying the ID of the DB subnet group in the project.

Modifying a DB Subnet Group

Change the following settings by specifying the ID of the DB subnet group in the project.

Table 112: Modifying a DB Subnet Group (List of Items That Can Be Set)

Item	Description	Required
DB subnet group ID	Specify the DB subnet group ID. The characters that you specify must meet the following specifications: • Use alphanumeric characters and hyphens • Use an alphabetic character as the first character • You cannot use a hyphen as the last character • You cannot use two or more consecutive hyphens • Specify at least 1 character, and no more than 63 characters	

Item	Description	Required
	Note If you omit the ID, random characters will be set.	
DB subnet group name	Specify a name to identify the DB subnet group. The characters that you specify must meet the following specifications: • You can use only alphanumeric characters and hyphens • Use an alphabetic character as the first character • You cannot use a hyphen as the last character • You cannot use two or more consecutive hyphens • Specify at least 1 character, and no more than 255 characters	
Subnet list	Specify as a list the subnets to register in the DB subnet group Note The specification of subnets must meet the following conditions: • Two or more subnets are specified • Each subnet belongs to different availability zones	
Description	Specify a description for the DB subnet group	

Deleting a DB Subnet Group

Specify the ID of a DB subnet group in the project to delete a DB subnet group that is no longer necessary.

Note Even if you delete the DB subnet group, the subnets that are registered in it will not be deleted.

5.2.3 DB Parameter Groups

A DB parameter group is a definition that sets various parameters for the database engine when you create a database instance.

Because which parameters you can specify depends on the database engine and the version, perform tuning after you create a DB parameter group by changing the parameters that are created under the DB parameter group.

Creating a DB Parameter Group

Create a DB parameter group by specifying the parameters as shown below.

Table 113: Creating a DB Parameter Group (List of Items That Can Be Specified)

Item	Description	Required
Parameter group family	Specify the type of parameter group, which is determined by the database engine and the version. You can specify the following value:	Yes

Item	Description	Required
	• symfoware_v12.1	
DB parameter group ID	Specify the ID of the DB parameter group. The characters that you specify must meet the following specifications: • Use alphanumeric characters and hyphens • Use an alphabetic character as the first character • You cannot use a hyphen as the last character • You cannot use two or more consecutive hyphens • Specify at least 1 character, and no more than 63 characters Note If you omit the ID, random characters will be set.	
DB parameter group name	Specify a name to identify the DB parameter group. The characters that you specify must meet the following specifications: • Use alphanumeric characters and hyphens • Use an alphabetic character as the first character • You cannot use a hyphen as the last character • You cannot use two or more consecutive hyphens • Specify at least 1 character, and no more than 255 characters	Yes
Description	Specify a description for the DB parameter group	

Acquiring the DB Parameter Group List

Acquire a list of the DB parameter groups in the project.

Checking DB Parameter Group Information

Check the detailed information of the DB parameter group by specifying the ID of the DB parameter group in the project. You can check the following items of each parameter that can be specified for a database.

Table 114: Each Parameter Item That Can Be Checked

Item	Description
Parameter name	You can check parameter names that can be specified
Parameter value	You can check the current setting value that corresponds to the parameter name
Parameter value range	You can check the range of values that can be parameter values
Parameter application method	You can check the time when the parameter value is to be applied. The following choices for timing are available: • immediate: The value is applied immediately • reboot: The value is applied when the DB instance is restarted
Parameter data type	You can check the data type of the parameter value (example: Integer, String)
Description	You can check the description of the parameter

Item	Description
Flags that indicate changeability	You can check whether or not the parameter value can be changed. "FALSE" indicates that it cannot be changed
Lowest version that supports the parameter	You can check what the lowest version that supports the parameter in the parameter group family is
Source of the default value	You can check where the default value is set from. • engine: Default value that is provided by the database engine • system: Default value that is set by K5 IaaS system

Changing a DB Parameter Value

In order to change the parameter value to be set on the database, modify the DB parameter group information that includes the parameter that you want to modify, instead of specifying individual parameters.

Table 115: Items That Can Be Changed for Each Parameter

Item	Description
Parameter name	Specify the parameter whose value you want to change. Specify the parameter name that is specified in the information of the DB parameter group
Parameter value	Specify the value that you want to change the parameter value to. Specify a value in the parameter value range that is specified in the information of the DB parameter group
Parameter application method	Specify the time when the parameter value is applied. The following choices for the timing are available: • immediate: The value is applied immediately • pending-reboot: The value is applied when the DB instance is restarted

Note

You can modify a maximum of 20 parameters per request.

Deleting a DB Parameter Group

Specify the ID of a DB parameter group in the project to delete a DB parameter group that is no longer necessary.

5.3 Managing a Database

5.3.1 Database Operations

This section describes functions that can be used after you put virtual database servers into operation.

Changing Database Settings

Table 116: Settings That Can Be Changed

Settings	Description	Restarting of Virtual Database Servers
Database engine version	Changes the version of the database engine	Necessary
Database instance type	Changes the type of the DB server instance	Necessary
Database capacity expansion, or changing of disk type	Increases the data block storage capacity, or changes the disk type	Necessary
Security group settings	Changes the security group information that is set on DB instances	Not necessary
Automatic backup time	Changes the time when automatic backup is performed	Not necessary
Backup retention period	Changes the backup retention period	Not necessary
Automatic maintenance	Changes whether or not to perform automatic maintenance	Not necessary
Automatic maintenance time	Changes the time when automatic maintenance is performed	Not necessary[5]
Automatic minor version upgrade	Changes whether or not to perform a minor version upgrade of the DB engine automatically	Not necessary[6]

Starting/Terminating/Restarting a Virtual Database Server

You can start up, terminate, or restart a virtual database server.

Deleting a Virtual Database Server

Take one of the following actions and then delete the DB server instance:

[5] Restarting is necessary when you perform maintenance.
[6] Restarting is necessary when you upgrade.

- Create a snapshot before deletion

Tip

If you create a snapshot before you delete a database instance, you can create a new DB server by restoring the snapshot that contains the DB server in the condition it was before it was deleted.

- Delete immediately

Settings for Monitoring

You can monitor the resources on virtual database servers. You can monitor resources at the OS level, and monitor resources within the database engine.

You can set threshold values for each item, and set an action that will be taken (send e-mail) when the threshold value is exceeded.

Table 117: Settings for Monitoring

Item		Description
Check interval		1 minute
Display period	Refresh	1 hour, 3 hours, 6 hours, 9 hours, 12 hours, 1 day (by default), 3 days, 1 week
	Custom	Any part of last week, from one to seven days
Items to monitor		• CPU usage • Number of DB connections • Free disk space • Free memory space • Average number of disk I/O operations (number of times read and write are executed) per sec. • Number of requests in disk IO queue (read and write requests) • Delay time behind the read replica master • Binary log size • Average value of number of bytes that are read from disk or written to disk per sec. • Average length of time that was spent per disk I/O (read and write) operation • Amount of swap space in use

Monitoring of Logs

You can view and download PostgreSQL engine logs.

Note

Log files are rotated every hour. 72 hours of data is retained.

Creating a Read Replica

You can create a read replica in order to distribute the load for database references.

Important

A read replica differs from redundancy settings in that the data is duplicated asynchronously from the source database. Therefore, you may view old data as a result of an SQL reference.

Managing Database Snapshots

You can create a snapshot of a virtual database server at a specific point in time, and create a new virtual database server by using the snapshot. Following functions related to snapshots are provided:

- Creation of a snapshot
- List display of a snapshot
- Information display of a snapshot
- Duplication of a snapshot
- Deletion of a snapshot

Event Notification Settings

You can configure settings so that you receive notifications (via email) regarding events that take place on a virtual database server.

Table 118: List of Events

Event Types	Description
Availability	Shutdown and restarting of databases
Backup	Start and end of backups
Configuration Change	Change of security groups, start and end of scaling of virtual database servers, and so on.
Creation	Creation or deletion of instances and snapshots
Failover	Start and completion of failover
Low Storage	Case where the allocated storage is full
Maintenance	Change to an off-line state or recovery to an on-line state due to a patch application
Recovery	Restoration of virtual database servers
Restoration	Restoration of database instances by performing point-in-time recovery or by using snapshots

5.3.2 Available Commands and SQL Statements

This section describes the SQL statements, which are client commands available with the Database as a Service.

Client Commands

The list of commands available with this Database as a Service is shown below.


Tip For details on each client command, refer to the PostgreSQL documentation, "PostgreSQL Client Applications."

Table 119: List of Available Client Commands

Command Name	Purpose
clusterdb	Clusters a database (physically reorders the tables, based on the index information)

Command Name	Purpose
createdb	Creates a new database Note: You cannot specify the -E option.
createuser	Defines a new user account
dropdb	Removes a database
dropuser	Removes a user account
ecpg	Uses an embedded SQL C preprocessor
pg_config	Provides information about the installed version
pg_dump	Extracts a database into a script file or other archive file
pg_dumpall	Extracts a database cluster into a script file
pg_restore	Restores a database from an archive file created by pg_dump
psql	Executes a command interactively
reindexdb	Reindexes a database
vacuumdb	Garbage-collects and analyzes a database

SQL Statements

The list of SQL statements available with this Database as a Service is shown below.

Tip: For details on each SQL statement syntax, refer to the PostgreSQL documentation, "SQL Commands."

Table 120: List of Available SQL Statements

SQL Statement	Purpose
ABORT	Aborts the current transaction
ALTER AGGREGATE	Changes the definition of an aggregate function
ALTER COLLATION	Changes the definition of a collation
ALTER CONVERSION	Changes the definition of a conversion
ALTER DATABASE	Changes a database (Note 1)
ALTER DEFAULT PRIVILEGES	Defines default access privileges
ALTER DOMAIN	Changes the definition of a domain
ALTER EXTENSION	Changes the definition of an extension
ALTER FUNCTION	Changes the definition of a function (Note 1)
ALTER GROUP	Changes a role name or membership
ALTER INDEX	Changes the definition of an index
ALTER LARGE OBJECT	Changes the definition of a large object
ALTER OPERATOR	Changes the definition of an operator

SQL Statement	Purpose
ALTER OPERATOR CLASS	Changes the definition of an operator class
ALTER OPERATOR FAMILY	Changes the definition of an operator family
ALTER ROLE	Changes a database role (Note 1)
ALTER SCHEMA	Changes the definition of a schema
ALTER SEQUENCE	Changes the definition of a sequence generator
ALTER TABLE	Changes the definition of a table
ALTER TABLESPACE	Changes the definition of a tablespace
ALTER TEXT SEARCH CONFIGURATION	Changes the definition of a text search configuration
ALTER TEXT SEARCH DICTIONARY	Changes the definition of a text search dictionary
ALTER TEXT SEARCH PARSER	Changes the definition of a text search parser
ALTER TEXT SEARCH TEMPLATE	Changes the definition of a text search template
ALTER TRIGGER	Changes the definition of a trigger
ALTER TYPE	Changes the definition of a type
ALTER USER	Changes a database role
ALTER VIEW	Changes the definition of a view
ANALYZE	Collects statistics about a database
BEGIN	Starts a transaction block
CHECKPOINT	Forces a transaction log checkpoint
CLOSE	Closes a cursor
CLUSTER	Clusters a table according to an index
COMMENT	Defines or changes the comment of an object
COMMIT	Commits the current transaction
COMMIT PREPARED	Commits a transaction that was earlier prepared for two-phase commit
COPY	Copies data between a client and a database table (Note 2)
CREATE AGGREGATE	Defines a new aggregate function (Note 4)
CREATE CAST	Defines a new cast (Note 4)
CREATE COLLATION	Defines a new collation
CREATE CONVERSION	Defines a new encoding conversion (Note 4)
CREATE DATABASE	Creates a new database (Note 6)
CREATE DOMAIN	Defines a new domain
CREATE EXTENSION	Installs an extension
CREATE FUNCTION	Defines a new function (Note 1) (Note 3)
CREATE GROUP	Defines a new database role

SQL Statement	Purpose
CREATE INDEX	Defines a new index
CREATE OPERATOR	Defines a new operator (Note 4)
CREATE OPERATOR CLASS	Defines a new operator class (Note 4)
CREATE OPERATOR FAMILY	Defines a new operator family
CREATE ROLE	Defines a new database role
CREATE RULE	Defines a new rewrite rule
CREATE SCHEMA	Defines a new schema
CREATE SEQUENCE	Defines a new sequence generator
CREATE TABLE	Define a new table
CREATE TABLE AS	Defines a new table from the results of a query
CREATE TABLESPACE	Defines a new tablespace (Note 5)
CREATE TEXT SEARCH CONFIGURATION	Defines a new text search configuration
CREATE TEXT SEARCH DICTIONARY	Defines a new text search dictionary
CREATE TEXT SEARCH PARSER	Defines a new text search parser (Note 4)
CREATE TEXT SEARCH TEMPLATE	Defines a new text search template (Note 4)
CREATE TRIGGER	Defines a new trigger (Note 4)
CREATE TYPE	Defines a new data type (Note 4)
CREATE USER	Defines a new database role
CREATE VIEW	Defines a new view
DEALLOCATE	Deallocates a prepared statement
DECLARE	Defines a cursor
DELETE	Deletes rows of a table
DISCARD	Discards session state
DO	Executes an anonymous code block
DROP AGGREGATE	Removes a defined aggregate function
DROP CAST	Removes a defined cast
DROP COLLATION	Removes a defined collation
DROP CONVERSION	Removes a defined conversion
DROP DATABASE	Removes a defined database
DROP DOMAIN	Removes a defined domain
DROP EXTENSION	Removes a defined extension
DROP FUNCTION	Removes a defined function
DROP GROUP	Removes a defined database role

SQL Statement	Purpose
DROP INDEX	Removes a defined index
DROP OPERATOR	Removes a defined operator
DROP OPERATOR CLASS	Removes a defined operator class
DROP OPERATOR FAMILY	Removes a defined operator family
DROP OWNED	Removes database objects owned by a defined database role
DROP ROLE	Removes a defined database role
DROP RULE	Removes a defined rewrite rule
DROP SCHEMA	Removes a defined schema
DROP SEQUENCE	Removes a defined sequence
DROP TABLE	Removes a defined table
DROP TABLESPACE	Removes a defined tablespace
DROP TEXT SEARCH CONFIGURATION	Removes a defined text search configuration
DROP TEXT SEARCH DICTIONARY	Removes a defined text search dictionary
DROP TEXT SEARCH PARSER	Removes a defined text search parser
DROP TEXT SEARCH TEMPLATE	Removes a defined text search template
DROP TRIGGER	Removes a defined trigger
DROP TYPE	Removes a defined data type
DROP USER	Removes a defined database role
DROP VIEW	Removes a defined view
END	Commits the current transaction
EXECUTE	Executes a prepared statement
EXPLAIN	Shows the execution plan of a query statement
FETCH	Retrieves rows from a table using a cursor
GRANT	Defines access privileges
INSERT	Creates new rows in a table
LISTEN	Listens for a notification
LOCK	Locks a table
MOVE	Positions a cursor
NOTIFY	Generates a notification
PREPARE	Prepares a statement for execution
PREPARE TRANSACTION	Prepares the current transaction for two-phase commit
REASSIGN OWNED	Changes the ownership of database objects owned by a database role

SQL Statement	Purpose
REINDEX	Rebuilds indexes
RELEASE SAVEPOINT	Destroys a previously defined savepoint
RESET	Restores the value of a run-time parameter to the default value (Note 1)
REVOKE	Removes access privileges
ROLLBACK	Aborts the current transaction
ROLLBACK PREPARED	Cancels a transaction that was earlier prepared for two-phase commit
ROLLBACK TO SAVEPOINT	Rolls back to a savepoint
SAVEPOINT	Defines a new savepoint within the current transaction
SECURITY LABEL	Defines or changes a security label applied to an object
SELECT	Retrieves rows from a table or view
SELECT INTO	Defines a new table from the results of a query
SET	Changes a run-time parameter (Note 1)
SET CONSTRAINTS	Sets constraint check timing for the current transaction
SET ROLE	Sets the user identifier of the current session
SET SESSION AUTHORIZATION	Sets the session user identifier and the user identifier of the current session
SET TRANSACTION	Sets the characteristics of the current transaction
SHOW	Shows the value of a run-time parameter
START TRANSACTION	Starts a transaction block
TRUNCATE	Empties a table or set of tables
UNLISTEN	Stops listening for a notification
UPDATE	Updates rows of a table
VACUUM	Garbage-collects and optionally analyzes a database
VALUES	Computes a set of rows

- Note 1: When you specify configuration_parameter, you cannot specify a parameter that takes a directory path as a value.
- Note 2: You cannot specify any file names for FROM and TO. Specify STDIN or STDOUT.
- Note 3: You can only specify the languages SQL, internal, or plpgsql for LANGUAGE.
- Note 4: If you specify a function, you can only specify a function that is implemented in SQL or the plpgsql language.
- Note 5: The directory specified in the LOCATION clause is generated under /userdata/tblspc automatically. You do not have to prepare the directory in advance. In the LOCATION clause, you can specify a path within a length of 958 bytes.
- Note 6: You cannot specify the ENCODING clause.

Note

You cannot use the following SQL statements that are available in PostgreSQL 9.2:

- ALTER FOREIGN DATA WRAPPER
- ALTER FOREIGN TABLE
- ALTER LANGUAGE

- ALTER SERVER
- ALTER USER MAPPING
- CREATE FOREIGN DATA WRAPPER
- CREATE FOREIGN TABLE
- CREATE LANGUAGE
- CREATE SERVER
- CREATE USER MAPPING
- DROP FOREIGN DATA WRAPPER
- DROP FOREIGN TABLE
- DROP LANGUAGE
- DROP SERVER
- DROP USER MAPPING
- LOAD

5.3.3 Database User

When you create a virtual database server, create the database management user and the system user as well. The points to note are as shown below.

Database Management User (Master User)

When you create the virtual database server, create the master user, who connects to the database and manages the database. The following privileges are granted to the master user:

- create role
- create db
- login

System User


Warning

If you delete system users (rdbadmin, rdbrepladmin, rdb_superuser), serious problems may occur with operations. Be careful not to delete them.

5.3.4 Failover

In a database environment where redundancy settings are enabled, if the system determines that the active virtual database server is down or unavailable, the system switches to the standby virtual database server. This operation is called failover.

A failover occurs when one of the following events is detected on the active DB server:

- Failure of a physical host
- Failure of an active virtual database server
- Changing of the virtual database server type
- Expansion of the database data area
- Restarting of a virtual database server by specifying "forced failover"


Note

After a failover occurs, it will take about one to five minutes to switch from the active server to the standby server.

Important If a failover occurs, the connection to the database will be lost. Therefore, you must implement the process to reconnect to the database on the application side.

