FUJITSU Cloud Service for OSS IaaS

Features Handbook

Version 3.8
FUJITSU LIMITED

K5IA-DC-M-004-016E

Preface

Purpose of This Manual

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

- When considering using the services and functions of 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 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.
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.
API Reference Manual	This document includes 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.
Database Service User Guide	This document explains the basic method of operation of the database service.

Abbreviations Used in This Manual

In this manual, product names are abbreviated as follows.

Official Name	Abbreviation	
FUJITSU Cloud Service for OSS IaaS	IaaS	
Microsoft® Windows Server®	Windows Server	Windows
Microsoft® Windows Server® 2016	Windows 2016	
Microsoft® Windows Server® 2012 R2	Windows 2012 R2	
Microsoft® Windows Server® 2012	Windows 2012	
Microsoft® Windows Server® 2008 R2	Windows 2008 R2	
Microsoft® Windows Server® 2008	Windows 2008	
Windows® 10	Windows 10	
Windows® 8.1	Windows 8.1	
Windows® 7	Windows 7	
Red Hat® Enterprise Linux® 6.x (for Intel64) (x is a number)	RHEL6.x (x is a number)	Linux
Red Hat® Enterprise Linux® 7.x (for Intel64) (x is a number)	RHEL7.x (x is a number)	
Red Hat® OpenShift Container Platform 3.x (English) (x is a number)	RHOCP 3.x (x is a number)	
Community Enterprise Operating System 6.x (x is a number)	CentOS 6.x (x is a number)	CentOS
Community Enterprise Operating System 7.x (x is a number)	CentOS 7.x (x is a number)	
Red Hat Update Infrastructure	RHUI	
Red Hat Enterprise Linux AUS (AMC Update Support)	RHEL AUS	
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, Red Hat Enterprise Linux, and OpenShift are trademarks of Red Hat, Inc. registered in the United States and/or other countries.
- Ubuntu is a registered trademark of Canonical Ltd.

- The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission.
- 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

The revision history for this manual is indicated below.
For the revision history prior to edition 3.0, refer to Revision History Prior to Edition 3.0.

Edition	Date of Update	Location	Overview
3.0	June 29, 2018	Creating a Virtual Database Server Database Operations	Function added
		Load Balancer Service	Description added
		Email Functions	Description added
		Limiting Values	Description added
		Connection/Disconnection from an OpenVPN Client (CentOS)	Description modified
3.1	July 31, 2018	OS Provision Service System Storage List of Software Support Service IDs	OS image added
		OS Provision Service Red Hat Update Infrastructure 3.0 Usage Procedure	Description regarding AUS added
		Provisioning Script Function	Description added
		Port Management	Description added
		SSL-VPN Connection	Description added
		Common Network Services	Description modified
3.2	August 30, 2018	Virtual Server for SAP	Added high performance storage
		Virtual Server for SAP Managing Virtual Server for SAP Cloning Images (Private Images) Managing Virtual Server for SAP Backup Images	Function added
		Region What is Virtual Server Import?	Description added
		Virtual Server Remote Console Function	Description added

Edition	Date of Update	Location	Overview
		Port Management	Description added
		Relationships with the Firewall Service and Security Group Function	Description modified
		Creating a Virtual Database Server	Description added
		Limiting Values	Description added
		Lists of Monitored Items	Description added
		Procedure for Connecting to the WSUS (Windows Server Update Services) Server	Description added
3.3	September 25, 2018	Database Operations	Function added
		OS Patch/Update Settings	Description modified
		Registering/Deleting an Object	Description added
		Creating/Deleting a Virtual Server for SAP	Corrected an error
3.4	-	-	-
3.5	October 18, 2018	Virtual Router Function	Description added
		Private Connection Function Direct Port Connection Function	Corrected an error
3.6	November 22, 2018	Virtual Server for SAP	Description added
		Security Group Functions Firewall Service	Description added
		IPsec VPN Function	Description added
		SSL-VPN Connection	Description added
		Load Distribution Condition Settings Monitoring for Abnormality on a Load Distribution Target	Description added
		Preset Roles and Privileges	Description added
		Connection/Disconnection from an OpenVPN Client (Windows) Connection/Disconnection from an OpenVPN Client (CentOS)	Description added

Edition	Date of Update	Location	Overview
		Character Strings Specifiable for Names	Description added
		Connection/Disconnection from an OpenVPN Client (CentOS)	Corrected an error
3.7	-	-	-
3.8	December 25, 2018	Red Hat Update Infrastructure 3.0 Usage Procedure Repositories Usable with Red Hat Update Infrastructure 3.0	Function added
		IPsec VPN Function SSL-VPN Connection	Description added
		Firewall Service	Description added
		Region Endpoint	Description modified
		Limiting Values	Description modified
		Port Management	Corrected an error

Contents

Part 1: Preface

Topics:

- Service Concept
- Location Services

This chapter describes the concept of 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

FUJITSU Cloud Service for OSS 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.
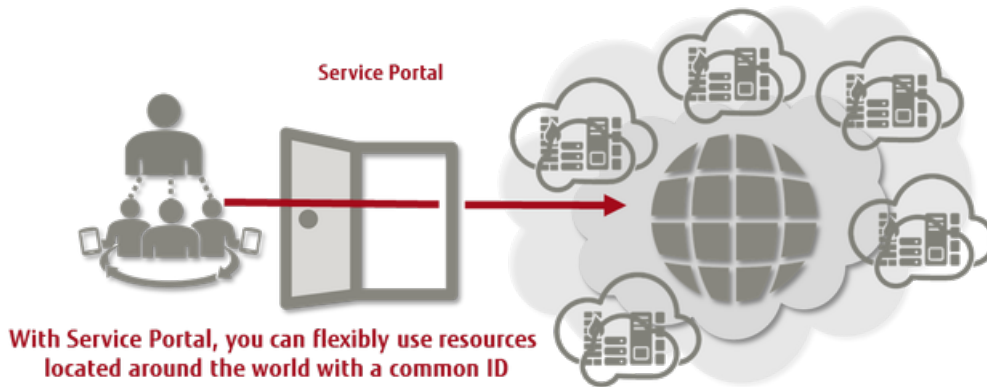
Figure 1: Global Cloud Service by Fujitsu

> **Tip**
>
> FUJITSU Cloud Service for OSS 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 IaaS. To use the full set of all functions, use the REST API.
>
> In addition, for details of the functions provided by the Service Portal, refer to the Service Portal User Guide.

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.
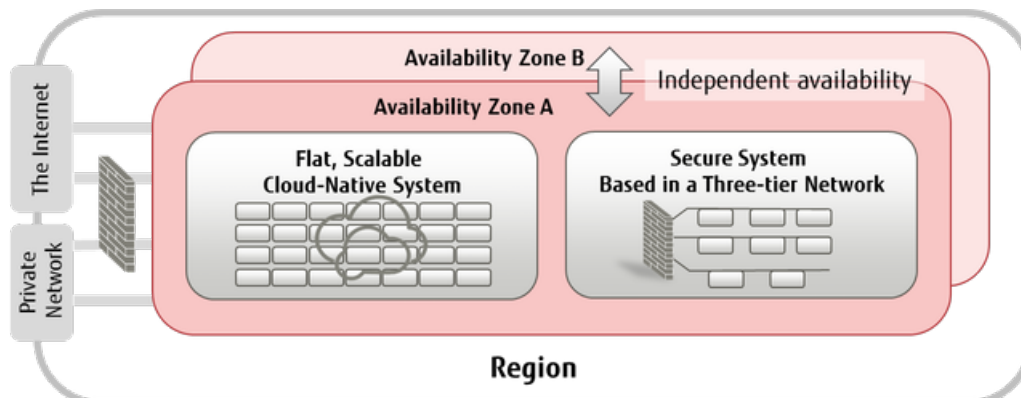
Figure 2: Providing Flexible Network Environment and Availability

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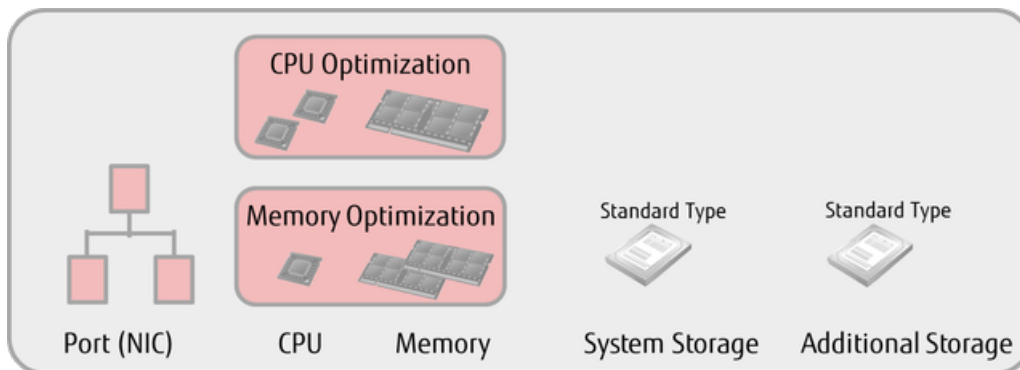
Figure 3: Providing Flexible Combinations of Virtual Resources to Fit Different Use Cases

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 IaaS.
On each of the four layers in the figure below, IaaS provides services specifically designed for your purposes and needs.
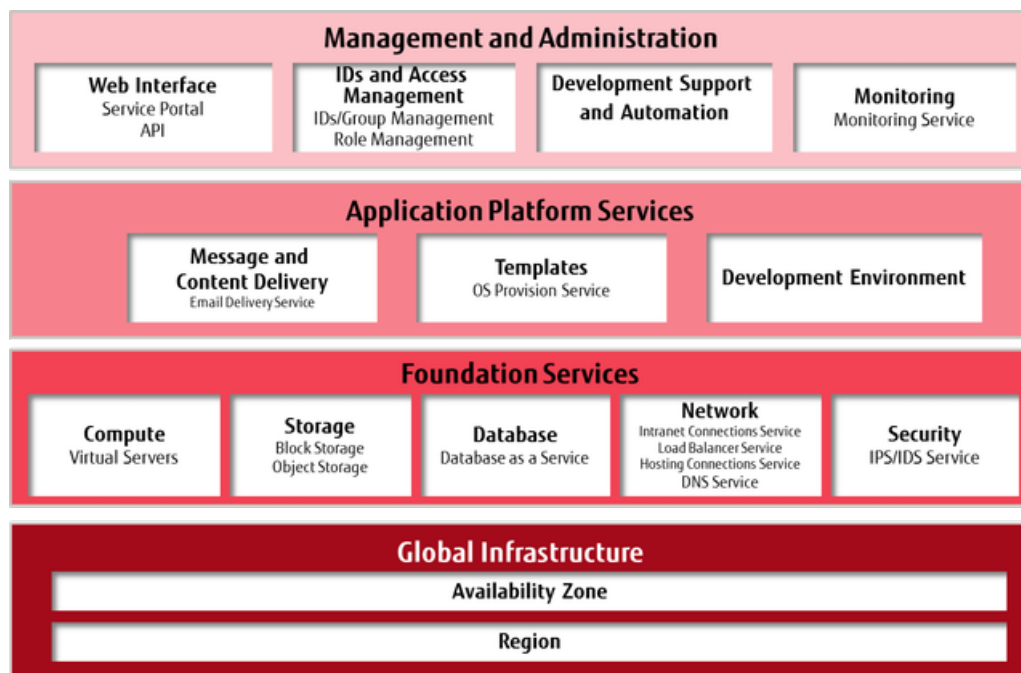
Figure 5: Structure of Services Available

Global Infrastructure

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

- Region

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

- 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 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.
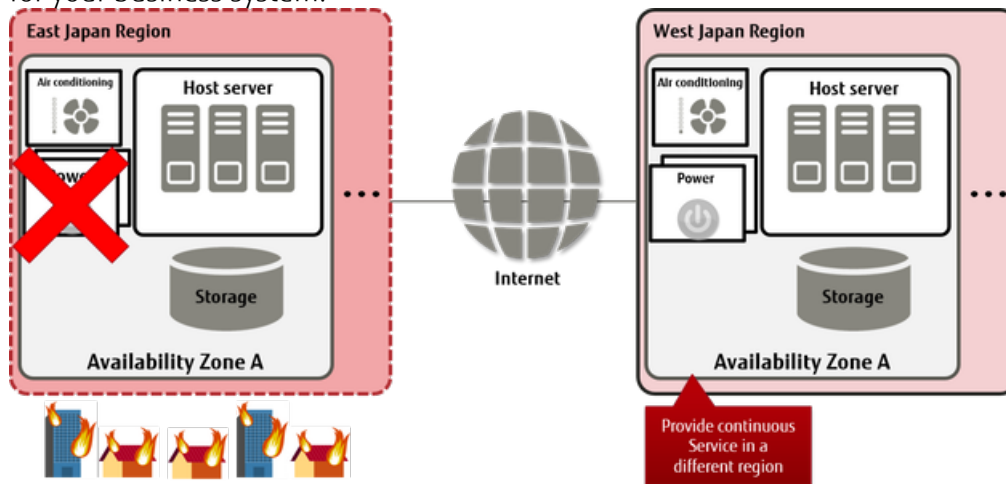
Figure 6: Example of Using Multiple Regions

Available Regions

The following regions are provided.

Table 1: List of Available Regions

Country	Name of Region	Abbreviation	Region Identifier
Japan	Eastern Japan Region 1	Japan East1	jp-east-1
	Eastern Japan Region 2	Japan East2	jp-east-2
	Western Japan Region 1	Japan West1	jp-west-1
	Western Japan Region 2	Japan West2	jp-west-2

> **Note** Eastern Japan Region 1 and Eastern Japan Region 2 are in the same physical region. When using multiple regions as a measure against disasters, please use them in combination with other regions.

IaaS Service Configurations

・Global Services

Global services have a single API endpoint as 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.

> For details, refer to the following manuals:
> *Tip*
> - Explanations of services in *IaaS Service Specification*
> - *IaaS API Reference Manual*
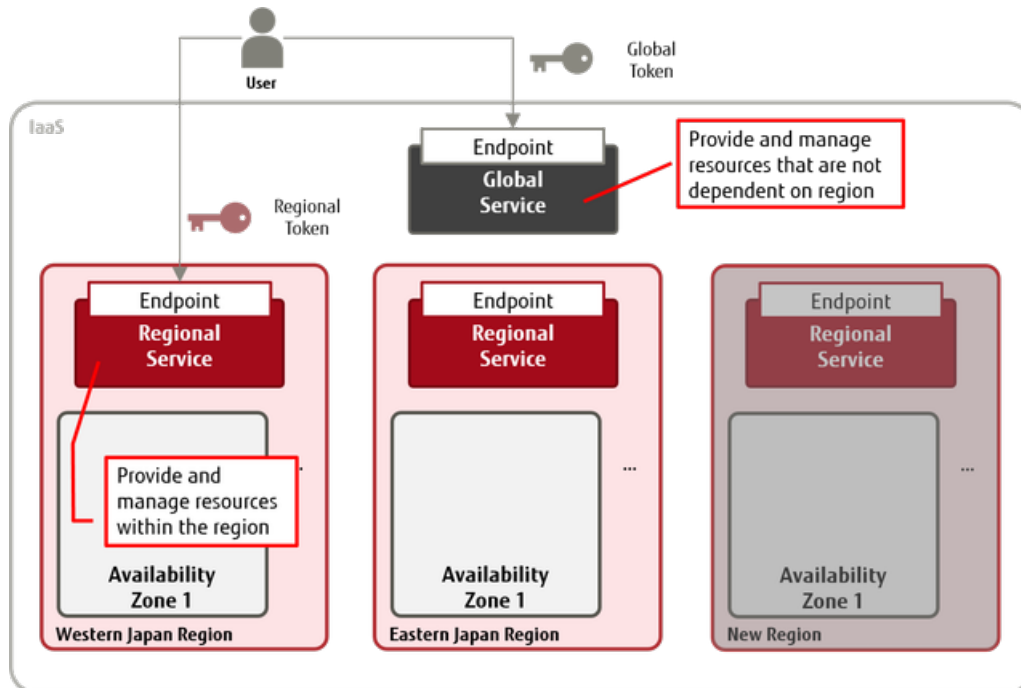
Figure 7: Concept of Global Services and Regional Services

Functions Included

- Region Activation Function

  This function is used to add a new region to the regions that are currently being used.