5.3.5 Database Recovery

You can perform recovery of virtual database servers from the following two types of data:

- Data that was acquired based on the automatic backup conditions that you specified when you created the virtual database server
- Snapshot data that was taken at a specific point in time

The difference between the types of data that is used for recovery is described as follows:

- Data that was acquired by automatic backup

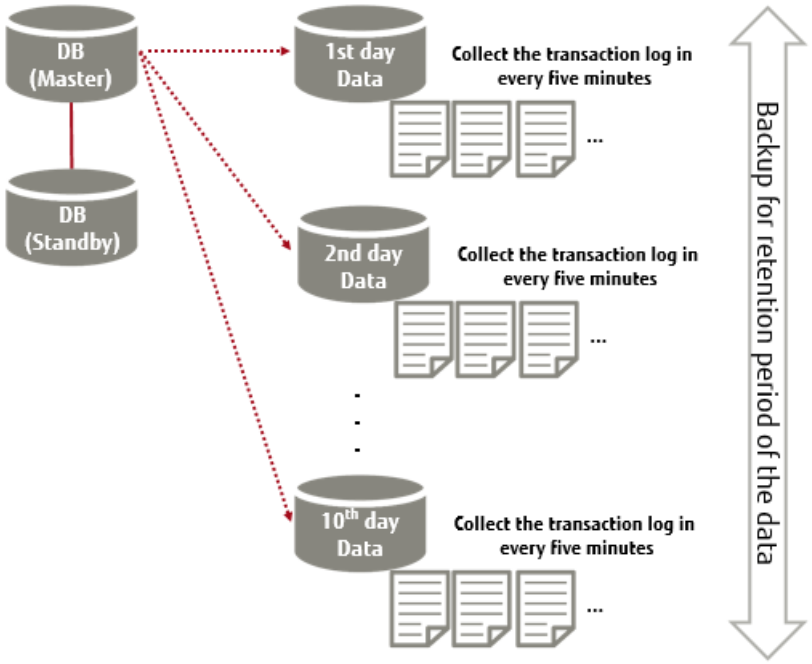
  Once a day, backup of all data is performed in the time period that you specified for backup when you created the virtual database server. After that, the transaction log is continuously backed up every five minutes.

  Tip The data that is acquired by automatic backup is given a name that complies with the following naming conventions:

  ```
  auto-snapshot-<DB instance ID>-<year>-<month>-<day>-<hour>-<minute>-<second>
  ```

  The backup data is stored for the duration of the backup retention period that you specified when you created the virtual database server, and data whose retention period has ended is automatically deleted.

  Figure 32: Automatic Backup



- Snapshot data that was taken at a specific point in time

  The data that is created with the database snapshot function will be retained until the user deletes the snapshot data.

Database Recovery Method

There are two methods of recovering databases, as shown below:

- Point-in-time recovery

  Out of the data that has been backed up automatically, you can specify the date and time of the point to which you intend to recover the database. Recover the database by specifying a point in time between the point when the backup was created and the point when the backup of the latest transaction log was created (at maximum five minutes prior).
- Recovery from snapshot data that you specify

  Recover the database by specifying snapshot data that was acquired at a specific point in time.

Important Create a new virtual database server from the snapshot data you use to recover the database. Confirm that there is no problem with the recovered data before you delete the old virtual database server.

Note Since a new virtual database server will be created, you must prepare in advance a DB subnet group and other elements that are necessary for building a database.

Note You can recover the database only in the same region where the data that will be used for recovery exists.

Part 6: Email Delivery Service

Topics:

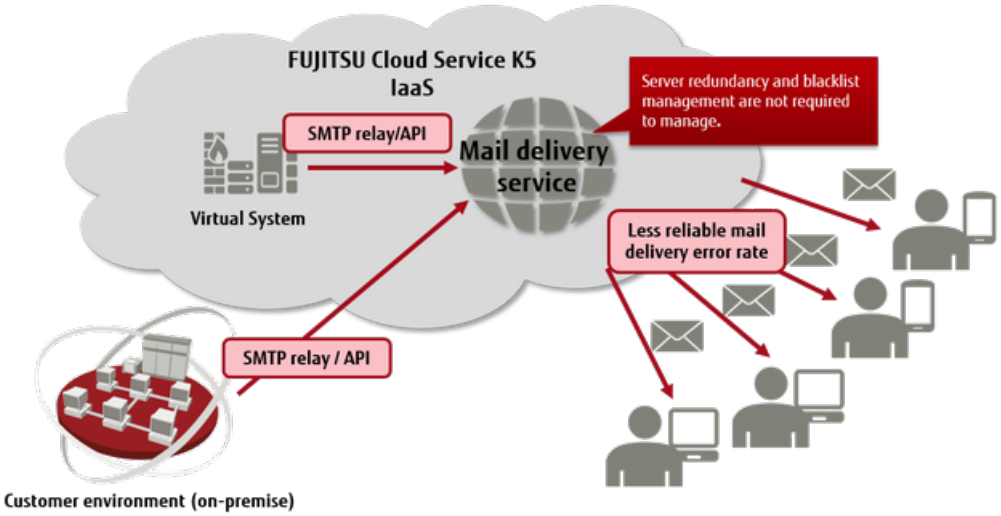
K5 IaaS provides an email delivery service.

6.1 Overview of Functions

6.1.1 Email Delivery Service

FUJITSU Cloud Service K5 IaaS provides a high-quality, efficient email delivery service. Tedious system operations such as building and managing an email server are handled by this service, allowing you to make significant reductions in operating cost.

Figure 33: Overall Layout of the Email Delivery Service



Functions Included

- Authentication Functions
  - Authentication of the address of the sender
  - Authentication of the domain
- Email delivery functions
  - Send by using an SMTP interface
  - Send by using an API
- Email certificate settings
  - SPF authentication settings
- Monitoring of results of sending
- Scheduling email

Limiting Values

Table 121: List of Limiting Values Related to the Email Delivery Service

Item	Limiting Values
Maximum Number of Emails Sent per Second	• Using API: 50 (1 request/second x 50 recipients) • Using SMTP interface: 500
Maximum Number of Registered Email Addresses per Domain	1,000
Maximum Number of Requests per Second	• 10 (different requests)

Item	Limiting Values
	• 1 (same request)
Number of Recipients per Request	50
Maximum Size per Email	• Using API: 2 MB • Using SMTP interface: 10 MB  This includes email attachments. Note

6.2 Authentication

6.2.1 Authentication Functions

There are two methods for authenticating the users of email services:

- Authentication by individual email addresses
- Bulk authentication by domain

You can specify only registered domains and email addresses as the From address (Envelope From and Header From).

Table 122: Settings for the Send Source

Item	Description
From Address	You can specify only an email address that has been registered, or an address with a domain that matches a registered domain name.
Settings for the Send Destination	• Local part: 64 bytes or less • 255 bytes or less in total (including the local part) • RFC-compliant (partially)

6.3 Mail Delivery

6.3.1 Email Functions

An interface for sending email is provided. You can use SMTP or REST API to send email.

SMTP Interface

You can connect from your email server to the SMTP server for this service to send email.

Table 123: Connection Information

Item	Settings
Server	ess-smtp.cloud.nifty.com
Port	587 (STARTTLS) 465 (TLS Wrapper)
Authentication	User authentication using SMTP-AUTH
Destination Email Address	• Local part: 64 bytes or less • 255 bytes or less in total (including the local part)

REST API

You can use REST API to send email.

6.3.2 Scheduling an Email to Be Delivered

When you send an email, you can specify the time for the email to be delivered.

Specifying the Time to Deliver an Email

Specify the time to deliver the email, in the following format, in the subject line:

```
[yyyy/MM/dd HH:mm] Content of subject line
```

Note

The time zone used for specification is the JST (Japan Standard Time) time zone.

Note

When the email is delivered, the part that specifies the time ([yyyy/MM/dd HH:mm]) is automatically deleted from the subject line.

6.4 Email Certificate

6.4.1 Authentication Settings for Sender Policy Framework

If you use the email delivery service to deliver email, information is provided that allows you to use SPF authentication to certify that the sender is legitimate.

Register the following values on the DNS server that you use to manage the domains of source email addresses:

Table 124: Settings for SPF Records

Setting Target	Settings
Record Type	SPF
Record Value	v=spf1 include:ess-spf.cloud.nifty.com -all

Note If the record already exists, add the following value: "include:ess-spf.cloud.nifty.com"

6.5 Monitoring

6.5.1 Monitoring the Status of Delivery

You can check the delivery status of email that was sent during the previous two weeks.

The following information can be obtained in 15-minute intervals for the previous two weeks:

Table 125: Items That Can Be Monitored

Item	Description
Emails Sent	This is the total number of emails that have been sent.
Bounces[7]	This is the total number of emails that were not delivered and returned to the sender.
Emails Refused[8]	This is the total number of emails that were refused by the incoming mail server at the destination.

Note

It is not possible to check the details of each email that was bounced.

[7] An email is determined to have bounced when any of the following errors occur: Address unknown, email refused, mailbox full, congestion, domain name resolution failure, server connection timeout, SMTP command response timeout, delivery period expired, other transmission errors

[8] An email is refused when the incoming mail server at the destination returns an error code of 400 or 500.

Part 7: Content Delivery Network Service

Topics:

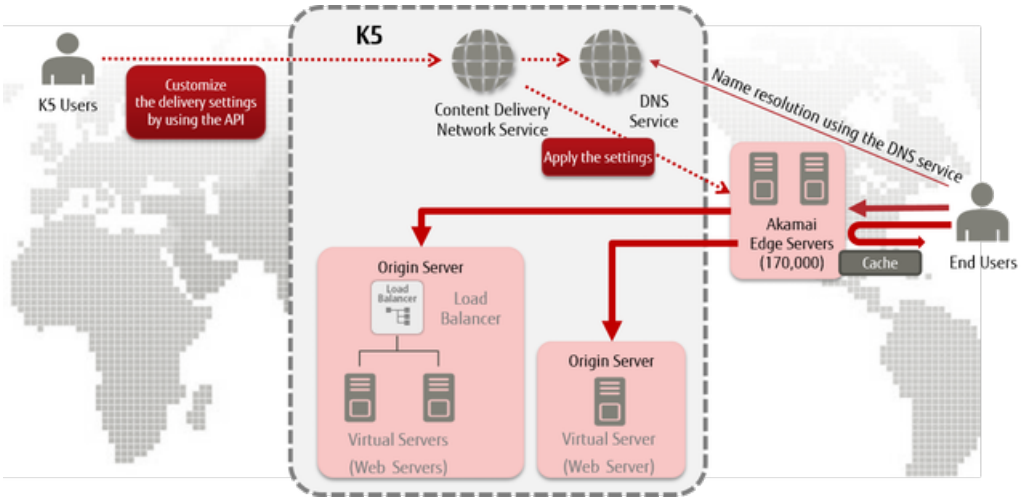
This service uses edge servers provided by Akamai to deliver content around the world.

7.1 Overview of Functions

7.1.1 Content Delivery Network Service

This service uses Akamai Intelligent Platform edge servers provided by Akamai Technologies Inc., located around the world, to cache and deliver the web content on your origin server. It makes content delivery faster and more efficient by directing end users who access your web content to the nearest edge server.

Figure 34: Overall Image of Content Delivery Network Service



Functions Included

- Acquire Delivery Settings List Function

  Acquire a list of delivery settings that can be set for your project.
- Create Delivery Settings Function

  Create delivery settings to start content delivery.
- Acquire Delivery Settings Function

  Specify the ID of the delivery settings you have created, to acquire the content for those delivery settings.
- Edit Delivery Settings Function

  Specify the ID of the delivery settings you have created, to edit the content for those delivery settings.
- Delete Delivery Settings Function

  Specify the ID of the delivery settings you have created, to delete those delivery settings.
- Delete Cache Function

  Specify a delivery settings ID that you have created to delete cached content from an edge server.
- Create Report Function

  You can create statistical information from the total amount for each of the delivery settings that have been created within the range of your project.
- Acquire Report Function

  Acquire statistical information that was created with the Create Report function in json format.
- Acquire Access Log Function

Store edge server access logs in a container that you created in object storage.

Content That Can Be Delivered

Table 126: List of Content That Can Be Delivered

Content Type	Details	Description	Deliverable?
Website content	Static content	.jpg, .pdf, .html, .css and so on.	Yes
	Dynamic content	Content that is generated by software on a web server, but not personalized. Examples: • Top pages generated on a server • Query strings for displaying weather forecasts ("?date=20141230")	Yes
		Content that is generated by software on a web server, and personalized. Examples: • Shopping carts • Questionnaire responses that include personal information and such	No (*1)
Streaming content	Progressive download method	Download method of content delivery used by YouTube and so on.	Yes
	Live streaming method	Real time method of content delivery used by Ustream and so on.	No

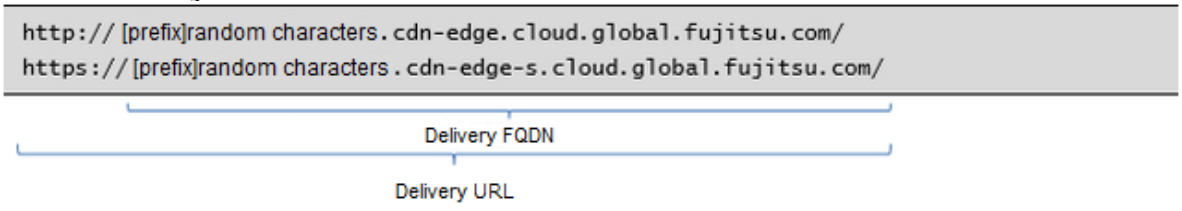
*1: For example, the content of a shopping cart should not be cached on an edge server. Therefore, create cache operation control rules that follow the cache settings to control whether cache is allowed on the origin server. For details, refer to API Reference Manual.

Delivery URL

When you create delivery settings, a unique delivery URL is assigned for the website that the end user can access.

- If you do not have your own domain (K5 cdn-edge domain)

  A URL that includes K5 cdn-edge domain provided by the content delivery network service is used as the delivery URL. The configuration of the delivery URL for both http and https is shown in the figure below.



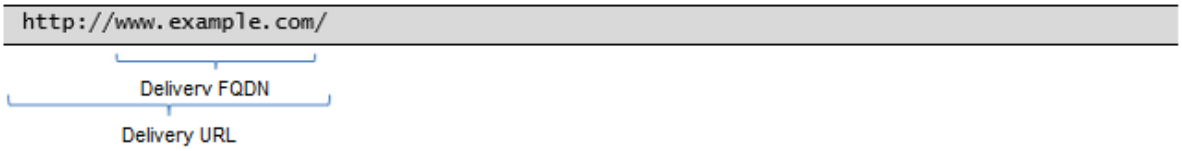
- If you have your own domain

  If you have your own domain, you can use that domain to deliver content. In addition to creating the delivery settings for the content delivery network service, you must also set CNAME for common-http.cdn-edge.cloud.global.fujitsu.com on a DNS server.

  An example of a DNS resource record is shown below.

```
www.example.com.  IN CNAME common-http.cdn-edge.cloud.global.fujitsu.com.
```

  The configuration for the delivery URL and delivery FQDN is shown in the figure below.



Secure Delivery

You can use HTTPS to securely deliver content from an edge server to the end user. HTTPS delivery is available only for assigned domains that have been assigned by the content delivery network service. Your own domains are not supported.

Note The following protocols are supported by the edge servers: TLS1.0, TLS1.1, TLS1.2. SSLv2, SSLv3, and RC4 (refer to RFC7465) are not supported.

If you use a virtual server or a load balancer as your origin server, you must provide a certificate that links with the certificates shown in the table below.

Table 127: List of Server Certificates That Can Be Used with an Origin Server for Access via HTTPS

Common Name	Expiry Date	SHA-1 Fingerprint
AddTrust External CA Root	May 30 2020	02faf3e291435468607857694df5e45b68851868
AffirmTrust Commercial	December 31 2030	f9b5b632455f9cbeec575f80dce96e2cc7b278b7
AffirmTrust Networking	December 31 2030	293621028b20ed02f566c532d1d6ed909f45002f
AffirmTrust Networking	May 29 2029	5f3b8cf2f810b37d78b4ceec1919c37334b9c774
AffirmTrust Premium	December 31 2040	d8a6332ce0036fb185f6634f7d6a066526322827
AffirmTrust Premium	September 30 2023	36b12b49f9819ed74c9ebc380fc6568f5dacb2f7
America Online Root Certification Authority 2	September 29 2037	85b5ff679b0c79961fc86e4422004613db179284
Baltimore CyberTrust Root	May 13 2025	d4de20d05e66fc53fe1a50882c78db2852cae474
Certum CA	June 11 2027	6252dc40f71143a22fde9ef7348e064251b18118
Class 2 Primary CA	July 7 2019	74207441729cdd92ec7931d823108dc28192e2bb
COMODO Certification Authority	January 1 2030	6631bf9ef74f9eb6c9d5a60cba6abed1f7bdef7b

Common Name	Expiry Date	SHA-1 Fingerprint
Cybertrust Global Root	December 15 2021	5f43e5b1bff8788cac1cc7ca4a9ac6222bcc34c6
DigiCert Assured ID Root CA	November 10 2031	0563b8630d62d75abbc8ab1e4bdfb5a899b24d43
DigiCert Global Root CA	November 10 2031	a8985d3a65e5e5c4b2d7d66d40c6dd2fb19c5436
DigiCert High Assurance EV Root CA	November 10 2031	5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25
DST Root CA X3	September 30 2021	dac9024f54d8f6df94935fb1732638ca6ad77c13
Entrust Root Certification Authority	November 28 2026	b31eb1b740e36c8402dadc37d44df5d4674952f9
Entrust.net Certification Authority (2048)	July 24 2029	503006091d97d4f5ae39f7cbe7927d7d652d3431
GeoTrust Global CA	May 21 2022	de28f4a4ffe5b92fa3c503d1a349a7f9962a8212
GeoTrust Primary Certification Authority	July 17 2036	323c118e1bf7b8b65254e2e2100dd6029037f096
GeoTrust Primary Certification Authority - G3	December 2 2037	039eedb80be7a03c6953893b20d2d9323a4c2afd
Global Chambersign Root	October 1 2037	339b6b1450249b557a01877284d9e02fc3d2d8e9
GlobalSign	December 15 2021	75e0abb6138512271c04f85fddde38e4b7242efe
GlobalSign	March 18 2029	d69b561148f01c77c54578c10926df5b856976ad
GlobalSign Root CA	January 28 2028	b1bc968bd4f49d622aa89a81f2150152a41d829c
Go Daddy Root Certificate Authority - G2	January 1 2038	47beabc922eae80e78783462a79f45c254fde68b
Network Solutions Certificate Authority	January 1 2030	74f8a3c3efe7b390064b83903c21646020e5dfce
QuoVadis Root CA 2	November 25 2031	ca3afbcf1240364b44b216208880483919937cf7
QuoVadis Root CA 2	June 30 2034	2796bae63f1801e277261ba0d77770028f20eee4
QuoVadis Root CA 3	November 25 2031	1f4914f7d874951dddae02c0befd3a2d82755185
QuoVadis Root Certification Authority	March 18 2021	de3f40bd5093d39b6c60f6dabc076201008976c9
SecureTrust CA	January 1 2030	8782c6c304353bcfd29692d2593e7d44d934ff11
StartCom Certification Authority	September 18 2036	3e2bf7f2031b96f38ce6c4d8a85d3e2d58476a0f

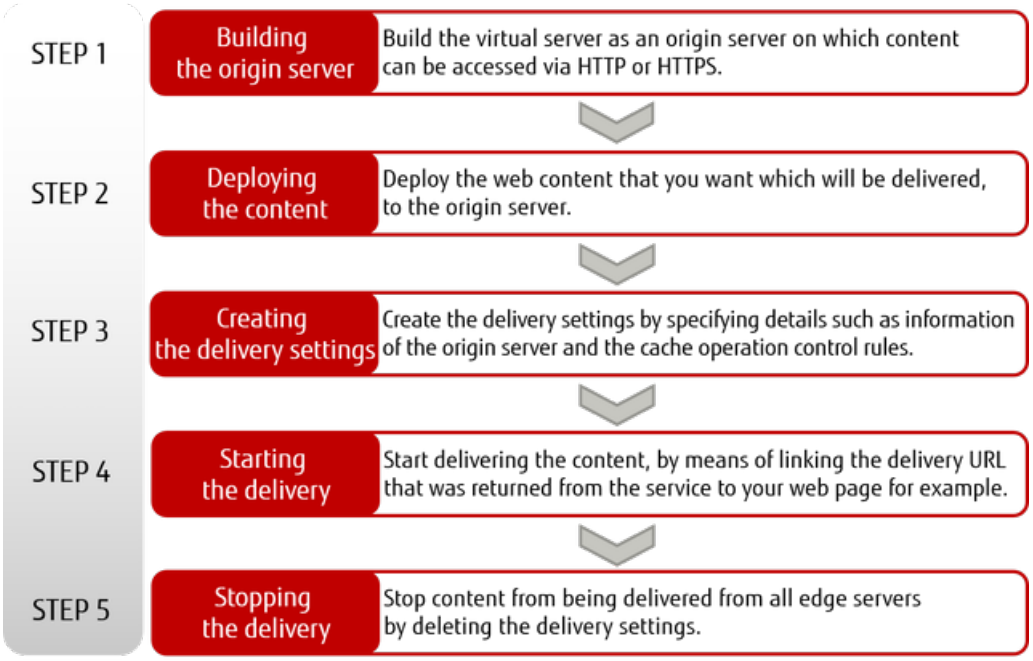
Common Name	Expiry Date	SHA-1 Fingerprint
SwissSign Gold CA - G2	October 25 2036	d8c5388ab7301b1b6ed47ae645253a6f9f1a2761
SwissSign Silver CA - G2	October 25 2036	9baae59f56ee21cb435abe2593dfa7f040d11dcb
SwissSign Silver CA - G2	June 6 2037	feb8c432dcf9769aceae3dd8908ffd288665647d
TC TrustCenter Class 2 CA II	January 1 2026	ae5083ed7cf45cbc8f61c621fe685d794221156e
thawte Primary Root CA	July 17 2036	91c6d6ee3e8ac86384e548c299295c756c817b81
thawte Primary Root CA - G3	December 2 2037	f18b538d1be903b6a6f056435b171589caf36bf2
UTN - DATACorp SGC	June 25 2019	58119f0e128287ea50fdd987456f4f78dcfad6d4
UTN-USERFirst-Hardware	July 10 2019	0483ed3399ac3608058722edbc5e4600e3bef9d7
VeriSign Class 3 Public Primary Certification Authority - G3	July 17 2036	132d0d45534b6997cdb2d5c339e25576609b5cc6
VeriSign Class 3 Public Primary Certification Authority - G5	July 17 2036	4eb6d578499b1ccf5f581ead56be3d9b6744a5e5
VeriSign Class 4 Public Primary Certification Authority - G3	July 17 2036	c8ec8c879269cb4bab39e98d7e5767f31495739d
VeriSign Universal Root Certification Authority	December 2 2037	3679ca35668772304d30a5fb873b0fa77bb70d54

Note

- Self-signed certificates are not supported.
- An unlimited license is not required. Provide a certificate only for the origin server.

How to Use This Service

Figure 35: How to Start the Content Delivery Network Service



Points to Note

- You can use only port 80 for access via HTTP, and only port 443 for access via HTTPS.
- Charges for content delivery network service are due 2 months after the end of the billing period.
- DNS-related operations for the content delivery network service cannot be performed during regularly scheduled maintenance for the DNS service (from midnight to 1am on the 1st of each month).
- You will be notified of the time and details of any maintenance to be performed by Akamai.

Tip

Content delivery is not stopped during maintenance.

7.2 Delivery Settings

7.2.1 Delivery Settings Function

This function allows you to manage delivery settings, in order to control the delivery of content from an edge server. There is also a function for saving edge server access logs in object storage.

Acquiring the Delivery Settings List

You can acquire a list of the delivery settings you have created, delivery URLs, and access log status.

Tip

Even if a delivery status is "undeployed," it will appear in the list.

Creating Delivery Settings

Content delivery starts when you create delivery settings. Specify the following information to create delivery settings.

Table 128: Creating Delivery Settings (List of Items That Can Be Set)

Item	Description	Required
FQDN Information	Specify one of the following formats for the FQDN information that you want to deliver: • When using your own domain: Specify FQDN Note You must set CNAME on the DNS server. • When not using your own domain: Specify a prefix	
Delivery Protocol Scheme	Specify one of the following: Tip If omitted, this is set to "http". • For delivery by HTTP: "http" • For delivery by HTTPS: "https" If you access an edge server by HTTP, the connection is redirected to HTTPS.	
Initial Status	Specify the initial status for the delivery settings. Tip If omitted, this is set to "activate". • To enable content delivery immediately: "activate" • To disable content delivery: "deactivate"	
Access Log Storage Destination	Specify a container in object storage to use as the storage destination for access logs. Tip If this is left blank, no access log is acquired.	

Item	Description	Required
	Note You can only use the object storage container on Eastern Japan Region 1 (jp-east-1)	
Access Log Prefix	Specify the prefix to assign to the object name of the access log.	
Caching Behavior Control Rules	Specify delivery operations in json format, such as specifying the origin server to use for delivery or specifying a cache TTL with a condition such as an extension or path. Tip Rules are used to implement an action specified as a "behavior" when the conditions specified in "match" are achieved. For details, refer to API Reference Manual.	Yes

Table 129: Match (List of Items That Can Be Set)

Item	Description
URL	You can set a character string that identifies the URL to be accessed by the end user. Examples: jpg, index.html, /img/*, /*
Method	You can set the HTTP methods to be accessed by the end user. (Example: "GET, POST") • GET • POST • PUT • DELETE • HEAD • PATCH
Scheme	You can set HTTP or HTTPS as the scheme to be accessed by the end user.
Header	You can set whether there is a header to be accessed by the end user. Example: "User-Agent: xxx yyy zzz"

Table 130: Behavior (List of Items That Can Be Set)

Item	Description
Origin Settings	You can specify FQDN and accompanying information for the origin server. As accompanying information, you can specify information for the origin server to determine if access is via the content delivery network service. Examples of accompanying information: • Host header

Item	Description
	• Cache key that affects cache conditions
Cache TTL Settings	You can specify cache TTL as a fixed value, dependent on the origin, etc.
Query Strings Used by Cache Keys	For dynamic pages that can keep a cache, you can specify behaviors that identify cache keys, such as excluding a query string that includes a session ID.
Disable Cache	You can disable the cache on an edge server at a specified time (including "immediately").
IP Address Restriction	You can restrict access by end users from specific IP addresses.
Region Restriction	You can restrict access by end users from specific regions.
Referer Restriction	You can restrict access by end users from specific referers.
Failover	If the originally specified origin server goes down, you can acquire content from a different origin server.

Acquiring Delivery Settings

Specify the ID of the delivery settings, to acquire the following content for those specific delivery settings.

- Caching behavior control rules
- Delivery URL
- Delivery protocol
- Delivery status
- Access log storage destination
- Access log status

Editing Delivery Settings

Specify the ID of the delivery settings, to edit the content for those specific delivery settings. You can make changes to the following content:

- Caching behavior control rules
- Delivery status
- Start/stop storing access logs, access log storage destination

Note

- For caching behavior control rules, specify the content in its entirety rather than specifying the content partially.
- You cannot make changes to delivery FQDN.

Deleting Delivery Settings

You can delete delivery settings that have been created, and stop content delivery. When the settings are deleted, the delivery URL is disabled and can no longer be accessed by end users. Storing access logs is also stopped.

Note

- Some time is required for the command to delete delivery settings reaches all edge servers.
- If delivery is performed on your own domain, you should disable the CNAME setting.

Deleting Cache

You can delete the cache for content that matches a specific delivery URL from an edge server, such as when replacing the files on an origin server or when incorrect files have been delivered.

Note

- Some time is required for the command to delete cache to reach all edge servers.
- If you delete the cache, content will be fetched from the origin server the next time there is access by an end user.

Access Log Function

You can store access logs in the container for object storage that was specified when creating delivery settings or with the edit function for delivery settings. Storing access logs continue until the information for the storage destination is changed which stops access logs from being stored, or until the delivery settings are deleted.

Note

The time lag to start or stop storing access logs is normally about 6 hours after accessing the edge server. Some examples are shown below.

- If delivery settings that enable access logs are created at 6am and the edge server is accessed immediately, that access log can be acquired at around 12pm.
- If storing access logs are stopped around 12:30pm, affects are immediate, and the access logs that were created after 7am cannot be acquired.

Specify the following information for the storage destination for access logs.

- Name of container for object storage

  Example: "container"
- Pseudo path for the object (optional), and prefix that includes the first letters of the file name

  Example: "path/PreFix01_"

The access logs are stored for every delivery FQDN, at least every hour, and normally at least every 12MB with the object name shown below. If the delivery setting is http, "-h" is added to the end. If the setting is https, "-s" is added.

```
[Prefix][Date][ApproximateStartTime]-[StartTime+1Hour]-[Number]-[h or s].log
```

Tip

Access logs are stored even if the edge server is not accessed.

Access logs are in CSV format, and include the following information.

Note

The date/time order is not guaranteed.

Table 131: List of Items Output to Access Logs

Item	Description
date	Date (UTC)
time	Time (UTC)
cs-ip	IP address of client
cs-method	HTTP methods such as GET, POST
cs-uri	Origin URI for accessed file (If the origin settings for the caching behavior control rule that you have set are not matched, "-" is output.)

Item	Description
sc-status	Status Code response
sc-bytes	Transferred size (Units: Bytes)
time-taken	Time required from reception of request by the edge server until a response is sent (Units: ms)
cs (Referer)	Referer information (If there is no information, "-" is output.)
cs (User-Agent)	User-Agent information
cs (Cookie)	Cookie information (If there is no information, "-" is output.)

Example of access log output:

```
date,time,cs-ip,cs-method,cs-uri,sc-status,sc-bytes,time-
taken,cs(Referer),cs(User-Agent),cs(Cookie)
2015/11/6,2:10:42,8.8.8.8,GET,/test01-fe102d0e775f4918abe81c17198bd62f.cdn-
edge.cloud.global.fujitsu.com/images/privatenetwork-
img-06.jpg,200,62038,82,-,Mozilla/5.0 (Windows NT 6.1; WOW64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80
 Safari/537.36,_ga=GA1.3.547601374.14474166xx; _gat_UA-290256xx-1=1;
 _ga=GA1.2.547601374.144741663
```

7.2.2 Example Usage Scenarios and Caching Behavior Control Rules

This section presents examples of common usage scenarios, operation procedures, and caching behavior control rules when using the content delivery network service.

Website Content Delivery

- Example building procedure
  1. Create a virtual server, and build the web server that will be the origin server.
  2. Also build a load balancer (example: http://lb-001.loadbalancing-jp-east-1.cloud.global.fujitsu.com), database and so on as required.
  3. Upload the content to the origin server.
  4. Confirm that you can access the origin server from a browser.
  5. Use the content delivery network service API to create the delivery settings.

     At this time, specify the URL for the load balancer in the caching behavior control rules that you specify in the API parameters. Temporarily specify 3 days (3d) for cache TTL.
  6. When you run the API, you will acquire the delivery URL. (Example: http://xxx-123abc.cdn-edge.cloud.global.fujitsu.com)
  7. Confirm that you can access the delivery URL from a browser.
- Example of caching behavior control rules

```
{
```

```
  "rules": [
    {
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/*"
        }
      ],
      "behaviors": [
        {
          "name": "origin",
          "value": "-",
          "params": {
            "digitalProperty": "-",
            "originDomain": "lb-001.loadbalancing-jp-
east-1.cloud.global.fujitsu.com",
            "cacheKeyType": "origin",
            "cacheKeyValue": "-",
            "hostHeaderType": "origin",
            "hostHeaderValue": "-"
          }
        },
        {
          "name" : "caching",
          "type" : "honor"
          "value" : "3d"
        }
      ]
    }
  ]
}
```

Content Delivery with Your Own Domain

- Example building procedure

Tip

If you are using the DNS service for the name resolution of your own domain, you should prepare a name and so on for the CNAME setting with a domain name that you own in advance. For details, refer to the K5 DNS service.

1. Create delivery settings using the procedures described in *Website Content Delivery* on page 161, to acquire the delivery URL.

   At this time, specify your own domain (example: www.example.com) for delivery FQDN in the API parameters.
2. Confirm that you can access the delivery URL from a browser.
3. Use the DNS service to create a CNAME record.

   At this time, create the CNAME settings so that the domain points to common-http.cdn-edge.cloud.global.fujitsu.com.
4. Confirm that you can access the domain from a browser.

- Example of caching behavior control rules

```
{
  "rules": [
    {
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/*"
        }
      ],
      "behaviors": [
        {
          "name": "origin",
          "value": "-",
```

```
          "params": {
            "digitalProperty": "www.example.com",
            "originDomain": "lb-001.loadbalancing-jp-
east-1.cloud.global.fujitsu.com",
            "cacheKeyType": "origin",
            "cacheKeyValue": "-",
            "hostHeaderType": "origin",
            "hostHeaderValue": "-"
          }
        },
        {
          "name" : "caching",
          "type" : "honor"
          "value" : "3d"
        }
      ]
    }
  ]
}
```

Secure Content Delivery

- Example building procedure

  1. If the origin server is a virtual server machine or load balancer that you have created, prepare an SSL certificate. For details about what certifications you can use, refer to *Secure Delivery*.

     Tip

     If the origin server can accept only connections via HTTPS, open only port 443.

  2. Create delivery settings using the procedures described in *Website Content Delivery* on page 161.

     At this time, specify https for the delivery protocol in the API parameters. In addition, to accept edge server connections via HTTPS only, specify HTTPS in the caching behavior control rules.
  3. When you run the API, you will acquire the delivery URL for HTTPS.
  4. Confirm that you can access the delivery URL from a browser.

- Example of caching behavior control rules

```
{
  "rules": [
    {
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/*"
        },
        {
          "name": "url-scheme",
          "value": "HTTPS"
        }
      ],
      "behaviors": [
        {
          "name": "origin",
          "value": "-",
          "params": {
            "digitalProperty": "-",
            "originDomain": "lb-001.loadbalancing-jp-
east-1.cloud.global.fujitsu.com",
            "cacheKeyType": "origin",
            "cacheKeyValue": "-",
            "hostHeaderType": "origin",
            "hostHeaderValue": "-"
```

```
          }
        },
        {
          "name" : "caching",
          "type" : "honor"
          "value" : "3d"
        }
      ]
    }
  ]
}
```

Replacing Content

In this section, it is assumed that you have created delivery settings using the procedures described in *Website Content Delivery* on page 161.

- Example operation procedure
  1. Replace image files, PDF files and so on stored in the origin server.
  2. Perform "Delete Cache" for the specified object on the edge server.
  3. Wait a few minutes, and then access the delivery URL from a browser to confirm that the replaced object is displayed.

Reconsidering the Content Update Frequency

In this section, it is assumed that you have created delivery settings using the procedures described in *Website Content Delivery* on page 161.

- Example operation procedure
  1. Change the TTL setting for the specified object (URL and so on) to 1 hour. (If the cache TTL has an image such as a "good weather", do not make this change.)
  2. Thereafter, cache will be maintained on the edge server for 1 hour.
- Example of caching behavior control rules

```
{
  "rules": [
    {
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/*"
        }
      ],
      "behaviors": [
        {
          "name": "origin",
          "value": "-",
          "params": {
            "digitalProperty": "-",
            "originDomain": "lb-001.loadbalancing-jp-
east-1.cloud.global.fujitsu.com",
            "cacheKeyType": "origin",
            "cacheKeyValue": "-",
            "hostHeaderType": "origin",
            "hostHeaderValue": "-"
          }
        },
        {
          "name" : "caching",
          "type" : "fixed"
          "value" : "3d"
        }
      ],
      "matches": [
        {
```

```
          "name": "url-extension",
          "value": "jsp"
        }
      ],
      "behaviors": [
        {
          "name" : "caching",
          "type" : "fixed"
          "value" : "1h"
        }
      ]
    }
  ]
}
```

Conditional Access Restrictions

In this section, it is assumed that you have created delivery settings using the procedures described in *Website Content Delivery* on page 161.

- Example operation procedure
  1. Edit the caching behavior control rules, and use the "Edit Delivery Settings" function to change the access region for the specified path (and lower directories) to Japan only.
  2. Thereafter, access is prevented from all regions other than Japan.
- Example of caching behavior control rules

```
{
  "rules": [
    {
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/*"
        }
      ],
      "behaviors": [
        {
          "name": "origin",
          "value": "-",
          "params": {
            "digitalProperty": "-",
            "originDomain": "lb-001.loadbalancing-jp-
east-1.cloud.global.fujitsu.com",
            "cacheKeyType": "origin",
            "cacheKeyValue": "-",
            "hostHeaderType": "origin",
            "hostHeaderValue": "-"
          }
        },
        {
          "name" : "caching",
          "type" : "honor"
          "value" : "3d"
        }
      ],
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/domestic/*"
        }
      ],
      "behaviors": [
        {
          "name": "geo-whitelist",
          "type": "country",
          "value": "JP"
        }
```

```
        ]
      }
   ]
}
```

Stopping Content Delivery

- Example operation procedure
  1. If you are using your own domain, return the CNAME destination from the delivery URL to a URL such as an on-premises URL.
  2. Use the "Delete Delivery Settings" function to delete the delivery settings.

7.3 Reporting

7.3.1 Report Functions

You can create and acquire reports that include statistical information such as the return status for status codes from an edge server to the end user, and the volume of data transferred. Such reports can be useful for looking up cache hit rates in order to reconsider cache TTL, for example.

Create Report Function

You can create statistical information from the total amount for each of the delivery settings that have been created within the range of a project. To create a report, specify the following items.

Table 132: Creating a Report (List of Items That Can Be Set)

Item	Description	Required
Granularity	Specify the granularity of the information from one of the following: • daily: A report is created every day. • hourly: A report is created every hour (from hh:00 to hh:59).	Yes
Starting Date	Specify the starting date (UTC). You can specify a maximum period of up to 60 days in the past.	Yes
Ending Date	Specify the ending date (UTC). If omitted, the current date is set. Note • You cannot specify a date before the starting date. • If granularity is set to "daily," you must set a date within 31 days from the starting date. • If granularity is set to "hourly," you must set a date within 14 days from the starting date.	
Protocol	Specify a protocol scheme for which data is gathered, from one of the following: • http: HTTP accesses only • ssl: HTTPS accesses onlyHTTP • all: Combined total (default)	
List of Metrics to Be Acquired	Specify the names of the metrics that you want to output from *Table 133: List of Metrics That Can Be Acquired with a Report* on page 167, separated by commas.	Yes

Table 133: List of Metrics That Can Be Acquired with a Report

Name	Description
IncompleteDownloadCount	Number of incomplete downloads
200Count	Number of Status Code 200 responses

Name	Description
206Count	Number of Status Code 206 responses
2XXCount	Combined total number of Status Code 2XX responses and incomplete downloads
302Count	Number of Status Code 302 responses
304Count	Number of Status Code 304 responses
3XXCount	Combined total number of Status Code 3XX responses
404Count	Number of Status Code 404 responses
4XXCount	Combined total number of Status Code 4XX responses
5XXCount	Combined total number of Status Code 5XX responses
RequestCount	Combined total number of requests from the end user to the edge server
TotalBytes	Volume of data transferred from the edge server to the end user [MB]
IngressBytes	Volume of data transferred from the origin server to the edge server [B]
IngressCount	Number of requests from the edge server to the origin server
IngressRequestBytes	Volume of data transferred from the edge server to the origin server [B]
OffloadHitRatio	Ratio of offload from the edge server to the origin server. Cache hit ratio.