> When a contract number (domain) is acquired, "Eastern Japan Region 2 (jp-east-2)" can be used as the default region.
> *Tip*
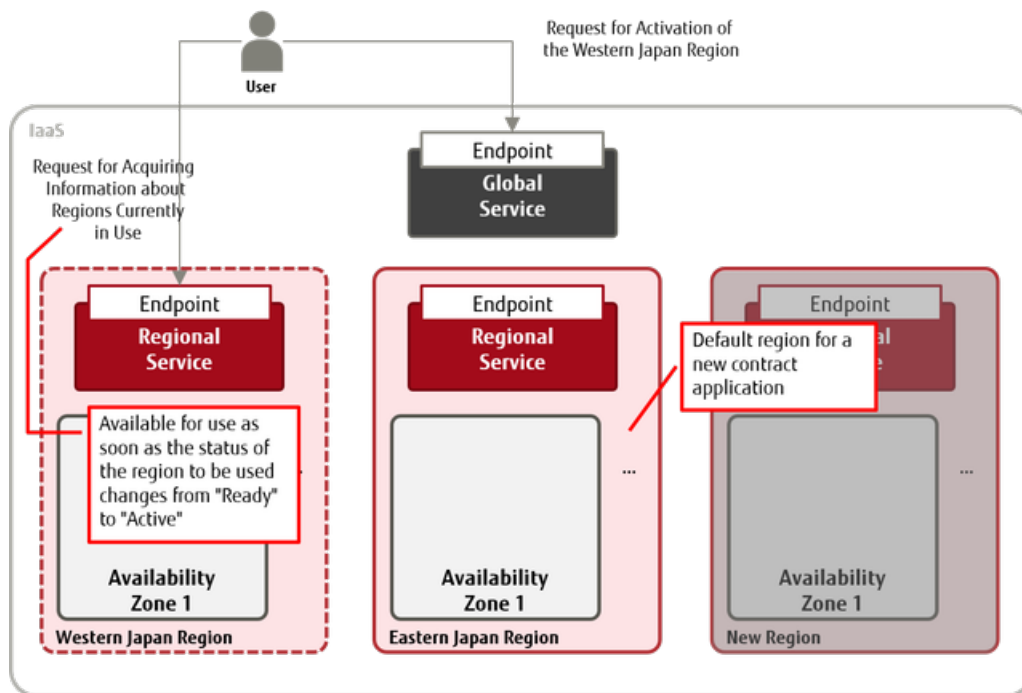
Figure 8: How to Use a Different Region

- 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.

    > 💡 Use the global user management service to acquire tokens.
    > Tip

  - Regional Authentication Function

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

    > 💡 Use the regional user management service to acquire tokens.
    > Tip

- API Endpoint

  For the API endpoints accessed in order to use the services, refer to Endpoint.

How to Use This Service

STEP 1	Selecting a Region	Select a region to add according to your system requirements.
STEP 2	Adding the Region	Add the region from Service Portal or by using an API.
STEP 3	Confirming the Region is Available for Use	Using the global user management service, confirm whether the added region has become available for use.
STEP 4	Designing the Multi-region	Create the system and operational design to suit the way in which each IaaS service is provided.
STEP 5	Starting Operation	For the new region, create resources and perform other required tasks, and start operation of the region.

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.

- Regional Services
  - Email Delivery Service

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

1.2.2 Endpoint

The API endpoints accessed in order to use the services are listed below.

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
Content Delivery 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/ Virtual Server Export	https://import-export .***.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
Mail Delivery	https://mail.***.cloud.global.fujitsu.com
Orchestration	https://orchestration.***.cloud.global.fujitsu.com
Monitoring	https://telemetry.***.cloud.global.fujitsu.com

> **Note** 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 |

1.2.3 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.
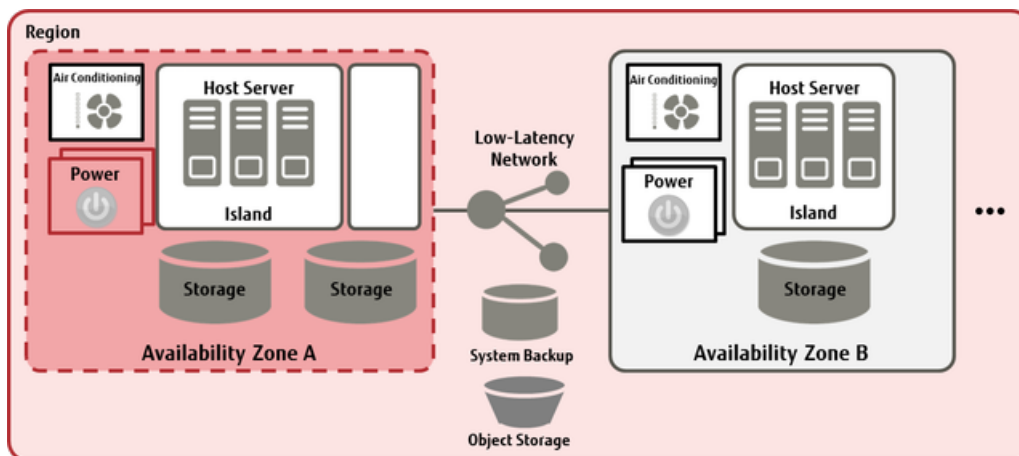
Figure 10: Example of Using Availability Zones

Part 2: Compute

Topics:

- Standard Services
- Services for SAP

With physical computers separated by virtualization technology, 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 or Software Provision Service
- Created by the user

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

  Image prepared by using virtual server import

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 group
- 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.

> **💡 Tip**
>
> For Red Hat Enterprise Linux and CentOS, the default host name for virtual servers is configured as the following:
>
> <Virtual_server_name_entered_when_creating_the_virtual_server>.fcxlocal

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**
> You can delete a virtual server even while it is running. Therefore, extra caution must be exercised when you delete one.

> **Note**
> While data obtained using a snapshot remains, it is not possible to delete the virtual server that is the source of the snapshot. To delete the virtual server, it is necessary to delete all obtained snapshots first.

> **Tip**
> - When you create a virtual server, specify whether to retain the system storage of the server upon deletion.
> - 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.

Virtual Server Type (Flavor)

There are two types of virtual server CPU: standard CPU and high-speed CPU.

Type	Overview
Standard CPU	Virtual CPU speed equivalent to 1.7 - 1.8 GHz
High-Speed CPU	Virtual CPU speed equivalent to 2.6 GHz

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

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

Type Name	Number of Virtual CPUs	Memory (GB)
P-1	1	0.5
T-1	1	1
C-1	1	2
C-2	2	4
C-4	4	8
C-8	8	16
C-16	16	32
S-1	1	4
S-2	2	8
S-4	4	16
S-8	8	32
S-16	16	64
M-1	1	8

Type Name	Number of Virtual CPUs	Memory (GB)
M-2	2	16
M-4	4	32
M-8	8	64
M-16	16	128
XM-4	4	128
LM-1	1	16
LM-2	2	32
LM-4	4	64
LM-8	8	128
L-12	12	128
L-24	24	128
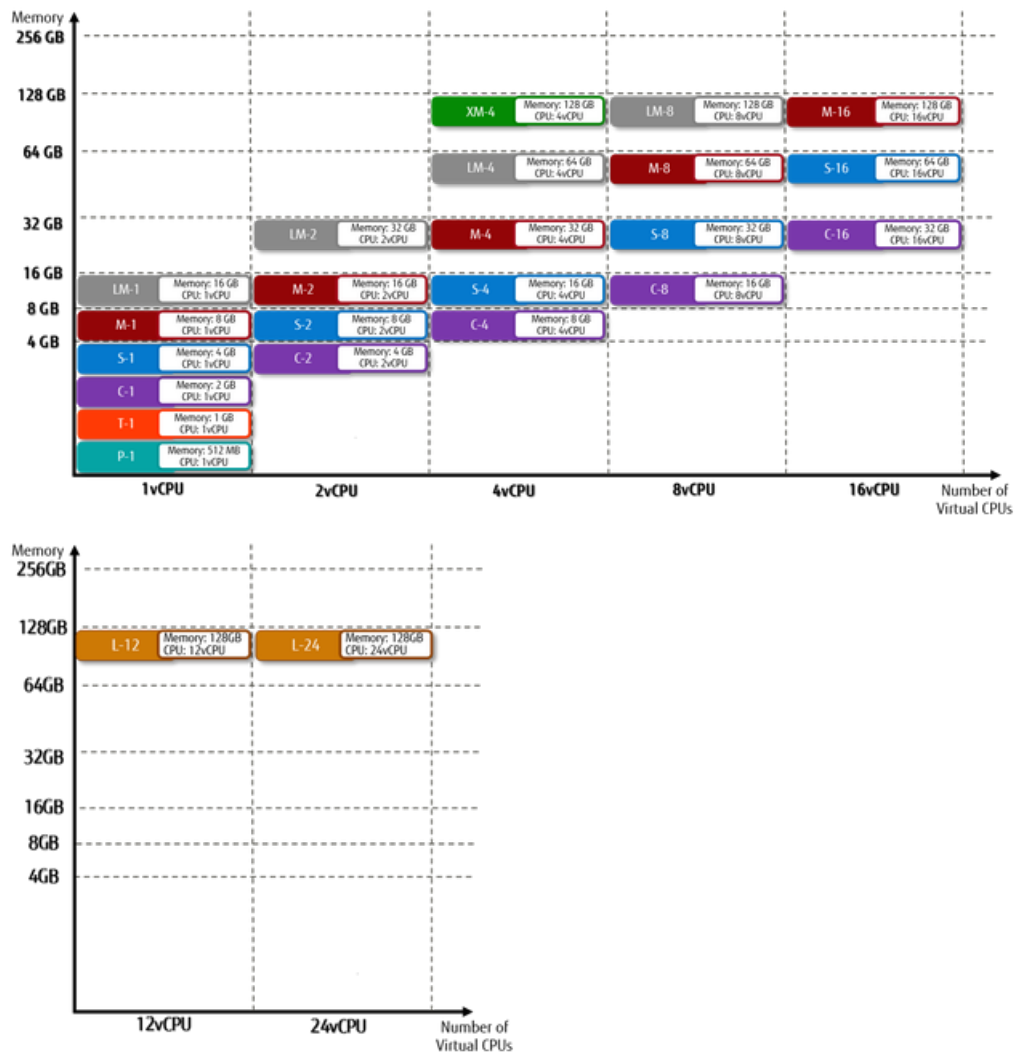
Figure 11: List of Virtual Server Types (Standard CPU)

Table 6: List of Provided Virtual Server Types (Flavors) (High-Speed CPU)

Type Name	Number of Virtual CPUs	Memory (GB)
P2-1	1	0.5
T2-1	1	1
C2-1	1	2
C2-2	2	4
C2-4	4	8
C2-8	8	16
C2-16	16	32
S2-1	1	4
S2-2	2	8
S2-4	4	16
S2-8	8	32
S2-16	16	64
M2-1	1	8
M2-2	2	16
M2-4	4	32
M2-8	8	64
M2-16	16	128
XM2-4	4	128
LM2-1	1	16
LM2-2	2	32
LM2-4	4	64
LM2-8	8	128
L2-12	12	128
L2-24	24	128

Figure 12: List of Virtual Server Types (High-Speed CPU)

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.

> **➡ Note**
> When automatic failover occurs or is completed, a notification email is sent to the overall administrator of the project the target resource belongs to. For details on notification emails, refer to Automatic Failover Notification Messages.

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.

> **➡ Note**
> Virtual servers obtain metadata from a special server on the IaaS. As necessary, configure the security group, the firewall, and routing so that virtual servers can communicate with http://169.254.169.254 via a virtual router.

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 Windows

  Describe the script using PowerShell or Windows Batch.

- For Red Hat Enterprise Linux

  Describe the script using sh or bash.
- For CentOS

  Describe the script using sh or bash.
- For Ubuntu

  Describe the script using sh or bash.
- For Red Hat OpenShift Container Platform

  Describe the script using sh or bash.

> **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 7: Software That Provides the Script Function by OS Type

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

> **Note**
> - When Cloudbase-init is installed, the "cloudbase-init" user will be created.
> - Do not delete the "cloudbase-init" user. If it is deleted, it may no longer be possible to successfully create virtual servers from private images.

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.
- When the target of resizing is a virtual server that is an operating state (ACTIVE) or shut-down state (SHUTOFF), resizing (changing of the type of virtual server) is possible.
- After performing resizing, confirm that the status of the virtual server has become "VERIFY_RESIZE", then execute "Confirm resized server" (fix the change), and then fix the resizing.

> **Note** When the virtual server is in an operating state (ACTIVE), resizing will forcibly reboot the virtual server. It is recommended to perform resizing after placing virtual servers in the shut-down state (SHUTOFF).

Rollback of Virtual Server Resizing

You can roll back the resizing of the virtual server in some situations; for example, 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 release a virtual server, regardless of whether it is in a running state or in 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 the virtual server.

> **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

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 keeps on running.

> **Tip**
> Specify the server group when you create the virtual server.
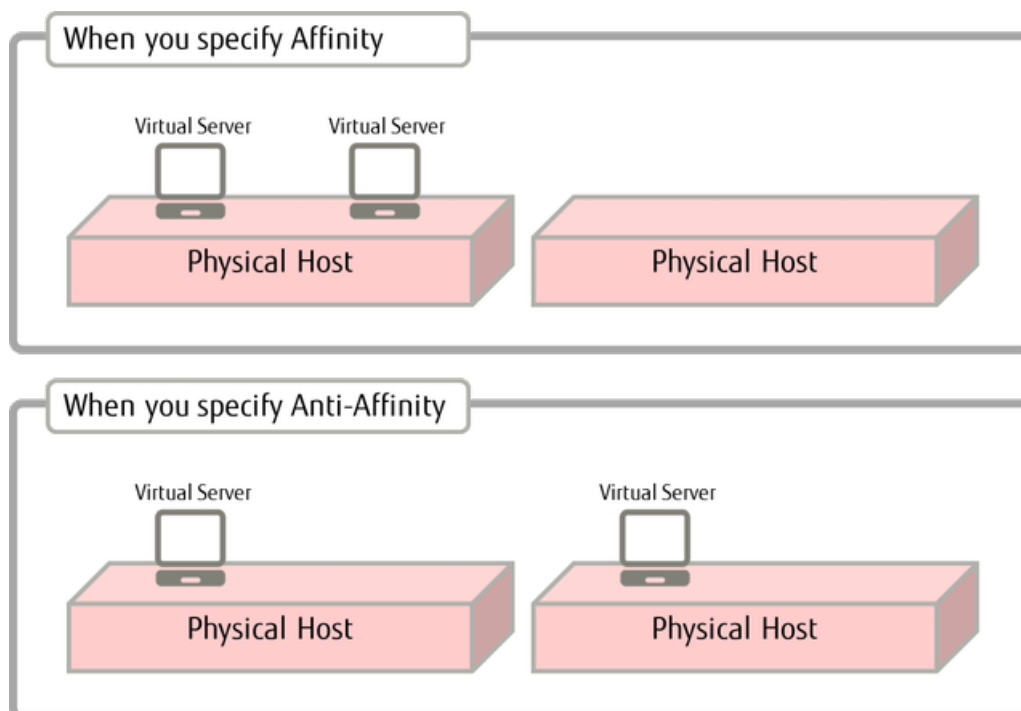
Figure 13: Operation of the Server Group Function

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 the 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 connect to the virtual server 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 when you created the virtual server.