A few minutes are required to create a report. Therefore, when the command to create a report is issued, the report ID can be acquired first. You can specify a report ID and then use the "Acquire Report" function to view a report that has been created.

Note

A report ID is valid for 1 hour after the report is created. Then, it is automatically deleted.

Reports are created based on the latest information aggregated on the edge server. Normally, the acquisition of this information starts in about 4 hours. Normally it takes about 1 or 2 days to aggregate the information on all edge servers.

Tip

For example, if on January 1 at 12pm a command is implemented to create a report until 11am, it is possible that the report that is acquired in a few minutes will be based on provisional information that was aggregated from the starting time until about 8am on January 1. To acquire all of the data, issue a command to create a report again at around 12pm two days later on January 3.

Acquire Report Function

Specify a report ID that was created with the Create Report function to acquire a report in json format. The json data in the report will have the following format.

```
{
    "headers": [
        {Definition of headers (index: 0 is fixed to "Time"(UTC))}
        {Definition of headers (index: 1 and later are according to the list
 of metrics you have specified)}
        ...
    ],
    "rows": [
```

```
        [Data in 1st row based on headers],
        ...
        [Data in nth row based on headers],
    ],
    "metadata": {
        "granularity": "daily" (or other conditions as you have specified),
        ...
    }
}
```

Example of json data in report:

```
{
    "headers": [
        {"index": 0, "name": "Time",},
        {"index": 1, "name": "200Count"},
        {"index": 2, "name": "TotalBytes"}
    ],
    "rows": [
        ["2015/12/01 00:00", "47", "100.0"],
        ["2015/12/02 00:00", "30", "67.4"]
    ],
    "metadata": {
        "time_created": "2015/12/10 00:11",
        "granularity": "daily",
        "start_date": "20151201",
        "end_date": "20151202",
        "delivery_option": "all",
        "metrics": ["200Count", "TotalBytes"],
    }
}
```

Part 8: Template

Topics:

K5 IaaS provides this function to create a template of the K5 resources built by the user.

8.1 Orchestration

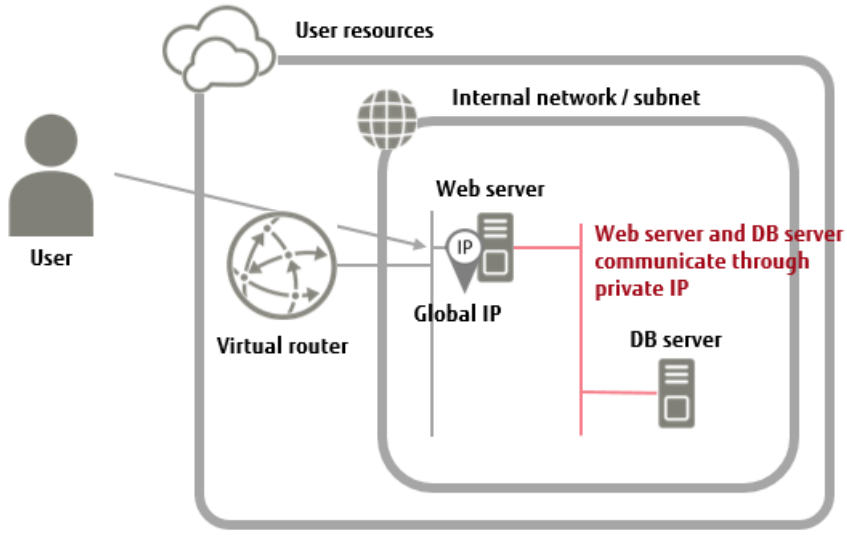
8.1.1 Orchestration Function

This function configures an environment automatically by using multiple virtual resources provided by the system.

As a basic example, this section explains the configuration of a Web system that uses a back-end DB server.

The orchestration function handles system groups like the one described below as one "stack."

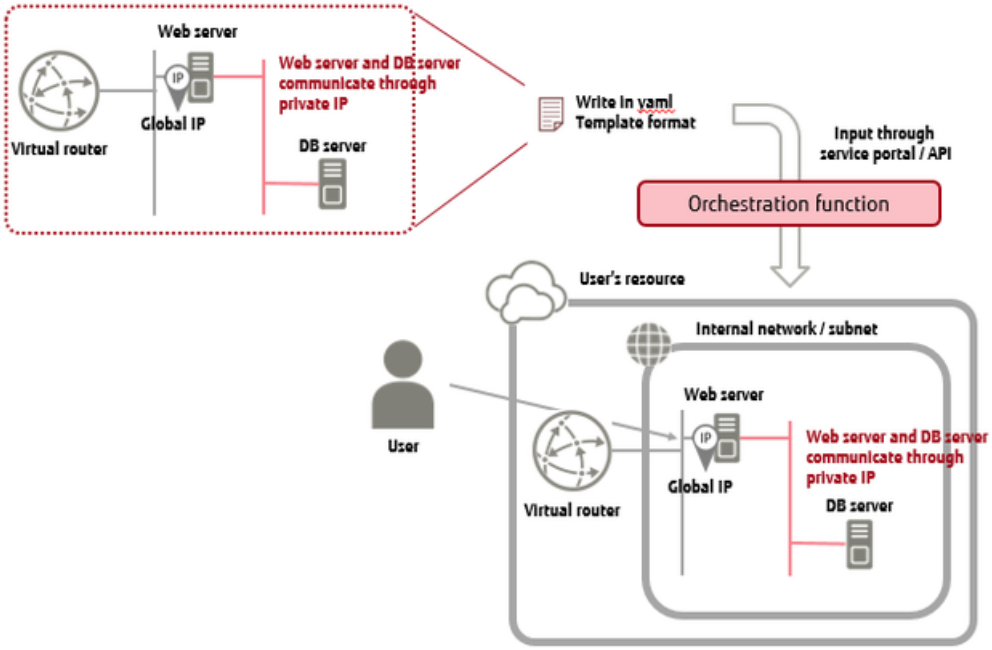
Figure 36: Example of an Automatically Configured System



The text that defines a stack is referred to as a "template."

If you submit a template file to the orchestration function via Service Portal or an API, the environment will be configured automatically.

Figure 37: Diagram of Use of the Orchestration Function



8.1.2 Building a Stack

Create the entire collection of resources defined in the template (YAML format) all at once. Manage the created set of resources as a stack.

Note To build a stack, the "System Owner role (cpf_systemowner)" of the project where you want to build the stack must be assigned in advance to the user of this function.

In addition to the parameter settings for the resources to be created, you can include the following information in the template file.

- A structure that includes resource dependency

  Example: Create block storage first, attach it to a virtual server, and then start the virtual server.
- A structure that uses multiple templates by calling one template from another

Note If the user applies a template that includes the parameters section, the user needs to configure the values when building the stack.

To build a stack, specify the following items:

Table 134: List of Items That Can Be Set for a Stack

Item	Description	Required
Stack Name	Specify a name to identify the stack to be created. Important The name must begin with an alphabetic character.	Yes
Project ID	Specify the ID of the project where you want to build the stack.	Yes

Item	Description	Required
Template URL	Specify the URL where the template can be acquired. Note: Specify either "Template URL" or "Template."	
Template	Specify a template character string. Note: Specify either "Template URL" or "Template." Important: If you specify both "Template URL" and "Template," this item will be given priority.	
environment	This item changes the resource type defined in the template to a different resource type. Use the JSON format to specify this item.	
files	Specify in the JSON format the mapping between file names and the content of the files. Note: Add this information when using the get_file section in the template.	
param_name-n	Specify in the "n" part the name of the input parameter to be passed to the template. Note: Add this information when using the get_param section in the template.	
param_value-n	Specify in the "n" part the value of the input parameter to be passed to the template. Note: Add this information when using the get_param section in the template.	
Creation Timeout	Specify the time, in minutes, to wait for the stack building process before timeout occurs. The default setting is 60 minutes.	
Rollback Settings	Configure these settings so that rollback is not carried out when the stack building process fails. • "true" (default): the created resources are not deleted • "false": the created resources included in the stack are deleted	

Creating a Template

Refer to *Example of Setting Auto-Scaling* on page 32.

Limiting Values

Table 135: List of Limiting Values Related to Orchestration

Item	Limiting Values
Number of Stacks that Can Be Created	1,000 per project

Item	Limiting Values
Stack Name	• Length: 1 - 255 characters • Available character type: Alphanumeric characters, underscores (_), hyphens (-), and periods (.)
Number of Resources that Can Be Included in a Stack	1,000 per stack
Number of Events that Can Be Created	1,000 per stack Note: If this limiting value is exceeded, the oldest events are deleted.
Size of Template File that Can Be Specified when a Stack Is Created	512 KB or less

8.1.3 Modifying/Deleting a Stack

Modify or delete a created stack.

Note: To modify or delete a stack, the "System Owner role (cpf_systemowner)" of the project where the stack to be modified/deleted exists must be assigned in advance to the user of this function.

Modifying a Stack

To modify the content of a stack, apply a new template file to the existing stack.

Note: If the user applies a template file that includes the parameters section, the user needs to configure the values when changing the stack, as is the case with the creation of a new stack.

Deleting a Stack

Delete an existing stack.

Part 9: Monitoring Service

Topics:

K5 IaaS provides a monitoring function for the K5 resources built by the user and for the applications executed by the user on the K5 resources.

9.1 Overview of Functions

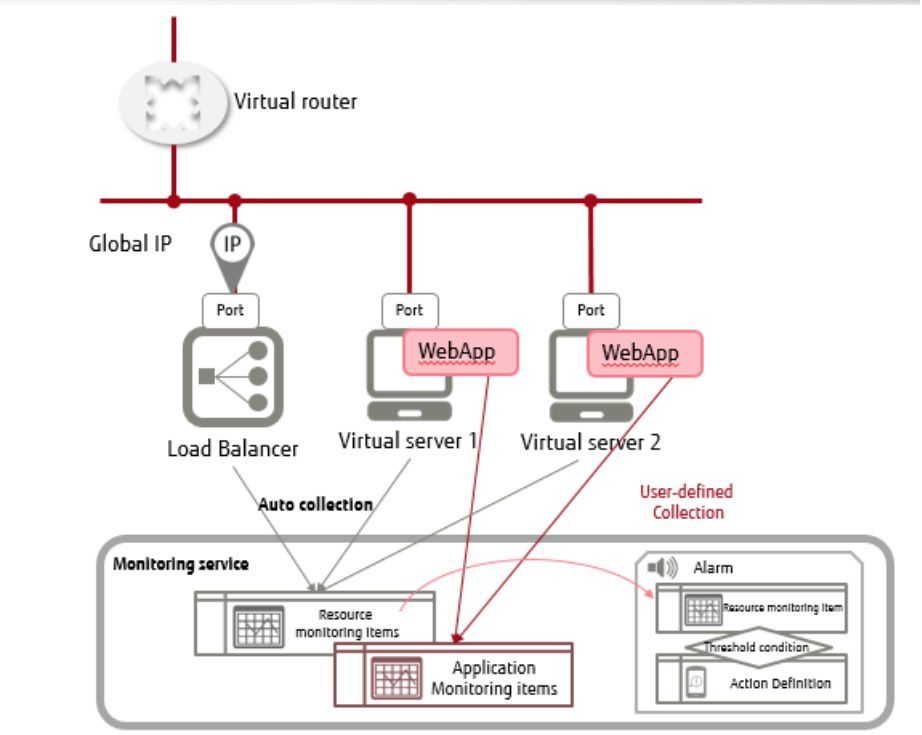
9.1.1 Monitoring Service

This service provides a function to monitor the applications that users run on the system.

- This function collects and tracks information on the monitored items of resources as well as applications run by the user. Rapid solutions based on the results of monitoring allow smooth operation of your application and business.
- This function monitors resources such as virtual servers and DBaaS DB instances. You can also create and monitor unique items for your applications and services.
- You can acquire monitoring data by using an API, or send notifications to programs via alarms. You can then perform troubleshooting based on the status of the cloud environment, visualize the trends, and run automated actions.

Overall Layout of the Monitoring Service

Figure 38: Overview of the Monitoring Service



List of Functions Included

Function	Overview
Monitoring of resources	This function automatically monitors resources. There is no need to install additional software.
Unique item monitoring	Unique items that are created by the user's application are sent and monitored by the monitoring service.
Settings for alarms	Set alarms for monitored items. When the specified threshold is exceeded for a monitored item, automated actions such as sending email and auto-scaling are performed.

Function	Overview
Dashboard	The dashboard displays graphs and statistics for all monitored items from the management console. You can also view all alarms and their history.
API	All operations and the acquisition of monitored items are performed by using an API (compatible with Ceilometer from OpenStack).

9.2 Monitoring of Resources

9.2.1 Monitoring Resources

The resources running on the system are monitored automatically. Monitoring data is acquired for the monitored items that are defined for each resource.

Note

Monitoring is available only within the same region.

Acquiring Monitoring Data

You can view the monitoring data in a graph as statistical values on Service Portal, or you can acquire the data by using an API. You can specify the following parameters when acquiring this data:

- Information that identifies the item to be monitored

  Meter name, resource ID, resource metadata
- Statistic type

  Average, minimum, maximum, total, number of samples
- Period for statistics calculation

  1 minute (minimum) to 2 weeks (maximum)
- Acquisition period

  Desired period within the previous two weeks

Important

Monitoring data is saved for two weeks. To save data that is older than two weeks, you must acquire the data by using an API before it is deleted and then save it in another location.

9.2.2 Monitoring with a Custom Meter

Users can create custom meters for each application, to register and monitor data.

Creating a Custom Meter

If there is no custom meter when you register data, a new custom meter is created.

Acquiring a Custom Meter

You can view the monitoring data from the created custom meter in a graph as statistical values on Service Portal, or you can acquire the data by using an API. You can specify the following parameters when acquiring this data.

- Information that identifies the custom meter

  Meter name, resource ID, resource metadata
- Statistic type

  Average, minimum, maximum, total, number of samples
- Period for statistics calculation

  1 minute (minimum) to 2 weeks (maximum)
- Acquisition period

  Desired period within the previous two weeks

- Units
  Units specified when the custom meter was created

9.3 Alarms

9.3.1 Settings for Alarms

When the specified threshold is exceeded for a monitored resource item or some other monitored item, automated actions such as sending email and auto-scaling are performed.

The item that is monitored, the threshold condition, and the action that is taken when the threshold has been exceeded are handled collectively as an object, which is called an alarm.

Creating an Alarm

Specify the items below to create an alarm:

- Information for monitored items

  Meter name, resource ID, resource metadata
- Threshold conditions
  - Threshold condition

    Greater than or equal, less than or equal, less than, greater than
  - Consecutive number of times for threshold condition

    Consecutive number of times the threshold condition must be reached
  - Statistic type

    Average, minimum, maximum, total
  - Period for statistics calculation (alarm check interval)

    1 minute (minimum) to 2 weeks (maximum)
- Action settings

  You can define actions for each alarm status shown below.

  Actions are performed only when the status changes.

  Note

Table 136: List of Alarm Statuses

Status	Description
OK	No abnormality (alarm thresholds have not been exceeded)
ALARM	Alarm threshold condition has been reached
INSUFFICIENT_DATA	Data insufficient to check for alarm Examples: Alarm disabled, monitored item instance stopped

Viewing Alarm History

Table 137: List of Alarm History Items

Item	Description
Date	This is the date and time for each history entry.

Item		Description
Type	Changed Settings	This is the information regarding operation events for an alarm. • Created: Information specified when an alarm was created • Deleted: Information for deleted alarms • Changed settings: Information on alarms before and after changes
	Change in Status	This is the information regarding status changes. The following information is included: • Statuses before and after changes (Example: OK -> NG) • Reason for change (Example: Threshold exceeded) • Measurements before and after changes • Threshold conditions for monitored items that are set for alarm
	Actions	This is the information regarding actions that were performed. The following information is included: • Action results • Notification destination (for email) • Message (for email) • Date and time of change in status that triggered alarm
Description		This is a description of each history entry.

Note

History information is retained for a maximum of two weeks. To save data that is older than two weeks, you must acquire the data by using an API before it is deleted and then save it in another location.

Part 10: Security

Topics:

- *IPS/IDS*

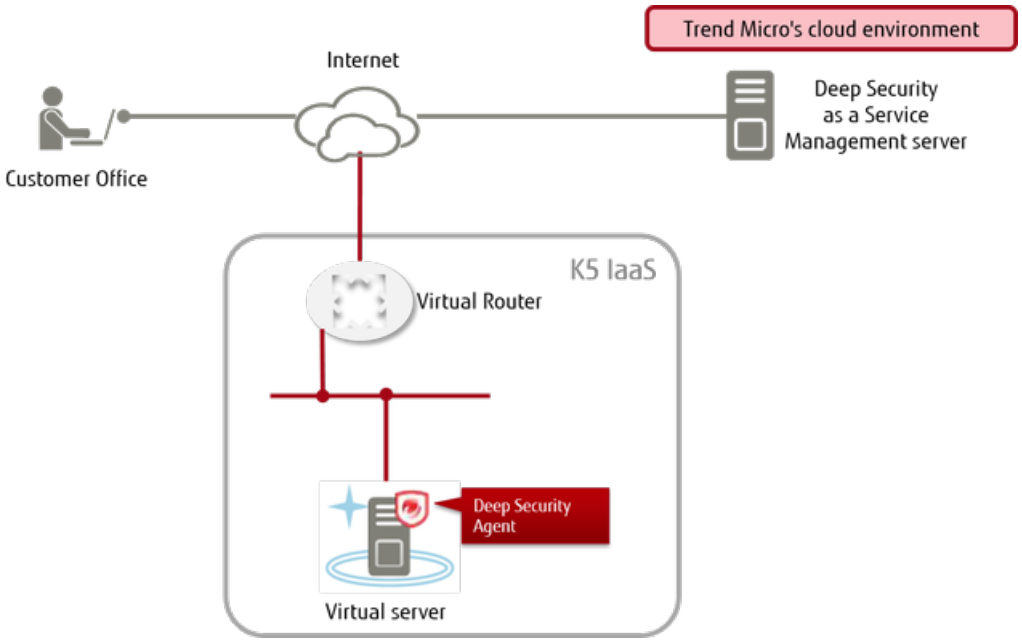
K5 IaaS provides security solutions for virtual servers.

10.1 IPS/IDS

10.1.1 Trend Micro Deep Security as a Service Option

We have provided Deep Security as a Service option, which allows you to carry out centralized management of your created virtual server by using the management server provided in the cloud by Trend Micro.

Figure 39: Overall Layout of Trend Micro Deep Security as a Service Option



Functions Included

By installing the Deep Security agent software on the virtual server you have created, you can use a multi-layered defense that utilizes the security functions described below.