> **Important**
> When you log in to Windows 2016 or 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 and work networks.
> ```
>
>
>
> Figure 14: Inquiry Message at Initial Login
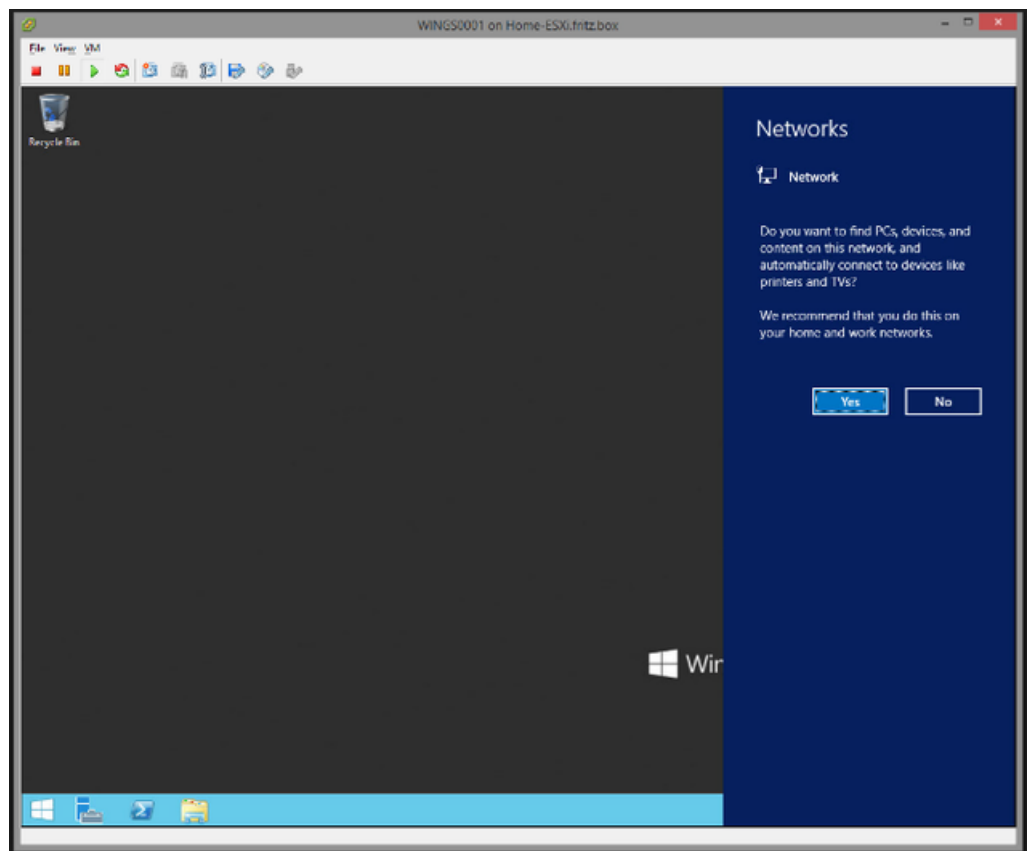
- 20 -

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.

> **Tip** The user ID for the Administrator is "k5user."

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.

> **Tip** The user ID for the Administrator is "k5user."

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 Red Hat OpenShift Container Platform Virtual Server

To log in to a Red Hat OpenShift Container Platform 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 "k5user."

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 by following the procedure below, you can acquire the key file for SSH authentication (*.pem). You can use the key file for SSH authentication (*.pem) to easily log in to a virtual server.

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).

> **Tip** Using a Downloaded Key Pair (*.pem) with PuTTY.exe

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.

Table 8: 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	

Example of Creating a Key Pair with a Passphrase

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"

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 the number of lines of the log, you can acquire the specified number of lines of console log content, from the newest line to the older lines.

> **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).

2.1.1.9 Virtual Server Remote Console Function

For cases where you cannot remotely log in with SSH or RDP to the virtual server or have other troubleshooting issues, IaaS provides a function that allows you to connect to the console of the virtual server. You can connect to the console using a web browser.

The requirements to use this function are as follows.

・Supported OS

Remote console connection is available for the following operating systems:

Windows, RedHat Enterprise Linux, CentOS, Ubuntu, RedHat OpenShift Container Platform
・Supported browsers

This function has been verified to work with the following browsers.

  ・Internet Explorer 11 (Windows 7, Windows 8.1, Windows 10)

  ・Firefox 49 (Windows 7, Windows 8.1, Windows 10)

  ・Chrome 54 (Windows 7, Windows 8.1, Windows 10)

・Keyboard settings

English-language keyboards

・Password settings

To connect to the console, you need to log in with a username and password. Therefore, be sure to prepare a user account to which a password is set.

The procedure to connect to the virtual server console is as follows.

Procedure

1. Specify the target virtual server and obtain the URL to connect to the console.

2. Enter the URL in the browser and connect to the virtual server via the console.
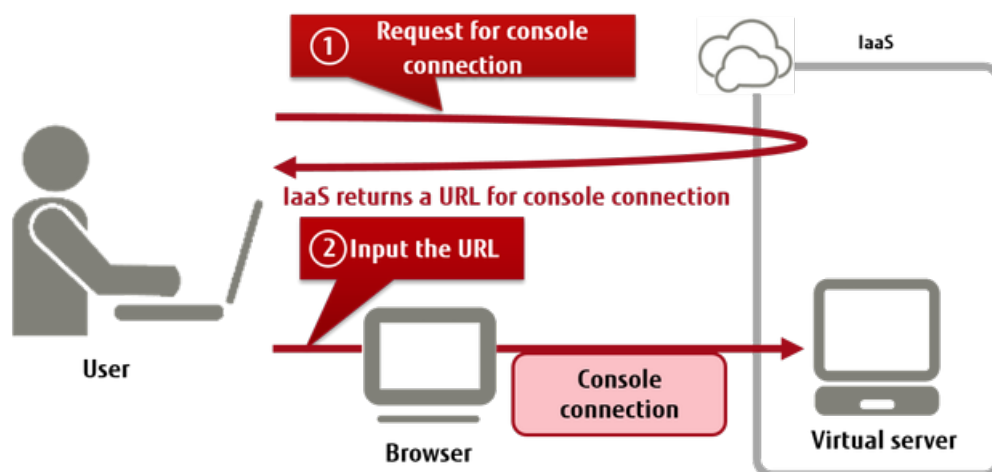
Figure 15: Console Connection to a Virtual Server

> **Note**
> - To connect to the console of a virtual server and log in to the OS, you must first be logged in by using password authentication.
> - Depending on the status of the virtual server, console connection may not be available. In addition, maintenance operations of IaaS may cause the remote console to be disconnected.
> - About URLs for connecting to the console of a virtual server
>   - The URL used for console connection expires in 10 minutes.
>   - When the region used is one of Eastern Japan Region 1, Eastern Japan Region 2, Western Japan Region 1, or Western Japan Region 2, once a URL used for console connection has been used, it cannot be reused. To reconnect to the console, obtain a new URL for console connection.
> - The maximum duration of a console connection is 30 minutes. It cannot be used continuously. Also, you cannot establish multiple console connections to one virtual server at the same time.
> - The remote console function cannot be used with services for SAP (virtual server for SAP, dedicated virtual server for SAP).
> - The remote console function of the virtual server is set up to allow normal key entry under the following conditions:
>
> | Item | Description |
> |---|---|
> | Keyboard setting of the virtual server OS | English (US, 101/102-key, etc.) |
> | Keyboard used in the client environment | English-language keyboard |
>
> In environments other than the above, certain keys may not work due to a different keyboard layout. For example, if the keyboard language in the OS of the virtual server is set to English and you use a Japanese keyboard (JIS keyboard) in your client environment, the following keyboard layout is used:

Figure 16: Keyboard Layout Used for Japanese-language Keyboards
(JIS keyboard) when the OS Keyboard Language is Set to English

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 creates a dedicated virtual server is provided.
Virtual servers for another customer will not be created on the physical host that you have secured. Therefore, this server can be used for environments that must be separate from other customers (single tenant) for reasons such as compliance and license management.