Table 138: Available Security Functions

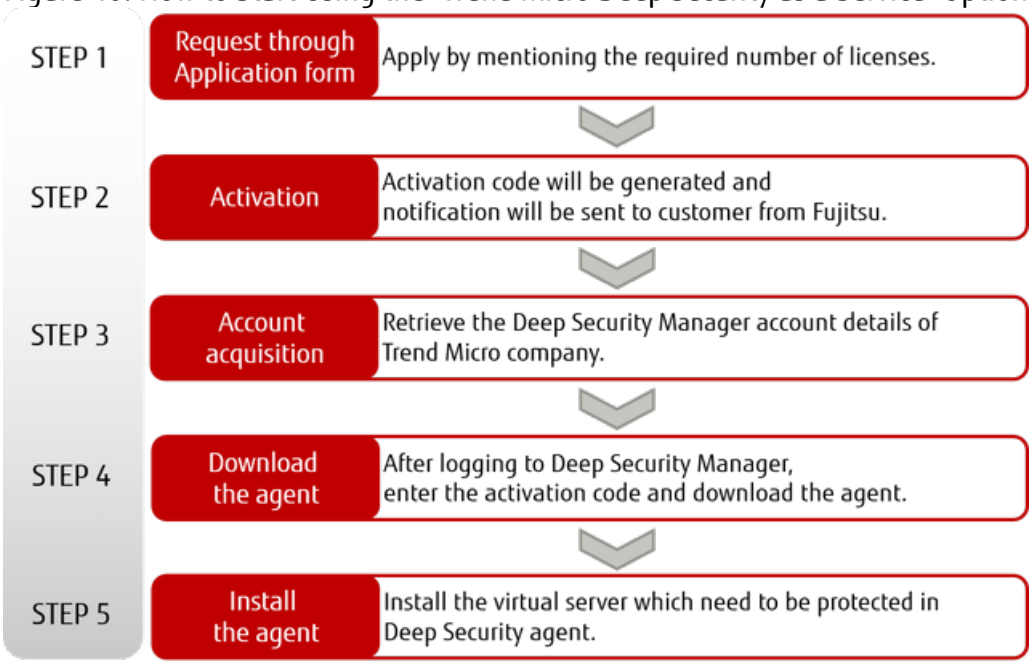
Security Functions	Description
IDS/IPS	Protects the server from attacks that target the vulnerability of the OS or applications
Firewall	Decreases the chances of an attack by blocking unauthorized communication at the end point
Virus Protection	Scans the system for viruses in real time and protects the server from malware and other attacks
Web Reputation	Protects web applications from SQL injections and other attacks
Integrity Monitoring	Ensures early detection of file or registry tampering
Log Monitoring	Ensures early detection of important security events in the OS or middleware

License Cancellation

In order to cancel a license, you must submit an application for cancellation of the Trend Micro Deep Security as a Service option. For more information, refer to the K5 IaaS service official website.

How to Use This Service

Figure 40: How to Start Using the "Trend Micro Deep Security as a Service" Option



Points to Note

- You must obtain a license for each virtual server.
- Note that you will still be charged per license for this optional service even if you delete the virtual server where the agent is installed.

Part 11: Management

Topics:

K5 IaaS provides a function to manage the privileges for using the K5 resources.

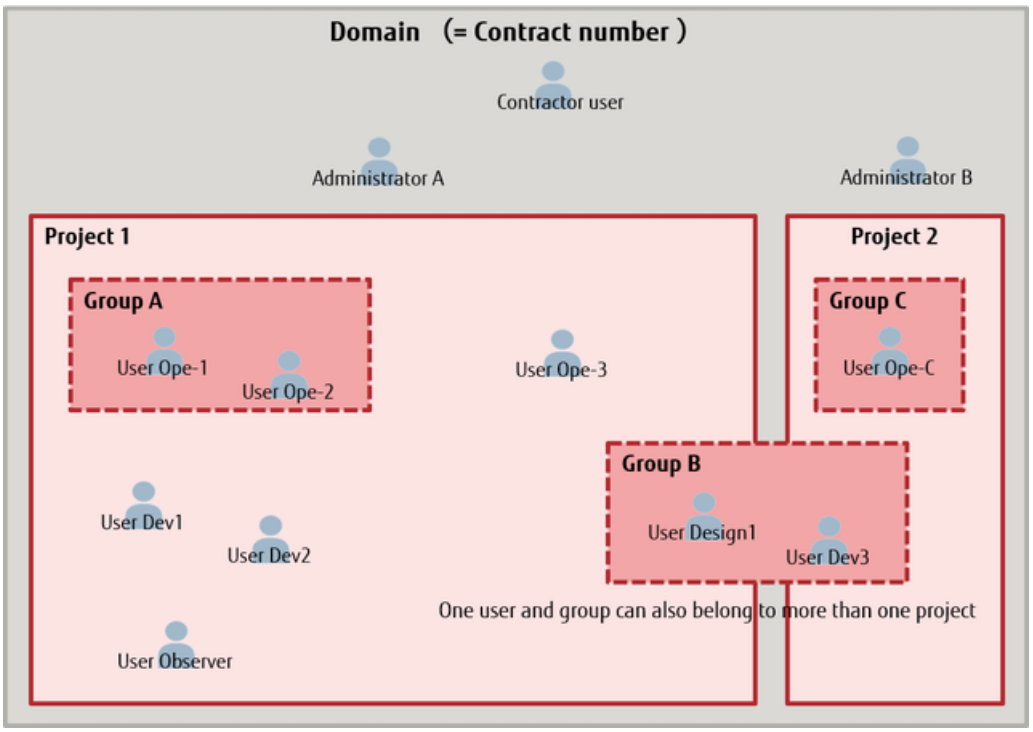
11.1 Overview of Functions

11.1.1 Information to Know in Advance

This section explains the concepts provided by the user management functions.

With K5 IaaS, the contractor user creates other users, and each user uses their created user name to log in to the system in order to access the services. The **users** shown in the following figure must be created in order to create and use virtual resources:

Figure 41: Relationship Concepts Provided by the User Management Functions



Domain

The area available to an organization that has subscribed to this service is shown in units of service contracts. When the organization successfully enters into a license agreement, the system grants a contract number, which is then set as the domain name.

User

A **person** who logs in to the system to use the service functions and to manage resources.

Project

An organization to which the user belongs. More than one project can be created within a domain. Most virtual resources are created under projects, so, for example, you can create and use a different project for each department at your company to implement different styles of system management appropriate to each department.

Group

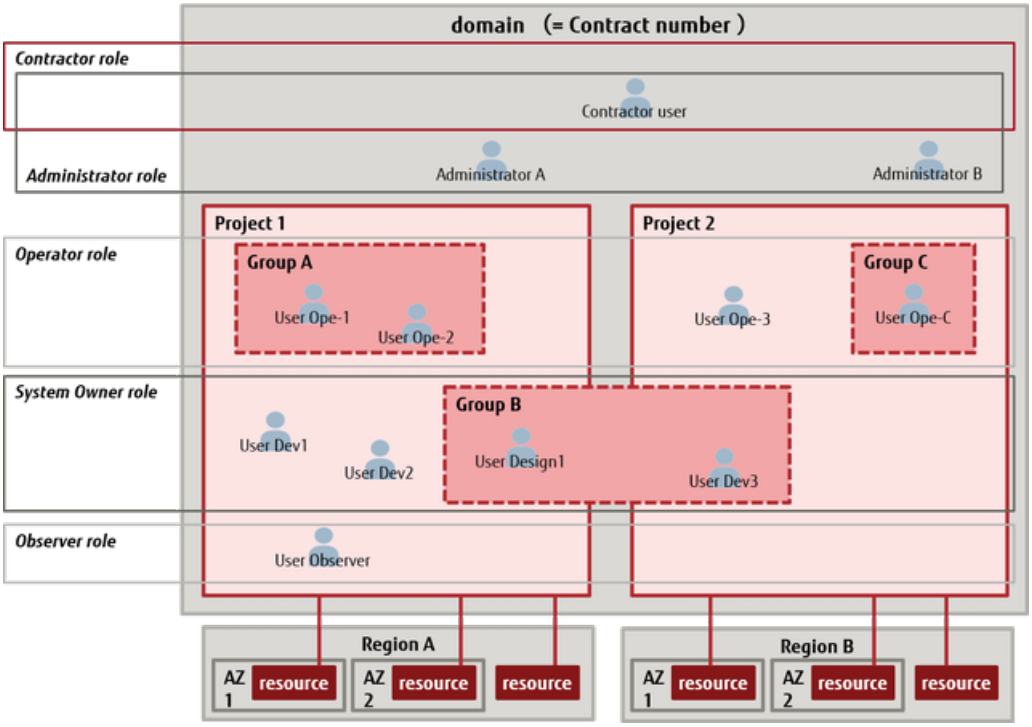
A collection to which multiple users can belong. For example, you can use this to manage user rights collectively.

Role

The information that is used to assign privileges to users or groups. The following six roles are defined by default. You can assign them according to the role of each user:

- Contractor role
- Administrator role
- System Owner role
- Operator role
- Observer role
- Member role

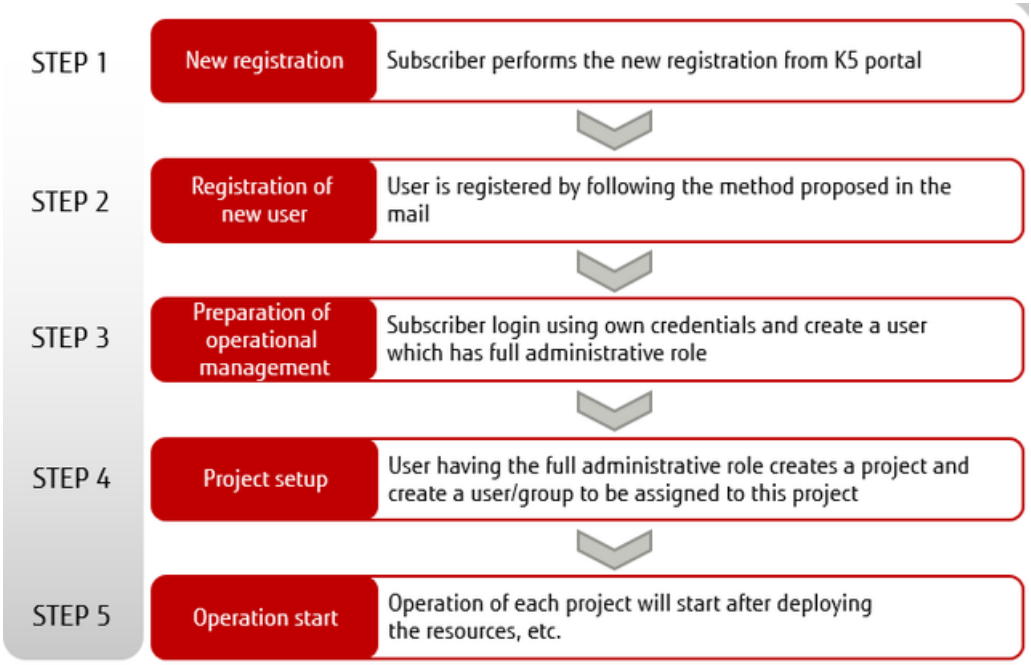
Figure 42: Domain, Group, and User Relationships



11.1.2 Procedure for Starting Operation

To create a domain and projects and start using virtual resources, the contractor user must create the first user. When a new user is created, a single contract number (domain) is assigned.

Figure 43: Procedure from Signup to Start of Operation



For details on new registration and the user management functions, refer to *K5 Portal User Guide*.

11.2 Subscription Management

11.2.1 Region Management

This function allows you to add and use regions in addition to the regions available at the time of the subscription, and to obtain information about regions currently used.

Note

A region can only be managed by the following user:

- A user that has the Contractor role

Functions Included

- Default Region

  This region is made available by default when a contract number (domain) is obtained at K5 Portal.

  Tip

  "Eastern Japan Region 1 (jp-east-1)" is set up as the default region.

- Region Activation Function

  This function allows you to activate and start to use a region that has not been used yet so that you can deploy resources in the region.

  Note

  The region to which this function is applied is not immediately available. Check the state of the region by using the information acquiring function of regions currently in use, and confirm that the region is in an "active" state before you start to use the region.

  Important

  If a region has already been activated with this function, do not use the function again to activate the same region.

- Region List Function

  This function displays a list of regions provided as K5 IaaS services.

- Function for Acquiring Information about Regions Currently in Use

  This function displays a list of regions that have been activated with the region activation function and the availability of each region. There are two states:

  - active
  - ready

  You can also obtain information about the default region.

11.3 User Management

11.3.1 Overview of Functions

11.3.1.1 Global User Management

The global user management functions allow you to manage global resources such as users and groups.

Global Resources in User Management Services

Among the resources managed with the user management services, global resources refer to the following resources that are consistent across all regions:

- Global token
- Contract number (domain)
- User
- Group
- Preset roles

11.3.1.2 Regional User Management

The regional user management functions allow you to manage regional resources such as projects and role assignments.

Regional Resources in User Management Services

Among the resources managed with the user management services, regional resources refer to the following resources that are independent from region to region:

- Regional token
- Project
- Role assignment

11.3.1.3 Preset Roles and Privileges

The combinations of privileges related to the system operations within a domain are defined as preset roles. Preset roles are assigned to groups and users to control the operations involving virtual resources.

Contractor Role (cpf_org_manager)

This role is for the user created at the time of the subscription to the service, and is used to manage the entire contract. The contractor user can cancel the service contract.

Administrator Role (cpf_admin)

This role can be created by an administrator. A user with this role is an administrator within the domain, and can handle all the projects within the domain.

Tip The Contractor role and the Administrator role are assigned to the user created at the time of subscription to the service.

System Owner Role (cpf_systemowner)

This role can be created by the contractor or an administrator. A user with this role can carry out the operations related to the resources within a project, such as adding and deleting resources, or starting virtual servers.

Operator Role (cpf_operator)

This role can be created by the contractor or an administrator. A user with this role can carry out the same operations within a project as a user with the System Owner role, except for adding and deleting resources.

Observer Role (cpf_observer)

This role can be created by the contractor or an administrator. A user with this role can monitor the resources within a project.

Member Role (_member_)

This role is assigned to all users. This role has general user privileges that allow you to carry out the operations related to your account, such as changing passwords.

Contractor Role (cpf_org_manager_provisional)

This role is for a user newly registered from K5 Portal (until activated).

Note

This role cannot be assigned by the customer.

Contractor Role (cpf_org_manager_cancelled)

This role is for the user during a cancellation process of the K5 service.

Note

This role cannot be assigned by the customer.

Trial Role (cpf_trial)

This role is for trial users.

Note

This role cannot be assigned by the customer.

11.3.2 Global User Management

11.3.2.1 Group Management

11.3.2.1.1 Group Management

You can create and delete groups, and manage the users that you assign to a group. You can also collectively manage the users that belong to a group, such as configuring their participation in projects and roles.

Note

To enable group management, the following conditions must be met:

- A user has the Administrator role.
- The authentication process is performed using global user management, and global tokens are acquired.

- For group management operations, global user management is used with global tokens.

Creating a Group

You can create a group in a domain. Items that you can specify are as follows.

Note
Although you can create multiple groups in a domain, you cannot assign a group to another group.

Table 139: List of Items That Can Be Set for Groups

Item	Description	Required
Group Name	Specify the name that identifies the group Important The group name must be unique within the domain.	Yes
Group Description	Specify a description of the group to be created	
Domain ID	Specify the ID of the domain where you wish to create the group Tip Specify the domain to which you belong.	Yes

Changing Group Information

Change the settings of an existing group. The items that you can change are as follows:

Table 140: List of Items That Can Be Set for Groups

Item	Description	Required
Group Name	Specify the name that identifies the group Important The group name must be unique within the domain.	Yes
Group Description	Specify a description of the group to be created	
Domain ID	Specify the ID of the domain where you wish to create the group Tip Specify the domain to which you belong.	Yes

Adding/Deleting Users in a Group

You can specify users to add to a group or to delete (exclude) from a group.

Deleting a Group

Delete an existing group.

Even if you delete a group, the users that belong to that group are not deleted.

Limiting Values

Table 141: List of Limiting Values Related to Domains, Projects, Groups, and Users

Item	Limiting Values
Number of Projects	1,000 per domain
Project Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), period (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No
Number of Groups	100 per project
Group Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), period (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No • Uniqueness constraint: Uniqueness is required within a domain
Number of Users	• 100 per group • 100,000 per domain
User Name	• Length: 4 - 255 characters • Available character type: Alphanumeric characters and the following symbols: Period (.), at mark (@), hyphen (-), underscore (_)

User Password	• Length: 16 - 64 characters
	• Available character type: Alphanumeric characters and the following symbols:
	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
	• Complexity constraint
	  • Must not contain the user name
	  • Must include at least 1 alphabetic character
	  • Must include at least 1 numeric character
	• Case sensitivity: Yes

Email Address	• Length: 5 - 64 characters • Available character type: Alphanumeric characters and the following symbols:

Item	Limiting Values
	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

11.3.3 Regional User Management

11.3.3.1 Project Management

11.3.3.1.1 Project Management

This function allows you to divide the virtual resources in the contract into projects to manage them. Use this function when you want to make a clear distinction between the virtual systems used by the organizations or departments inside a company.

To enable a specific user or group to use the virtual resources in a project, you can control the user or group by having them belong to the project.

A user that does not have the Administrator role can only handle the resources within the project to which the user belongs. By combining roles and projects, you can block users from operating the virtual systems of other projects.

Note

To enable project management, the following conditions must be met:

- A user has the Administrator role.
- For the region in which the project to be managed belongs, the authentication process is performed using regional user management, and regional tokens are acquired.
- For project management operations, regional user management is used with regional tokens.

Default project

When a user is created from K5 Portal, the default project of the Contractor user is set for the created user. Information for the default project is synchronized in all the regions that are currently in use and can be used in each region.

Note

- The default project set for a user cannot be changed.
- Although the information of the default project is synchronized among regions, the virtual resources that belong to the region must be handled using the regional service for each region.

Creating a Project

Create projects within a domain. Items that you can specify are as follows.

Table 142: List of Items That Can Be Set for Projects

Item	Description	Required
Project Name	Specify the name of the project Note The project name must be unique within a region.	Yes

Item	Description	Required
Project Description	Specify a description of the project	

Modifying a Project

Change the existing settings of a project. The items that you can change are as follows.

Table 143: List of Items That Can Be Changed for Projects

Item	Description	Required
Project Name	Specify the name of the project Note The project name must be unique within a region.	Yes
Project Description	Specify a description of the project	

Disabling a Project

Disable existing projects that are not needed.

Important If you simply disable a project, the virtual resources belonging to that project are not returned automatically. If you no longer require the resources, return them.

Limiting Values

Table 144: List of Limiting Values Related to Domains, Projects, Groups, and Users

Item	Limiting Values
Number of Projects	1,000 per domain
Project Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), period (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No
Number of Groups	100 per project
Group Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), period (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No • Uniqueness constraint: Uniqueness is required within a domain
Number of Users	• 100 per group

Item	Limiting Values
	• 100,000 per domain
User Name	• Length: 4 - 255 characters • Available character type: Alphanumeric characters and the following symbols: Period (.), at mark (@), hyphen (-), underscore (_)

User Password	• Length: 16 - 64 characters
	• Available character type: Alphanumeric characters and the following symbols:
	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
	• Complexity constraint
	  • Must not contain the user name
	  • Must include at least 1 alphabetic character
	  • Must include at least 1 numeric character
	• Case sensitivity: Yes

Email Address	• Length: 5 - 64 characters • Available character type: Alphanumeric characters and the following symbols: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

11.3.3.2 Role Management

11.3.3.2.1 Assigning a Role

Assign roles registered in the system to each user in order to grant operation privileges accordingly.