> (!) **Important** The storage and networks are shared. They cannot be dedicated to a single customer.
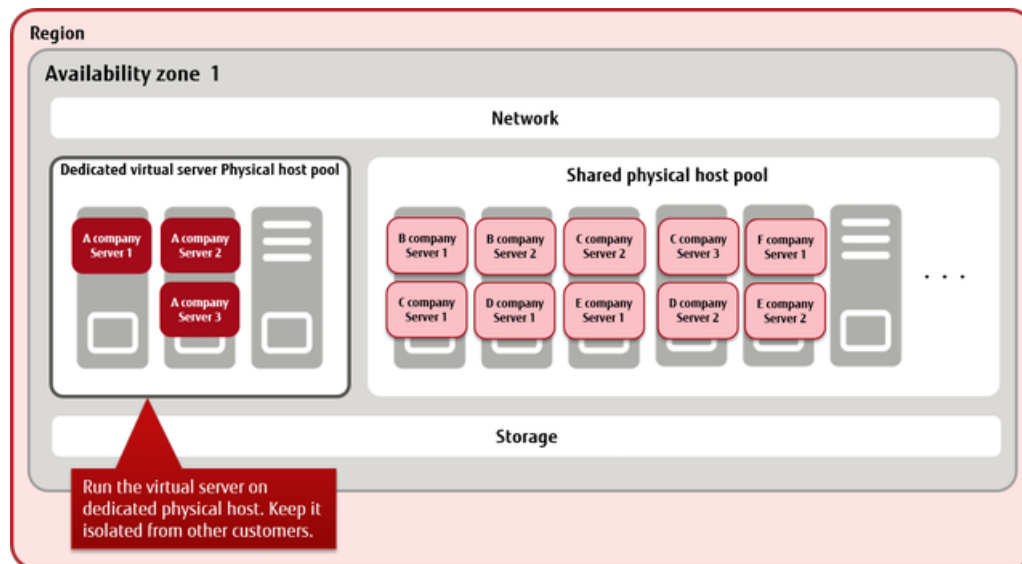
Available Server Types for Dedicated Virtual Servers

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

Table 9: List of Provided Virtual Server Types (Flavors) (Standard CPU)

Type Name	Number of Virtual CPUs	Memory (GB)
P-1	1	0.5

Type Name	Number of Virtual CPUs	Memory (GB)
T-1	1	1
C-1	1	2
C-2	2	4
C-4	4	8
C-8	8	16
C-16	16	32
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
LM-1	1	16
LM-2	2	32
LM-4	4	64
LM-8	8	128
L-12	12	128
L-24	24	128

Table 10: List of Provided Virtual Server Types (Flavors) (High-Speed CPU)

Type Name	Number of Virtual CPUs	Memory (GB)
P2-1	1	0.5
T2-1	1	1
C2-1	1	2
C2-2	2	4
C2-4	4	8
C2-8	8	16
C2-16	16	32
S2-1	1	4
S2-2	2	8
S2-4	4	16

Type Name	Number of Virtual CPUs	Memory (GB)
S2-8	8	32
S2-16	16	64
M2-1	1	8
M2-2	2	16
M2-4	4	32
M2-8	8	64
M2-16	16	128
XM2-4	4	128
LM2-1	1	16
LM2-2	2	32
LM2-4	4	64
LM2-8	8	128
L2-12	12	128
L2-24	24	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.

> **Tip**
>
> The following amounts of resources can be used by each physical host.
>
> | 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.
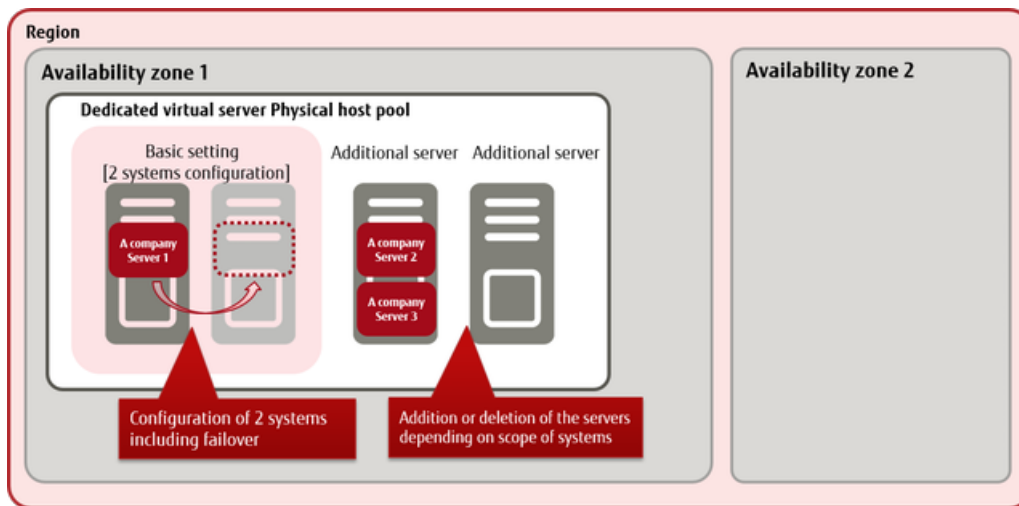
Figure 17: Using the Physical Host Pool Menu

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 are 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
    ・Remote Console Function
  ・OS Provision Service
  ・Software Support Service
  ・Auto-Scaling
  ・Image
  ・Virtual Server Import
  ・Virtual Server Export

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

How to Use This Service
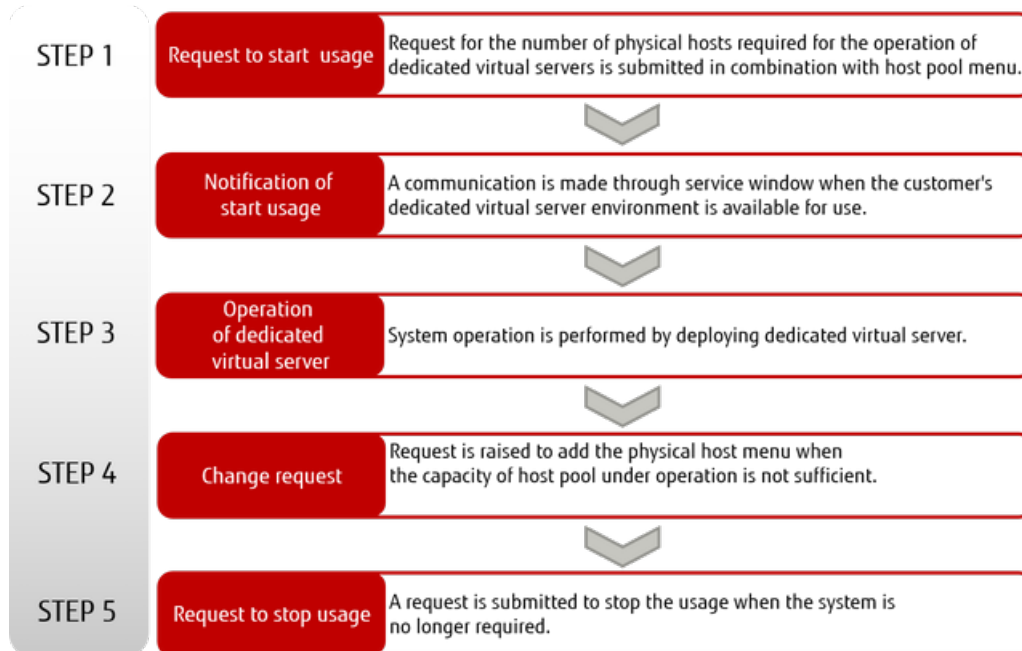
Figure 18: Procedure from Starting to Stopping a Dedicated Virtual Server

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, security is not guaranteed because the network is shared. 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 IaaS.

OS Provision Service

The service provides the following lineup of OSs for the virtual server. When you create the virtual server, select the OS image that you will use.