You can use the standard roles (*Preset Roles and Privileges* on page 190).

To include a user or a group in a project, select a role and assign it to the user or group.

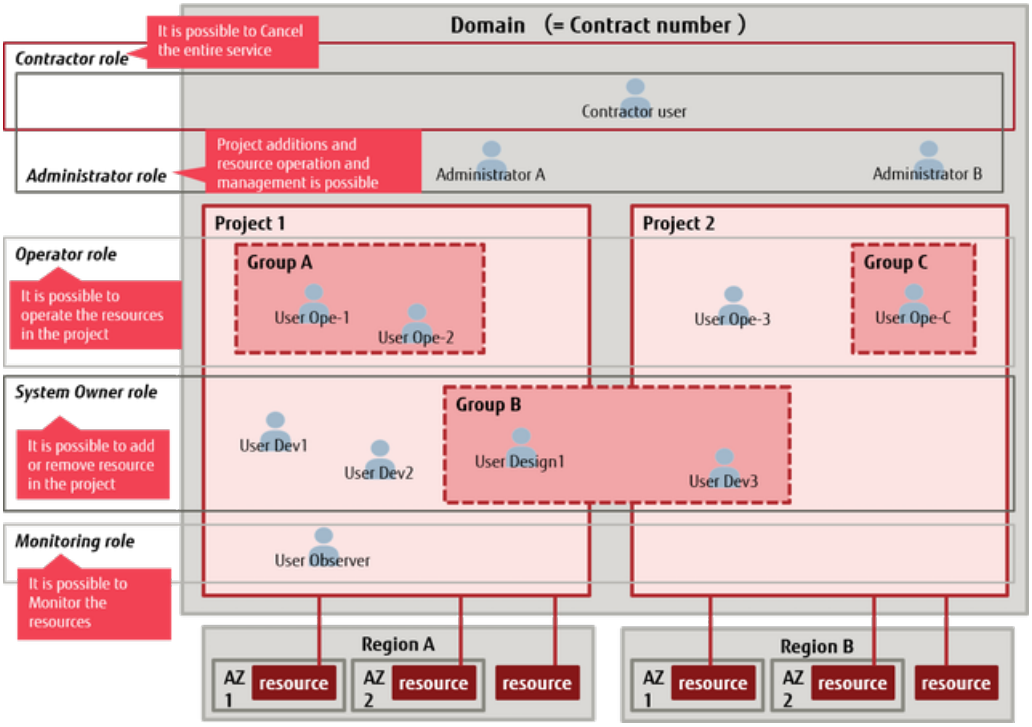
Note

To enable role assignment management, the following conditions must be met:

- A user has the Administrator role.
- For the regions in which the project to be managed belongs, the authentication process is performed using regional user management, and regional tokens are acquired.

- For project management operations, regional user management is used with regional tokens.

Figure 44: Role Assignment Example



11.4 Key Management

11.4.1 Key Management Function

This function allows you to centrally manage the key information that is required for SSL communication. Users can use key information that they have created and registered as well as key information that is registered by services such as the load distribution service.

Managing Key Information

Register and manage key information that was created in PEM format by a user.

Table 145: Registering Key Information (List of Items That Can Be Set)

Item	Description	Required
Key Information Name	Specify the name of the key information	
Encryption Algorithm	Specify the encryption algorithm for the key information to be registered	
Mode	Specify the mode of the algorithm associated with confidential information	
Key Length	Specify a key length that is a multiple of 8 to be used for encryption	
Retention Period	When the specified retention period is exceeded, the registered key information will be deleted automatically. If this setting is omitted, no limit is set on use of the key information Tip: Specify a future date and time in the following format: "YYYY-MM-DDThh:mm:ss.SSSSSS"	
Confidential Information	Specify confidential information to be registered Important: This information must be enclosed between "-----BEGIN XXXX-----" and "-----END XXXX-----." Note: No check is performed to determine if the specified confidential information is in PEM format. Be sure to check in advance if the format is correct.	
Content Type for Confidential Information	Specify the content type to be used when viewing confidential information • text/plain • application/octetstream	Required when confidential information is specified
Encoding Format for Confidential Information	Specify an encoding format (base64) Note: If you specified "text/plain" as the content type for confidential information, you cannot configure this setting.	

PEM format refers to the following type of text data:

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA
+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCBtTELMAkGA1UEBh
MCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL........
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV
+DiuTxcfA4uhwMDSe0nynbn1qiwRk450mCOnq
H4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5YR7CKx7fc5xRaeQdyGj/
dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

Managing Certificate Information

Manage the following key information required for SSL communication as a single set of certificate information:

- SSL Certificate
- CA Certificate (including information for intermediate certification authorities)
- Private Key
- DH (Diffie Hellman) Key

Part 12: Private Connection

Topics:

This service provides the functions and ports for a closed connection between the K5 environment and an environment such as a hosting environment to which the user subscribes or an on-premises environment.

12.1 Overview of Functions

12.1.1 Private Connection Function

This function and ports are provided to allow a closed connection between the K5 environment and an environment such as the hosting environment to which the contractor user subscribes or an on-premises environment.

Provided Service Menu

- K5 environment connection
- Data center outsourcing environment connection
- On-premises (FENICS) connection


Tip For further details about this service, refer to the "FUJITSU Cloud Service K5 - Private Connection Service Descriptions."

12.1.2 Direct Port Connection Function

This function provides physical ports to allow a direct connection to the K5 environment via L3, not via the Internet or a closed connection network.

Provided Service Menu

- Direct port connection


Tip For further details about this service, refer to the "FUJITSU Cloud Service K5 - Private Connection Service Descriptions."

Appendix

A.1 Limiting Values

This section shows the limiting values for the resources available in each service.

Limiting Values Related to Compute

- Standard Services

  Table 146: List of Limiting Values Related to Virtual Servers

Item	Limiting Values
Number of Virtual Servers	Up to 20 per project per availability zone
Number of Virtual CPUs (vCPUs)	80 per project per availability zone
Memory Capacity (total for a project)	327,680 MB per project per availability zone
Number of Metadata Items that Can Be Specified for a Virtual Server	128 per virtual server
Number of Key Pairs	100 per project per availability zone

  Table 147: List of Limiting Values Related to Virtual Server Import Service

Item	Limiting Values
Possible Number of Virtual Server Import Requests	100 per domain
Maximum Execution Period of Virtual Server Import Processing	7 days
Number of Virtual Server Import Processing Results Retained	1,000 Note: If this limiting value is exceeded, the oldest processing results are deleted.
File Size of a Single Virtual Server Image	300 GB Tip: This is the total size of separately uploaded files.

- Services for SAP

  Table 148: List of Limiting Values Related to Virtual Server for SAP and Dedicated Virtual Server for SAP

Item	Limiting Values
System Storage	The size is fixed according to the OS image
Additional Storage	0.1 - 2,048 GB

Item	Limiting Values
Number of Storage Systems that Can Be Added	1 - 55
Number of Snapshots Taken	10
Number of Ports that Can Be Added	1 - 9

Limiting Values Related to Storage

Table 149: List of Limiting Values Related to Block Storage

Item	Limiting Values
Size of Additional Storage	1 GB or more (specified in GB)
Number of Storage Systems	50 per project per availability zone Note: The total number of additional storage systems and additional ports must be within 26 for a single virtual server.
Storage Capacity (total for a project)	5,000 GB per project per availability zone
Number of Snapshots Taken	100 per project per availability zone

Table 150: List of Limiting Values Related to Object Storage

Item	Limiting Values
Number of Objects per User	Unlimited
Number of Objects per Container	Unlimited
Length of Object Name	1,024 bytes or less
Size of Object that Can Be Uploaded	0 - 5 GB
Length of Object Metadata Name	128 bytes or less
Length of Object Metadata	2,048 bytes or less
Number of Containers per User	Unlimited
Length of Container Name	256 bytes or less
Uniqueness of Container Name	Unique name in a project
Length of Container Metadata Name	128 bytes or less
Length of Container Metadata	2,048 bytes or less

Limiting Values Related to Networking

Table 151: List of Limiting Values Related to Networking

Item	Limiting Values
Number of Networks	10 per project per availability zone
Number of Subnets	10 per project per availability zone

Item	Limiting Values
Number of Host Routes that Can Be Set for the Subnet	20 per project
Number of Ports	50 per project per availability zone Note: The total number of additional storage systems and additional ports must be within 26 for a single virtual server.
Number of Allowed Address Pairs that Can Be Set for Ports	10 per project per availability zone
Number of Global IP Addresses	50 per project per availability zone
Number of Security Groups	10 per project
Number of Rules that Can Be Specified for a Security Group	100 per project Note: This is the number of rules that can be specified for the entire security group. Note that this is not the number allowed for a single security group.
Number of Virtual Routers	10 per project per availability zone
Number of Routes that Can Be Set for a Virtual Router	128 per virtual router
Number of Firewalls	10 per project per availability zone
Number of Firewall Policies	1 per firewall
Number of Firewall Rules	500 per firewall policy

Table 152: List of Limiting Values Related to the Load Balancer Service

Item	Limiting Values
Load Balancer Name	• Length: 1 - 30 characters • Available character type: Alphanumeric characters and hyphens (-)
Number of Load Balancers Created	20 per project
Maximum Number of Connections	32,768 per subnet

Table 153: List of Limiting Values Related to DNS Zone Management

Item	Limiting Values
Number of DNS Zones Registered	100 per domain
Time To Live (TTL) for Cache that Can Be Specified	60 - 86,400 seconds

Item	Limiting Values
Maximum Number of Records for Bulk Acquisition of Zone Information	100 records

Table 154: List of Limiting Values Related to DNS Record Management

Item	Limiting Values
Number of Records that Can Be Specified	10,000 per zone
Supported Record Type	A, AAAA, CNAME, MX, NS, TXT
Record Type with Wildcard Support	A, AAAA, MX, CNAME, TXT

Table 155: List of Limiting Values for DNS Record Entries

Record Type	Item	Limitations
A	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Available character type: Alphanumeric characters and dots (.) Must be a valid IPv4 address
	Memo	Length: 255 characters or less Available character type: Double-byte characters
	Weight	0 - 100 Available character type: Numeric characters
	Health Check IP Address	Length: 1 - 32 characters Alphanumeric characters and dots (.)
	Health Check Port Number	Length: 1 - 5 characters Available character type: Numeric characters
	Health Check Host Name	Length: 0 - 255 characters Available character type: Single-byte characters
	Health Check Path	Available character type: Single-byte characters
AAAA	Record Name	Length: 1 - 63 characters Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds

Record Type	Item	Limitations
	Value	Alphanumeric characters and dots (.) Must be a valid IPv6 address
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
	Weight	0 - 100 Available character type: Numeric characters
	Health Check IP Address	Length: 1 - 32 characters Available character type: Alphanumeric characters and dots (.)
	Health Check Port Number	Length: 1 - 5 characters Available character type: Numeric characters
	Health Check Host Name	Length: 1 - 255 characters Available character type: Single-byte characters
	Health Check Path	Available character type: Single-byte characters
CNAME	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
MX	Record Name	Length: 1 - 63 characters Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)
	Priority	Character type: Numeric characters, 0 - 64,000
	Memo	Length: 1 - 255 characters

Record Type	Item	Limitations
		Available character type: Double-byte characters
TXT	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)
	TTL	60 - 86,400 seconds
	Value	Alphanumeric characters, single-byte spaces, and single-byte symbols other than double quotation marks (")
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
NS	Record Name	Character type: Alphanumeric characters, dots (.), and hyphens (-)
	TTL	60 - 86,400 seconds
	Value	Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters
LBR	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), and hyphens (-)
	Memo	Length: 1 - 255 characters Available character type: Double-byte characters

Limiting Values Related to Database as a Service

Table 156: List of Limiting Values Related to Database as a Service

Item	Limiting Values
Number of DB Instances	40 per project
Total Disk Size of All DB Instances	100 TB
Number of DB Snapshots that Can Be Created	50 generations per DB instance
Maximum Capacity of DB	10 TB
Number of DB Subnet Groups	20
Number of DB Subnets	20 per subnet group
Number of DB Parameter Groups	50
Number of Event Notification Registrations	20

Item	Limiting Values
Number of Read Replicas	5

DB Instance Name	• Length: 1 - 255 characters
	• Available character type: Alphanumeric characters and hyphens (-)
	• Other limitations
	  • Use an alphabetic character as the first character
	  • You cannot use a hyphen as the first character
	  • You cannot use two or more consecutive hyphens

Description of DB Instance	• Length: 1 - 1,024 characters
Master User Name	• Length: 1 - 63 characters • Available character type: Alphanumeric characters and underscores (_) • Other limitations • You can only use an alphabetic character or underscore as the first character
Master User Password	• Length: 1 - 1,024 characters

DB Snapshot Name	• Length: 1 - 255 characters
	• Available character type: Alphanumeric characters and hyphens (-)
	• Other limitations
	  • The name must begin with an alphabetic character
	  • You cannot use a hyphen as the first character
	  • You cannot use two or more consecutive hyphens

Read Replica Name	• Length: 1 - 255 characters
	• Available character type: Alphanumeric characters and hyphens (-)
	• Other limitations
	  • The name must begin with an alphabetic character
	  • You cannot use a hyphen as the first character
	  • You cannot use two or more consecutive hyphens

Limiting Values Related to the Email Delivery Service

Table 157: List of Limiting Values Related to the Email Delivery Service

Item	Limiting Values
Maximum Number of Emails Sent per Second	• Using API: 50 (1 request/second x 50 recipients) • Using SMTP interface: 500
Maximum Number of Registered Email Addresses per Domain	1,000
Maximum Number of Requests per Second	• 10 (different requests) • 1 (same request)
Number of Recipients per Request	50
Maximum Size per Email	• Using API: 2 MB • Using SMTP interface: 10 MB Note: This includes email attachments.

Limiting Values Related to the Content Delivery Network Service

Table 158: List of Limiting Values Related to the Content Delivery Network Service

Item	Limiting Values
Time to Be Available for Content Delivery	Within 10 minutes Tip: From API request of Creating Delivery Settings accepted.
Time to Delete Caches	Within 10 minutes Tip: From API request of Deleting Cache accepted.
Maximum Number of Delivery Settings	200 per project
Maximum Number of Caching Behavior Control Rules	100 behaviors per delivery setting
Maximum File Size that Can Be Delivered	1.8 GB per file
Maximum Number of Files that Can Be Located on a Edge Server	No limit
Maximum Size of Caching Behavior Control Rules	• Sending:16 KB Tip: Includes the amount of following factors. • Length of the specified Caching Behavior Control Rules

Item	Limiting Values
	• (Length of delivery FQDN) x (Number of behaviors in the origin setting) • Receiving: No limit
FQDN Information	In case of K5 cdn-edge domain: • Length of Prefix: 0 - 30 characters • Available character type: Alphanumeric characters and hyphens (-) In case of your own domain: • Length of FQDN: 1 - 255 characters • Available character type: Alphanumeric characters, periods (.) and hyphens (-) Note • Capital letters are handled as small letters • You cannot use a hyphen as the first character or the last character • You cannot include "xn--" anywhere
Cache TTL	0 - 9999 days
Maximum Number of API Requests per Second (Rate Limiting)	According to the API method, there is the Rate Limiting. Tip Please retry the API request when you receive '429' status code.
Maximum Number of Concurrent Access	No limit for the edge servers
Access Log Prefix	Length: 1 - 255 characters Tip This includes account name and container name.

Limiting Values Related to the Template Service

Table 159: List of Limiting Values Related to Orchestration

Item	Limiting Values
Number of Stacks that Can Be Created	1,000 per project
Stack Name	• Length: 1 - 255 characters • Available character type: Alphanumeric characters, underscores (_), hyphens (-), and periods (.)
Number of Resources that Can Be Included in a Stack	1,000 per stack
Number of Events that Can Be Created	1,000 per stack

Item	Limiting Values
	Note If this limiting value is exceeded, the oldest events are deleted.
Size of Template File that Can Be Specified when a Stack Is Created	512 KB or less

Limiting Values Related to Management Functions

Table 160: List of Limiting Values Related to Tokens

Item	Limiting Values
Number of Global Tokens	5,000 per domain
Expiration of Global Tokens	3 hours
Number of Regional Tokens	5,000 per domain
Expiration of Regional Tokens	3 hours

Table 161: List of Limiting Values Related to Domains, Projects, Groups, and Users

Item	Limiting Values
Number of Projects	1,000 per domain
Project Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), period (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No
Number of Groups	100 per project
Group Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), period (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No • Uniqueness constraint: Uniqueness is required within a domain
Number of Users	• 100 per group • 100,000 per domain
User Name	• Length: 4 - 255 characters • Available character type: Alphanumeric characters and the following symbols:

Item	Limiting Values
	Period (.), at mark (@), hyphen (-), underscore (_)

User Password	• Length: 16 - 64 characters
	• Available character type: Alphanumeric characters and the following symbols:
	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
	• Complexity constraint
	  • Must not contain the user name
	  • Must include at least 1 alphabetic character
	  • Must include at least 1 numeric character
	• Case sensitivity: Yes

Email Address	• Length: 5 - 64 characters • Available character type: Alphanumeric characters and the following symbols: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Table 162: List of Values Related to Password Policies

Item	Limiting Values
Minimum Character Length	16 characters
Minimum Days	1 day
Effective Days	90 days
Lockout	• Duration: 15 minutes • Number of invalid attempts: 5 • Time from locking to unlocking: 15 minutes
History	The same password string as any of the last 4 passwords is not allowed.

Table 163: List of Limiting Values Related to Key Management Functions

Item	Limiting Values
Key Information Container Name	• Length: 1 - 255 characters • Available character type: Alphanumeric characters and single-byte symbols
Number of Key Information Containers	100
Key Information Records that Can Be Stored in a Key Information Container	10 per key information container
Number of Key Information Records	100
Key Information Name	• Length: 1 - 255 characters

Item	Limiting Values
	• Available character type: Alphanumeric characters and single-byte symbols
Key Length	8 or more

A.2 Points to Note

This section explains points to note regarding K5 IaaS services.

Points to Note regarding the Infrastructure within Availability Zones

If a hardware failure occurs in an availability zone, it may affect your virtual resources as follows:

- Block storage

  I/O delays up to 180 seconds
- Network/subnet/virtual router/network connector

  Communication disconnections up to 335 seconds

A.3 List of Software Support Service IDs

ID Used with the Software Support Service

The list of ID for each type of software and support level is shown below.

Table 164: List of Software Support Service Related ID

Software	Software ID	Support Level	Support ID
Windows Server 2008 SE R2 SP1 64bit English Version	W2k8R2SE	No support	nosupport
Windows Server 2008 EE R2 SP1 64bit English Version	W2k8R2EE	No support	nosupport
Windows Server 2012 SE R2 64bit English Version	W2k12R2SE	No support	nosupport
Windows Server 2012 SE 64bit English Version	W2k12SE	No support	nosupport
Red Hat Enterprise Linux 6.5 64bit English Version	RHEL	24-hour support	spt_24h
Red Hat Enterprise Linux 7.2 64bit English Version	RHEL	24-hour support	spt_24h
CentOS 6.5 64bit English Version	CentOS6.5	No support	nosupport
CentOS 7.2 64bit English Version	CentOS	No support	nosupport
Ubuntu Server 14.04 LTS English Version	UBUNTU	No support	nosupport
Microsoft SQL Server 2014 SE 64bit English Version	MSSQL2K14SE	No support	nosupport

A.4 Common Network Services

The following common network services are provided and available on virtual networks:

- DNS server (name resolution on the network)
- yum repository mirror server
- Red Hat Update Infrastructure (RHUI)
- Windows activation (KMS)
- NTP server

The following is a list of servers that provide common network services:

DNS Server

Table 165: Eastern Japan Region 1 (jp-east-1)

Availability Zone	Name Server 1	Name Server 2
jp-east-1a	133.162.193.9	133.162.193.10
jp-east-1b	133.162.201.9	133.162.201.10

Table 166: Western Japan Region 1 (jp-west-1)

Availability Zone	Name Server 1	Name Server 2
jp-west-1a	133.162.161.9	133.162.161.10
jp-west-1b	133.162.169.9	133.162.169.10

Table 167: Western Japan Region 2 (jp-west-2)

Availability Zone	Name Server 1	Name Server 2
jp-west-2a	133.162.145.9	133.162.145.10
jp-west-2b	133.162.153.9	133.162.153.10

Table 168: UK Region 1 (uk-1)

Availability Zone	Name Server 1	Name Server 2
uk-1a	62.60.39.9	62.60.39.10
uk-1b	62.60.42.9	62.60.42.10

yum repository mirror server

Table 169: Eastern Japan Region 1 (jp-east-1)

Availability Zone	FQDN
Common to all AZ	yum.jp-east-1.cloud.global.fujitsu.com

Table 170: Western Japan Region 1 (jp-west-1)

Availability Zone	FQDN
Common to all AZ	yum.jp-west-1.cloud.global.fujitsu.com

Table 171: Western Japan Region 2 (jp-west-2)

Availability Zone	FQDN
Common to all AZ	yum.jp-west-2.cloud.global.fujitsu.com

Table 172: UK Region 1 (uk-1)

Availability Zone	FQDN
Common to all AZ	yum.uk-1.cloud.global.fujitsu.com

Windows Activation (KMS)

Table 173: Eastern Japan Region 1 (jp-east-1)

Availability Zone	FQDN
Common to all AZ	kms.jp-east-1.cloud.global.fujitsu.com

Table 174: Western Japan Region 1 (jp-west-1)

Availability Zone	FQDN
Common to all AZ	kms.jp-west-1.cloud.global.fujitsu.com

Table 175: Western Japan Region 2 (jp-west-2)

Availability Zone	FQDN
Common to all AZ	kms.jp-west-2.cloud.global.fujitsu.com

Table 176: UK Region 1 (uk-1)

Availability Zone	FQDN
Common to all AZ	kms.uk-1.cloud.global.fujitsu.com

NTP Server

Table 177: Eastern Japan Region 1 (jp-east-1)

Availability Zone	NTP Server 1	NTP Server 2
jp-east-1a	133.162.193.106	133.162.195.141
jp-east-1b	133.162.203.207	133.162.203.208

Table 178: Western Japan Region 1 (jp-west-1)

Availability Zone	NTP Server 1	NTP Server 2
jp-west-1a	133.162.161.19	133.162.161.20
jp-west-1b	133.162.169.19	133.162.169.20

Table 179: Western Japan Region 2 (jp-west-2)

Availability Zone	NTP Server 1	NTP Server 2
jp-west-2a	133.162.145.19	133.162.145.20
jp-west-2b	133.162.153.19	133.162.153.20

Table 180: UK Region 1 (uk-1)

Availability Zone	NTP Server 1	NTP Server 2
uk-1a	62.60.39.19	62.60.39.20
uk-1b	62.60.42.19	62.60.42.20

A.5 Domains That Can Be Registered in a Zone

The domains that you can register in a zone are as follows.

Table 181: List of Domains That Can Be Registered in a Zone

.ae.org	.ar.com	.br.com	.cn.com	.de.com
.eu.com	.eu.org	.gb.com	.gb.net	.hu.com
.jpn.com	.kr.com	.no.com	.qc.com	.ru.com
.sa.com	.se.com	.se.net	.uk.com	.uk.net
.us.com	.uy.com	.web.com	.za.com	.za.net
.za.org	.ac	.ae	.aero	.af
.ag	.ai	.al	.am	.edu.ar
.ar	.arpa	.as	.asia	.at
.asn.au	.com.au	.id.au	.net.au	.org.au
.au	.az	.ba	.be	.bg

.bi	.biz	.bj	.bm	.bo
.br	.bs	.bv	.by	.bz
.co.ca	.ca	.cat	.cc	.cd
.cg	.ch	.ci	.ck	.cl
.co.cm	.com.cm	.net.cm	.edu.cn	.cn
.com	.coop	.cu	.cx	.cy
.cz	.de	.dk	.dm	.do
.dz	.ec	.edu	.ee	.eg
.es	.eu	.fi	.fj	.fm
.fo	.fr	.gd	.gi	.gov
.gg	.gm	.gp	.gr	.gs
.gt	.hk	.hm	.hn	.hr
.ht	.hu	.id	.ie	.il
.in	.info	.int	.io	.ir
.im	.is	.it	.je	.jobs
.jp	.ke	.kp	.kg	.ki
.kr	.kz	.la	.lb	.lc
.li	.lk	.lt	.lu	.lv
.ly	.ma	.md	.me	.mil
.mk	.mm	.mn	.mobi	.ms
.mt	.mu	.museum	.mw	.mx
.my	.na	.name	.net	.nf
.ng	.nl	.no	.nu	.nz
.org	.pa	.pe	.pk	.pl
.pm	.pr	.pro	.ps	.pt
.pw	.re	.ro	.edu.ru	.ru
.rw	.sa	.sb	.sc	.se
.sg	.sh	.si	.sj	.sk
.sl	.sm	.sn	.so	.sr
.st	.su	.sv	.tc	.tel
.tf	.tg	.th	.tj	.tk
.tl	.tm	.tn	.to	.tr
.travel	.tt	.tv	.tw	.ua
.ug	.ac.uk	.gov.uk	.uk	.fed.us
.us	.com.uy	.uy	.co.uz	.com.uz
.uz	.va	.vc	.ve	.vi
.vg	.vn	.vu	.wf	.ws

.xn--mgbaam7a8h	.yt	.yu	.ac.za	.org.za
.co.za	.nom.za	.co.zw	co.jp	or.jp
ne.jp	ac.jp	ad.jp	ed.jp	go.jp
gr.jp	lg.jp	hokkaido.jp	aomori.jp	iwate.jp
miyagi.jp	akita.jp	yamagata.jp	fukushima.jp	ibaraki.jp
tochigi.jp	gunma.jp	saitama.jp	chiba.jp	tokyo.jp
kanagawa.jp	niigata.jp	toyama.jp	ishikawa.jp	fukui.jp
yamanashi.jp	nagano.jp	gifu.jp	shizuoka.jp	aichi.jp
mie.jp	shiga.jp	kyoto.jp	osaka.jp	hyogo.jp
nara.jp	wakayama.jp	tottori.jp	shimane.jp	okayama.jp
hiroshima.jp	yamaguchi.jp	tokushima.jp	kagawa.jp	ehime.jp
kochi.jp	fukuoka.jp	saga.jp	nagasaki.jp	kumamoto.jp
oita.jp	miyazaki.jp	kagoshima.jp	okinawa.jp	

A.6 Lists of Monitored Items

Lists of the standard metrics provided with the monitoring service are shown below.

Common Specifications

The measurements for monitored items are divided into the following three types.

Table 182: Monitored Items - Types of Metering

Type	Description
cumulative	Displays the cumulative value. This is the cumulative figure for values that are always increasing or decreasing
gauge	Displays discrete/fluctuating values. This is an instantaneous value when samples are collected
delta	Displays the differential value. This is the amount of change during the collection interval for values that are always increasing or decreasing.

These types are abbreviated as C, G, and D in the following tables.

Network

Table 183: Network Services - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.ip.floating	G	ip	Number of global IP addresses

Table 184: Load Distribution Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.loadbalancing.instance.healthy	G	instance	Number of virtual servers running normally
fcx.loadbalancing.instance.unhealthy	G	instance	Number of virtual servers that are experiencing abnormality
fcx.loadbalancing.throughput	D	B	Difference of throughput

Compute

Table 185: Compute Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.compute.instance	G	instance	Number of virtual servers
fcx.compute.cpu_util	G	%	CPU usage rate
fcx.compute.vcpus	G	vcpu	Number of vCPUs
fcx.compute.disk.read.requests	C	request	Number of disk reads
fcx.compute.disk.read.requests.rate	G	request/s	Number of disk reads per second
fcx.compute.disk.write.requests	C	request	Number of disk writes
fcx.compute.disk.write.requests.rate	G	request/s	Number of disk writes per second
fcx.compute.disk.read.bytes	C	B	Number of disk bytes read
fcx.compute.disk.read.bytes.rate	G	B/s	Number of disk bytes read per second
fcx.compute.disk.write.bytes	C	B	Number of disk bytes written
fcx.compute.disk.write.bytes.rate	G	B/s	Number of disk bytes written per second
fcx.compute.disk.root.size	G	GB	Capacity of root disk
fcx.compute.network.incoming.bytes	C	B	Number of bytes received by the network interface
fcx.compute.network.incoming.bytes.rate	G	B/s	Number of bytes received by the network interface per second
fcx.compute.network.outgoing.bytes	C	B	Number of bytes sent by the network interface
fcx.compute.network.outgoing.bytes.rate	G	B/s	Number of bytes sent by the network interface per second

Monitored Item	Type	Units	Description
fcx.compute.instance.status_check.failed	G	count	Status check information for instance • 0: Normal • 1: Error

Storage

Table 186: Block Storage - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.blockstorage.volume.size	G	GB	Capacity of block storage

Table 187: Object Storage Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.storage.objects.size	G	B	Total size of object

Image Archiving Service

Table 188: Image Archiving Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.image.size	G	B	Size of uploaded image

Database

Table 189: Database Environment Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.database.disk.bin_log.size	G	B	Size of disk area used exclusively for binary log on master
fcx.database.cpu_util	G	%	CPU usage rate
fcx.database.connections	G	connection	Number of current database connections
fcx.database.disk.wait.requests	G	request	Number of unprocessed disk I/O access requests (read/write requests)
fcx.database.memory.free	G	B	Amount of available RAM
fcx.database.disk.free	G	B	Amount of available storage space
fcx.database.replica.lag	G	s	Lag from source DB instance to read replica DB instance

Monitored Item	Type	Units	Description
fcx.database.swap.size	G	B	Size of swap space used for DB instance
fcx.database.disk.read.requests.rate	G	request/s	Average number of disk read operations per second
fcx.database.disk.write.requests.rate	G	request/s	Average number of disk write operations per second
fcx.database.disk.read.latency	G	s	Average time required for a single disk read operation
fcx.database.disk.write.latency	G	s	Average time required for a single disk write operation
fcx.database.disk.read.bytes.rate	G	B/s	Average number of bytes read from the disk per second
fcx.database.disk.write.bytes.rate	G	B/s	Average number of bytes written to the disk per second

A.7 Formula for Estimation

When you use the functions of K5 IaaS, you may need to estimate the setting values. This section describes the reasons for the setting values and how to estimate them.


Note

The estimation formulas use parameter names in the API so that you can refer to the correct numeric values. Refer to API Reference Manual as needed.

Formula for Estimating Cool Down Period after Auto-Scaling

If you use auto-scaling and the cool down period is not specified appropriately, scaling occurs without sufficient time after the previous scaling. This may cause unexpected behavior and undesirable effects, including the creation of excess resources. For example, if CPU usage rate is used as a threshold value and the cool down period is not specified appropriately, the virtual servers added by the first scale out may cause other virtual servers to be added one after another before load balancing occurs.

To prevent scaling from occurring more frequently than expected, specify the cool down period as whichever is the larger of the two values produced by the following two formulas:

- Formula for calculating a cool down period in case of scaling out (in seconds)

```
(<Time required for creating a virtual server> + <HealthCheckGracePeriod
 value of FCX::AutoScaling::AutoScalingGroup>) x <ScalingAdjustment
 value of FCX::AutoScaling::ScalingPolicy> + <Time required for deleting
 a virtual server> x 5 + <period value of OS::Ceilometer::Alarm> x
 <evaluation_periods value of OS::Ceilometer::Alarm>
```

- Formula for calculating a cool down period in case of scaling in (in seconds)

```
<Time required for deleting a virtual server> x <ScalingAdjustment
 value of FCX::AutoScaling::ScalingPolicy> + <period value
 of OS::Ceilometer::Alarm> x <evaluation_periods value of
 OS::Ceilometer::Alarm>
```

A.8 Setup of SQL Server

A.8.1 SQL Server 2014 Standard Edition Usage Guide

This section describes the procedure to make SQL Server available after creating a virtual server from the "Windows Server 2012 R2 Standard Edition + SQL Server 2014 Standard Edition" image.

Before you begin

Create a virtual server using an image with SQL Server 2014 Standard Edition installed.

About this task

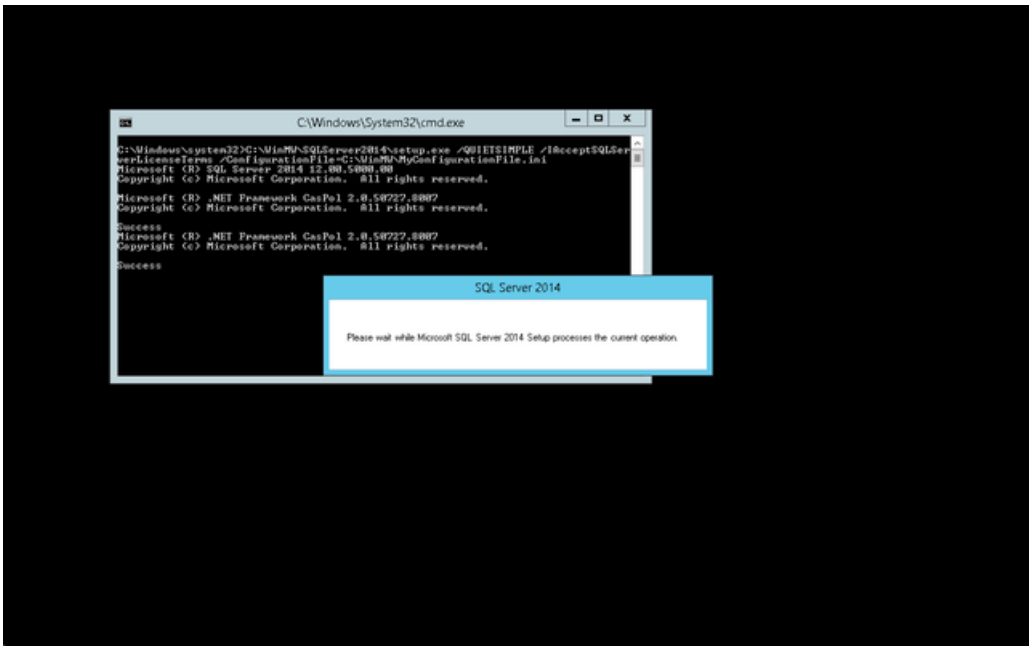
Complete the setup of SQL Server 2014 by following the procedure below.

Procedure

1. Confirm that the virtual server has started, and then log on to the virtual server as the default user "k5user."

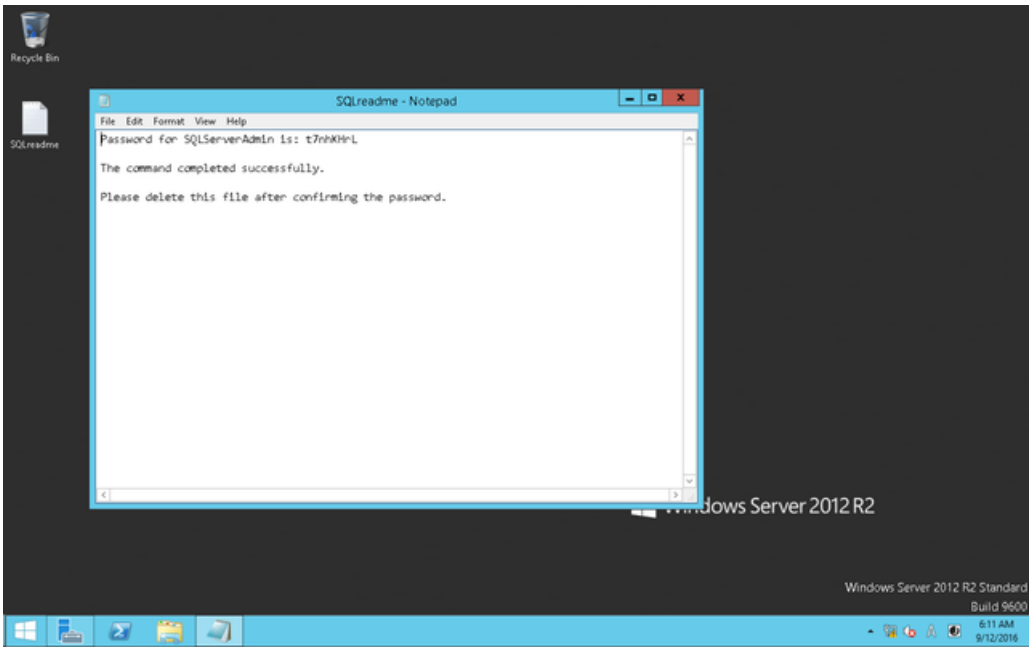
   Note: After logging on to the virtual server, do not stop or release the virtual server until the following setup procedure has been completed.

2. Installation of SQL Server 2014 automatically starts as shown below.

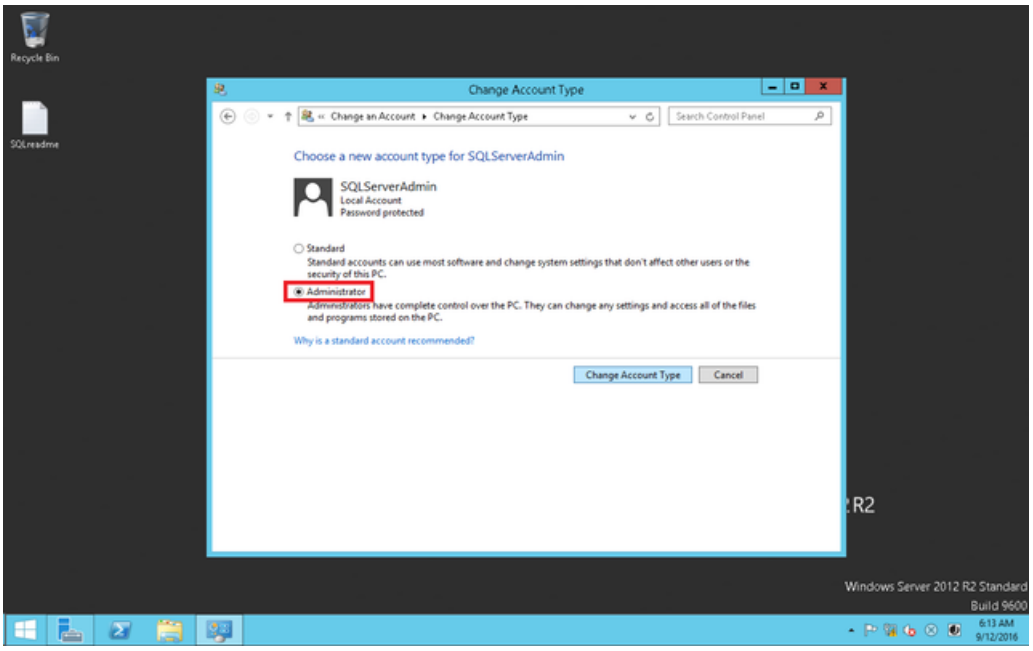


3. When installation is completed, the password file for the SQL Server administration account is created on the desktop.