Table 11: OS Environment Provided

Type	OS Provided	Available Regions
		Japan East1 Japan East2 Japan West1 Japan West2
Windows Monthly Charging	Windows Server 2008 R2 SE SP1 64bit Japanese version	✓
	Windows Server 2008 R2 EE SP1 64bit Japanese version	✓
	Windows Server 2012 R2 SE 64bit Japanese Version	✓
	Windows Server 2012 SE 64bit Japanese Version	✓
	Windows Server 2016 SE 64bit Japanese Version	✓
	Windows Server 2008 R2 SE SP1 64bit English Version	✓
	Windows Server 2012 R2 SE 64bit English Version	✓
	Windows Server 2016 SE 64bit English Version	✓
Windows Metered Charging	Windows Server 2008 R2 SE SP1 64bit Japanese version	✓
	Windows Server 2012 R2 SE 64bit Japanese Version	✓
	Windows Server 2016 SE 64bit Japanese Version	✓
	Windows Server 2008 R2 SE SP1 64bit English Version	✓
	Windows Server 2012 R2 SE 64bit English Version	✓
	Windows Server 2016 SE 64bit English Version	✓
Linux	Red Hat Enterprise Linux 6.8 64bit (English)	✓
	Red Hat Enterprise Linux 6.9 64bit (English)	✓
	Red Hat Enterprise Linux 7.2 64bit (English)	✓
	Red Hat Enterprise Linux 7.2 AUS 64bit (English)	✓
	Red Hat Enterprise Linux 7.3 64bit (English)	✓
	Red Hat Enterprise Linux 7.4 64bit (English)	✓
	CentOS 6.8 64bit (English)	✓
	CentOS 6.9 64bit (English)	✓
	CentOS 7.2 64bit (English)	✓
	CentOS 7.3 64bit (English)	✓
	Ubuntu Server 14.04 LTS (English)	✓
	Ubuntu Server 16.04 LTS (English)	✓
	Red Hat OpenShift Container Platform 3.6 (Node)	✓
	Red Hat OpenShift Container Platform 3.6 (Master)	✓
	Red Hat OpenShift Container Platform 3.9 (Node)	✓
	Red Hat OpenShift Container Platform 3.9 (Master)	✓

It is not possible to switch deployed virtual servers between monthly charging and metered charging. When deploying a virtual server, select either an image with monthly charging or one with metered charging.

For OSs to which the password policies below apply, specify a password string that satisfies the relevant policies. Otherwise, even if you set up a password successfully, you will not be able to log in to the OS with that password.

- Windows Server passwords must meet the following complexity requirements:
  - At least six characters
  - Use at least one character from three or more of the following four categories:
    1. Uppercase alphabetic characters (A - Z)
    2. Lowercase alphabetic characters (a - z)
    3. Decimal numbers (0 - 9)
    4. Characters other than alphabetic characters (such as ! , $, #, %)
- The values of the items in the password policies of Windows 2016, Windows 2012, and Windows 2012 R2 in Table 11: OS Environment Provided have been changed from the default values to the following values.

<div align="center">Table 12: Details of Changes from Password Policy Default Values</div>

Policy	Details of Change from Default Value
Password length	At least 8 characters
Threshold value for account lockout	10 unsuccessful attempted logins
Reset of the lockout counter	30 minutes later
Lockout period	30 minutes

For the usage procedure for Red Hat OpenShift Container Platform, refer to the "IaaS Red Hat OpenShift Container Platform Startup Guide".

DNS Server Settings of the OS

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

Combinations of Virtual Server Type and OS That Cannot Be Used

The following combinations of virtual server type and OS cannot be used because they do not meet the operating requirements of the OS.

<div align="center">Table 13: List of Combinations of Virtual Server Types and OS That Are Inoperable</div>

OS type	OS Provided	Inoperable virtual server type
Windows	Windows Server 2008 R2 SE SP1 64bit Japanese version	P-1, P2-1
	Windows Server 2008 R2 EE SP1 64bit Japanese version	P-1, P2-1
	Windows Server 2012 R2 SE 64bit Japanese Version	P-1, P2-1

OS type	OS Provided	Inoperable virtual server type
	Windows Server 2012 SE 64bit Japanese Version	P-1, P2-1
	Windows Server 2016 SE 64bit Japanese Version	P-1, P2-1, T-1, T2-1
	Windows Server 2008 R2 SE SP1 64bit English Version	P-1, P2-1
	Windows Server 2012 R2 SE 64bit English Version	P-1, P2-1
	Windows Server 2016 SE 64bit English Version	P-1, P2-1, T-1, T2-1
Linux	Red Hat Enterprise Linux 6.x 64bit (English) (x is a number)	P-1, P2-1
	Red Hat Enterprise Linux 7.x 64bit (English) (x is a number)	P-1, P2-1
	CentOS 6.x 64bit (English) (x is a number)	P-1, P2-1
	CentOS 7.x 64bit (English) (x is a number)	P-1, P2-1
	Ubuntu Server 14.04 LTS (English)	None
	Ubuntu Server 16.04 LTS (English)	None
	Red Hat OpenShift Container Platform 3.6 (Node)	S-1, P-1, T-1, C-1, C-2, S2-1, P2-1, T2-1, C2-1, C2-2
	Red Hat OpenShift Container Platform 3.6 (Master)	S-1, S-2, M-1, P-1, T-1, C-1, C-2, C-4, LM-1, S2-1, S2-2, M2-1, P2-1, T2-1, C2-1, C2-2, C2-4, LM2-1
	Red Hat OpenShift Container Platform 3.9 (Node)	S-1, P-1, T-1, C-1, C-2, S2-1, P2-1, T2-1, C2-1, C2-2
	Red Hat OpenShift Container Platform 3.9 (Master)	S-1, P-1, T-1, C-1, C-2, S2-1, P2-1, T2-1, C2-1, C2-2

> **Note** Depending on the OS, the maximum number of sockets (number of CPUs) and the maximum memory size may be limited. Therefore, you may not be able to use the full CPU resources and memory of the OS, even if you select a virtual server type that can be operated on the OS.

Restrictions for Combinations of Virtual Server Type and OS

Because of the limitations of the OS, not all resources of the virtual server type can be used for the following combinations of virtual server type and OS.

Table 14: List of Virtual Server Type Combinations with Restrictions

OS Type	OS Provided	Restriction	Virtual Server Type
Windows	Windows Server 2008 R2 SE	The number of virtual CPUs that can be used is limited to 4	S-8, S-16, M-8, M-16, C-8, C-16, LM-8, L-12, L-24
			S2-8, S2-16, M2-8, M2-16, C2-8, C2-16, LM2-8, LM2-12, L2-24

OS Type	OS Provided	Restriction	Virtual Server Type
		The amount of memory that can be used is limited to 32 GB	S-16, M-16, XM-4, LM-4, LM-8, L-12, L-24
			S2-16, M2-16, XM2-4, LM2-4, LM2-8, L2-12, L2-24
	Windows Server 2008 R2 EE	The number of virtual CPUs that can be used is limited to 8	S-16, M-16, C-16, L-12, L-24
			S2-16, M2-16, C2-16, L2-12, L2-24

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

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 following network settings to connect to the repository where the virtual server provides patch files and updates:
> - Connection to external networks
> - Firewall
> - Security group settings

Settings for Activation Using Key Management Service (KMS)

For details on Windows Server activation using KMS, refer to "Batch Files for Windows KMS License Activation" at the following URL.

https://doc.cloud.global.fujitsu.com/en/iaas/index_en.html

Settings for Windows Server Update Services

For details on the WSUS settings for Windows Server, refer to Procedure for Connecting to the WSUS (Windows Server Update Services) Server.

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 15: List of RHUI Agent Modules by Version

Version	Name of Module Transferred
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 the virtual server
3. Use yum to perform update

Red Hat Satellite Server Settings

By using Red Hat OpenShift Container Platform, you have access to Red Hat Satellite, a service for patch distribution. For the usage procedure, refer to the "IaaS Red Hat OpenShift Container Platform Startup Guide".