   Tip: The SQL Server administration account name is "SQLServerAdmin."



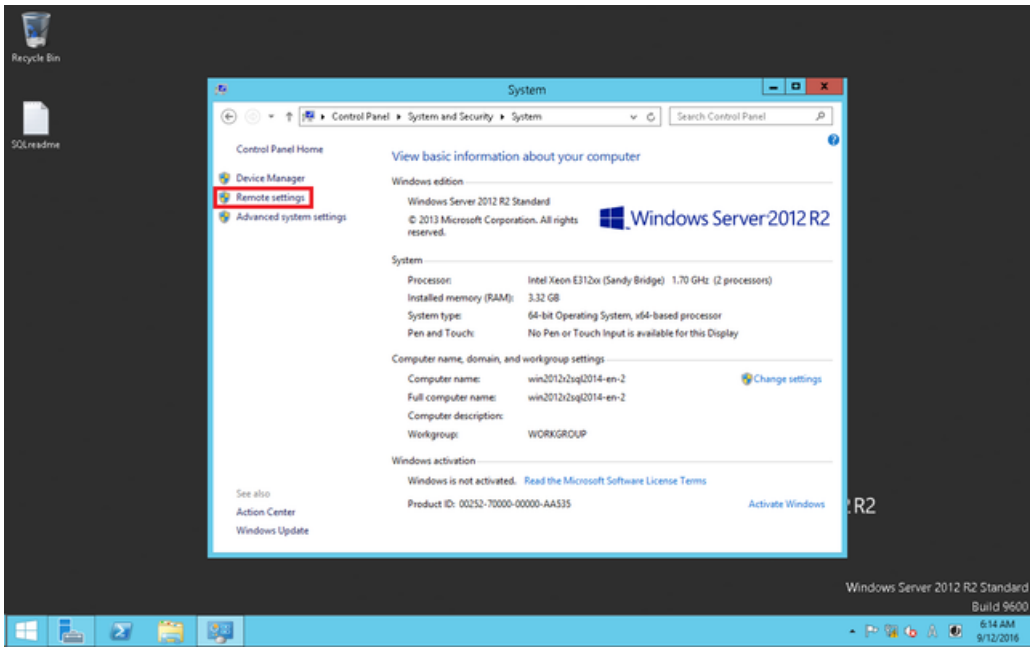
4. To use the "SQLServerAdmin" account to connect to Integration Services, change the account type to [Administrator].



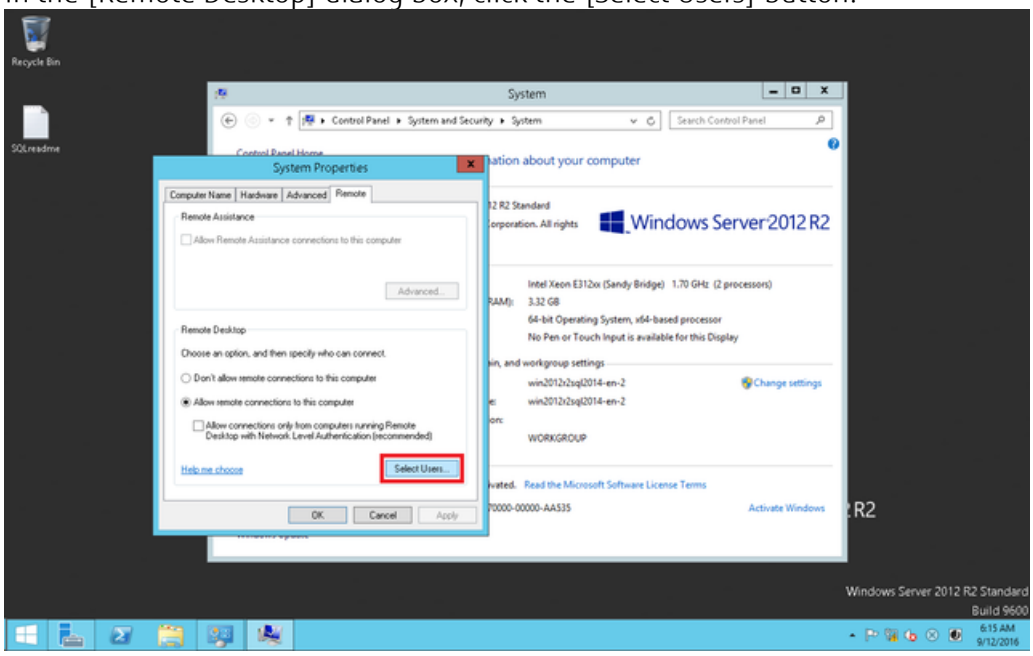
Tip

To use the "SQLServerAdmin" account as is without changing to an Administrator account, add "SQLServerAdmin" to the remote desktop users by following the procedure below.

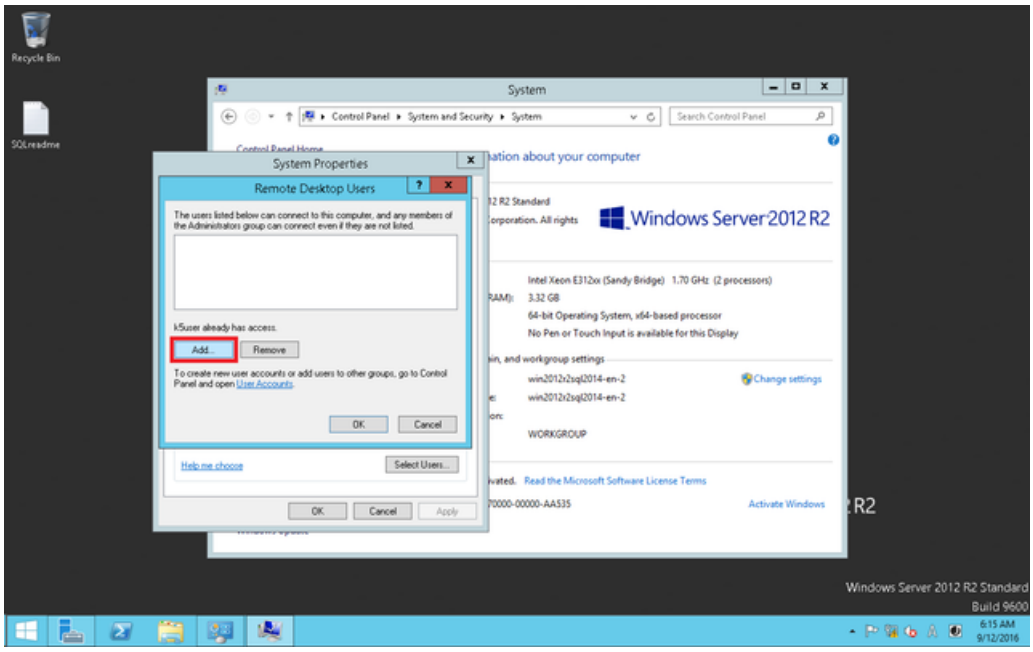
1. From the Start menu, click [Control Panel] > [System and Security] > [System] > [Remote settings].



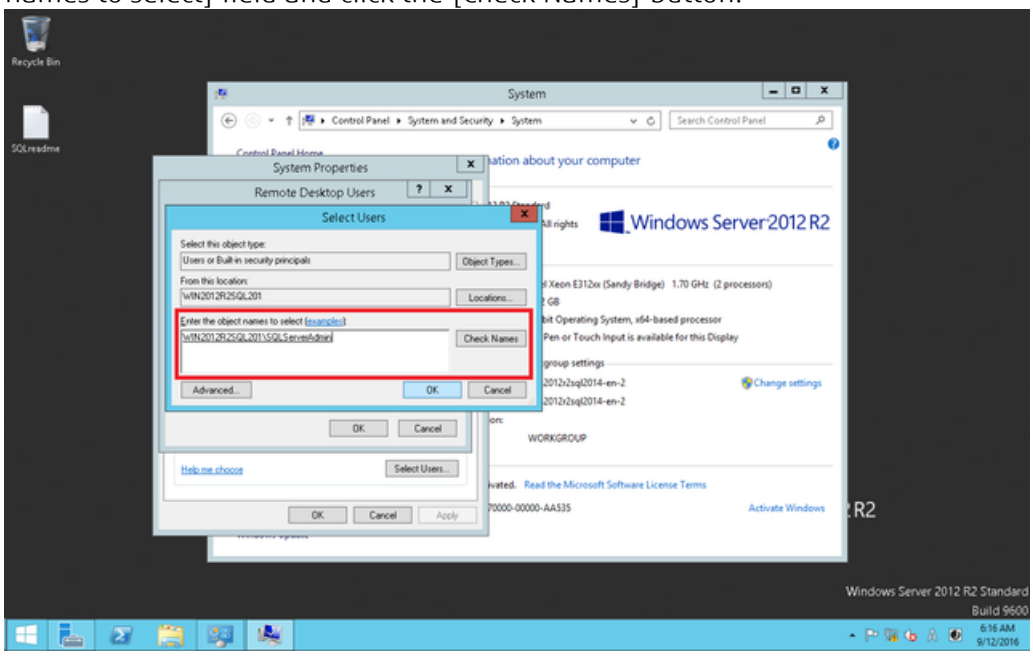
2. In the [Remote Desktop] dialog box, click the [Select Users] button.



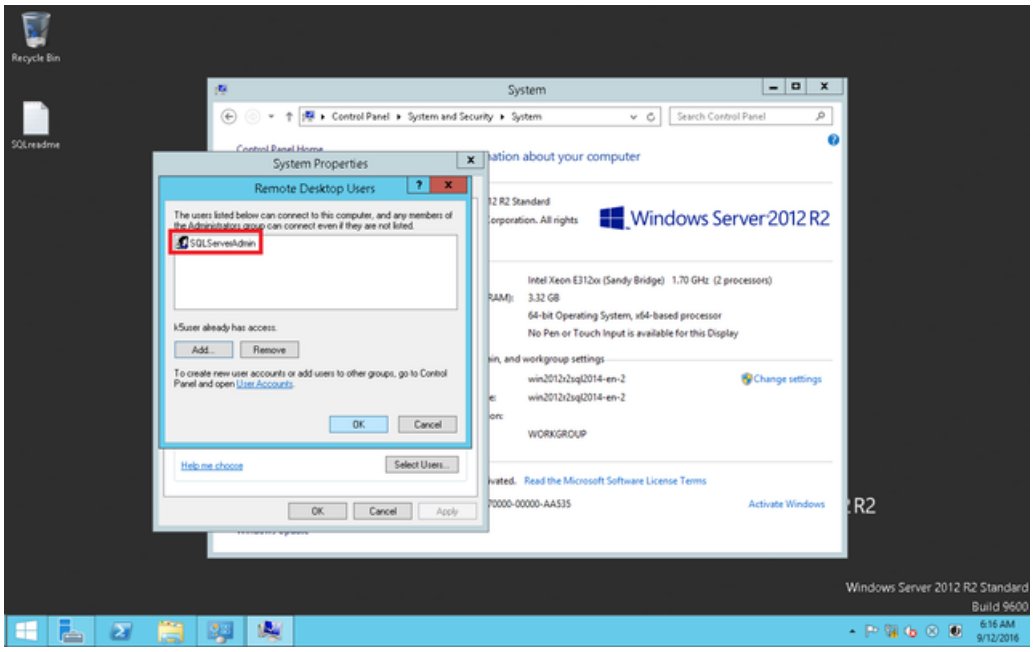
3. In the [Remote Desktop Users] dialog box, click the [Add] button.



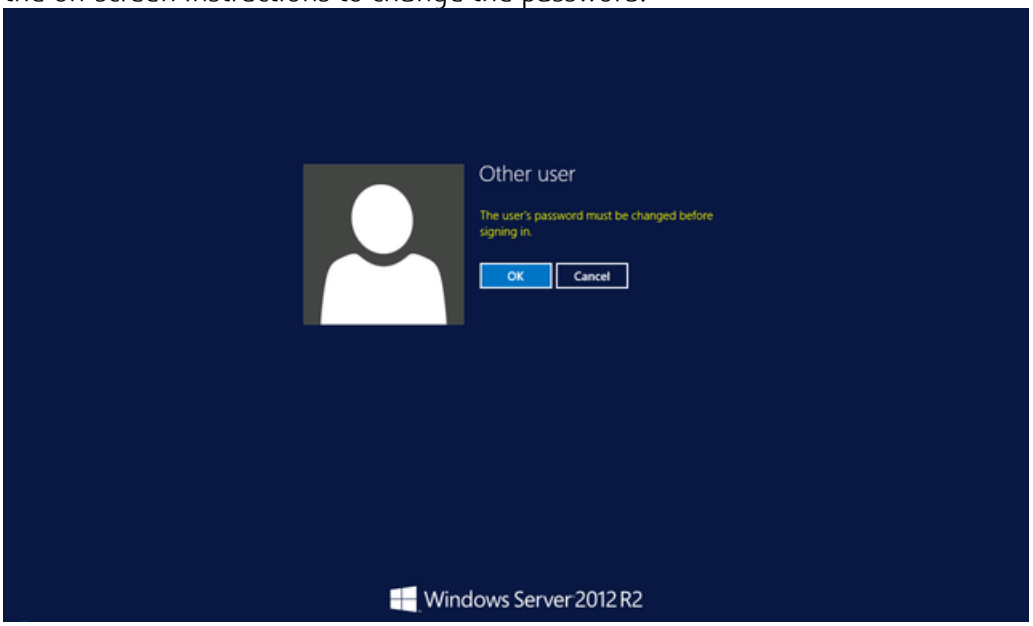
4. In the [Select Users] dialog box, enter "SQLServerAdmin" in the [Enter the object names to select] field and click the [Check Names] button.



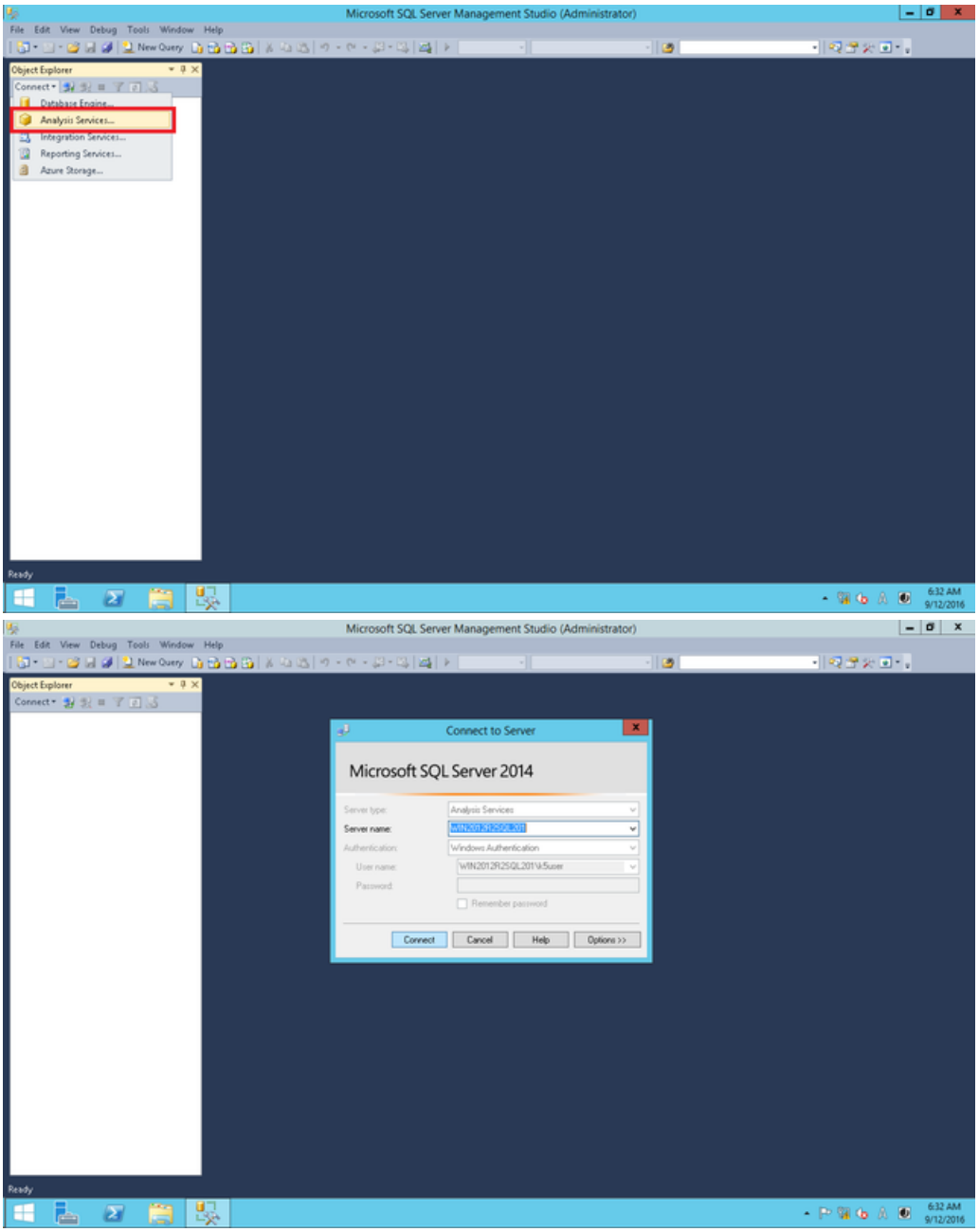
5. Click the [OK] button.
6. In the [Remote Desktop Users] dialog box, confirm that "SQLServerAdmin" has been added.



5. Restart the virtual server.
6. When the server starts up, log on to Windows as "SQLServerAdmin."
   When the logon is completed, the dialog box to prompt a password change appears. Follow the on-screen instructions to change the password.



7. Select [Apps] > [SQL Server Management Studio].
8. Confirm that a connection can be established with the "SQLServerAdmin" account.



This completes the setup procedure.

Tip

Table 190: List of Execution Accounts for SQL Server Related Services

Service	Account Name
SQL Server Agent	NT Service\SQLSERVERAGENT
SQL Server Database Engine	NT Service\MSSQLSERVER
SQL Server Analysis Services	NT Service\MSSQLServerOLAPService
SQL Server Reporting Services	NT Service\ReportServer
SQL Server Integration Services	NT Service\MsDtsServer120
SQL Server Distributed Replay Client	NT Service\SQL Server Distributed Replay Client

Service	Account Name
SQL Server Distributed Replay Controller	NT Service\SQL Server Distributed Replay Controller

FUJITSU Cloud Service K5 IaaS

Features Handbook 1.9 version

Published Date September, 2016