Related concepts

Common Network Services

The following common network services are provided and available on virtual networks:

2.1.3.3 Japanese Language Settings for RHEL 6.x / CentOS 6.x

You can create an image of the English Linux OS provided by the service and use it in Japanese. Supported OS:

・Red Hat Enterprise Linux 6.x 64bit (English) (x is a number)

・CentOS 6.x 64bit (English) (x is a number)

Log in to the virtual server that you want to use in Japanese and configure the following settings:

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.UTF-8"
```

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.

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

2.1.3.4 Japanese Language Settings for RHEL 7.x / CentOS 7.x / RHOCP 3.x

You can create an image of the English Linux OS provided by the service and use it in Japanese. Supported OS:

・Red Hat Enterprise Linux 7.x 64bit (English) (x is a number)

・CentOS 7.x 64bit (English) (x is a number)

・Red Hat OpenShift Container Platform 3.x (English) (x is a number)

Log in to the virtual server that you want to use in Japanese and configure the following settings:

Time Zone Settings

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

1. Execute the following command:

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

2. To confirm that the command has been completed successfully, execute 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

1. Execute the following command:

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

2. To confirm that the command has been completed successfully, execute 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 16: Software Provision Service

Software	Version Provided	Available Regions
		Japan East1 Japan East2 Japan West1 Japan West2
Microsoft SQL Server	Microsoft SQL Server 2008 SE SP4 64bit Japanese Version	✓
	Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version	✓
	Microsoft SQL Server 2014 SE 64bit Japanese Version	✓
	Microsoft SQL Server 2014 EE 64bit Japanese Version	✓
	Microsoft SQL Server 2014 SE 64bit English Version	✓
	Microsoft SQL Server 2016 SE 64bit Japanese Version	✓
	Microsoft SQL Server 2016 SE 64bit English Version	✓

Combinations of Virtual Server Type and Software That Cannot Be Used

The following combinations of virtual server type and software cannot be used because they do not meet the operating requirements of the software.

Table 17: List of Combinations of Virtual Server Type and Software That Are Inoperable

Software	Version Provided	Inoperable virtual server type
Microsoft SQL Server	Microsoft SQL Server 2014 SE 64bit Japanese Version	P-1, P2-1
	Microsoft SQL Server 2014 EE 64bit Japanese Version	P-1, P2-1
	Microsoft SQL Server 2014 SE 64bit English Version	P-1, P2-1
	Microsoft SQL Server 2016 SE 64bit Japanese Version	P-1, P2-1
	Microsoft SQL Server 2016 SE 64bit English Version	P-1, P2-1

> **Note** Depending on the OS, the maximum number of sockets (number of CPUs) and the maximum memory size may be limited. Therefore, you may not be able to use the full CPU resources and memory of the OS, even if you select a virtual server type that can be operated on the OS.

Because of the specifications of the software, the number of virtual CPUs is limited to 4 for the virtual server types listed in the following table. Note that you cannot use the full virtual CPU resources depending on the virtual server type.

Table 18: Virtual Server Type with Limited Number of Virtual CPUs

Software	Version Provided	Virtual Server Type
Microsoft SQL Server	Microsoft SQL Server 2008 SE SP4 64bit Japanese Version	S-8, S-16, M-8, M-16, C-8, C-16, LM-8, L-12, L-24
	Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version	S2-8, S2-16, M2-8, M2-16, C2-8, C2-16, LM2-8, L2-12, L2-24
	Microsoft SQL Server 2014 SE 64bit Japanese Version	
	Microsoft SQL Server 2014 SE 64bit English Version	
	Microsoft SQL Server 2016 SE 64bit Japanese Version	
	Microsoft SQL Server 2016 SE 64bit English Version	

Required Number of Licenses

Table 19: List of Required Number of Licenses by Virtual Server Type

Software	Name of Virtual Server Type	Required Number of Licenses
Microsoft SQL Server	T-1 / T2-1	1
	C-1 / C2-1	1
	C-2 / C2-2	1
	C-4 / C2-4	1
	C-8 / C2-8	2
	C-16 / C2-16	4
	S-1 / S2-1	1
	S-2 / S2-2	1
	S-4 / S2-4	1
	S-8 / S2-8	2
	S-16 / S2-16	4
	M-1 / M2-1	1
	M-2 / M2-2	1
	M-4 / M2-4	1
	M-8 / M2-8	2

Software	Name of Virtual Server Type	Required Number of Licenses
	M-16 / M2-16	4
	XM-4 / XM2-4	1
	LM-1 / LM2-1	1
	LM-2 / LM2-2	1
	LM-4 / LM2-4	1
	LM-8 / LM2-8	2
	L-12 / L2-12	3
	L-24 / L2-24	6

How to Use This Service

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

Table 20: Software Provision Service, List of Images

Image Name	OS and Software
Windows Server 2008 R2 SE SP1 + SQL Server 2008 SE SP4 (Japanese)	OS: Windows Server 2008 R2 SE SP1 64bit Japanese version Software: Microsoft SQL Server 2008 SE SP4 64bit Japanese Version
Windows Server 2008 R2 SE SP1 + SQL Server 2008 R2 SE SP3 (Japanese)	OS: Windows Server 2008 R2 SE SP1 64bit Japanese version Software: Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version
Windows Server 2012 R2 SE + SQL Server 2014 SE (Japanese)	OS: Windows Server 2012 R2 SE 64bit Japanese Version Software: Microsoft SQL Server 2014 SE 64bit Japanese Version
Windows Server 2012 R2 SE + SQL Server 2014 EE (Japanese)	OS: Windows Server 2012 R2 SE 64bit Japanese Version Software: Microsoft SQL Server 2014 EE 64bit Japanese Version
Windows Server 2012 R2 SE + SQL Server 2014 SE (English)	OS: Windows Server 2012 R2 SE 64bit English Version Software: Microsoft SQL Server 2014 SE 64bit English Version
Windows Server 2016 SE + SQL Server 2016 SE (Japanese)	OS: Windows Server 2016 SE 64bit Japanese Version Software: Microsoft SQL Server 2016 SE 64bit Japanese Version
Windows Server 2016 SE + SQL Server 2016 SE (English)	OS: Windows Server 2016 SE 64bit English Version Software: Microsoft SQL Server 2016 SE 64bit English Version

> **Tip**　For OS password policies, refer to Table 12: Details of Changes from Password Policy Default Values.

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

Table 21: Software Provision Service Usage Guide

Software	Reference
Microsoft SQL Server	Microsoft SQL Server Usage Guide

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

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. Change these settings after the virtual server is created.

Software Whose Support Option You Can Change

・OS Provision Service

Table 22: OS that Allow Changes to Support Options

Type	OS Provided	Available Regions Japan East1 Japan East2 Japan West1 Japan West2
Windows Monthly Charging	Windows Server 2008 R2 SE SP1 64bit Japanese version	✓
	Windows Server 2008 R2 EE SP1 64bit Japanese Version	✓
	Windows Server 2012 R2 SE 64bit Japanese Version	✓
	Windows Server 2012 SE 64bit Japanese Version	✓
	Windows Server 2016 SE 64bit Japanese Version	✓
Linux	Red Hat Enterprise Linux 6.x 64bit English Version (x is a number)	✓
	Red Hat Enterprise Linux 7.x 64bit English Version (x is a number)	✓

・Software Provision Service

Table 23: Software that Allows Changes to Support Options

Software	Version Provided	Available Regions Japan East1 Japan East2 Japan West1 Japan West2
Microsoft SQL Server	Microsoft SQL Server 2008 SE SP4 64bit Japanese Version	✓
	Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version	✓
	Microsoft SQL Server 2014 SE 64bit Japanese Version	✓
	Microsoft SQL Server 2014 EE 64bit Japanese Version	✓
	Microsoft SQL Server 2016 SE 64bit Japanese Version	✓
Interstage Application Server	Interstage Application Server Standard-J Edition V11	✓
Symfoware Server	Symfoware Server Lite Edition V12	✓
Systemwalker Operation Manager	Systemwalker Operation Manager Standard Edition V13	✓
Systemwalker Centric Manager	Systemwalker Centric Manager Standard Edition (for Managers) V15	✓
	Systemwalker Centric Manager Standard Edition (for Agents) V15	✓

Functions Included

・Support Option Change Function

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

Table 24: System Default Support Level Overview (OS that Allow Changes to Support Options)

OS	Default Support Level
Windows Server 2008 R2 SE SP1 64bit Japanese Version	No support
Windows Server 2008 R2 EE SP1 64bit Japanese Version	No support
Windows Server 2012 R2 SE 64bit Japanese Version	No support
Windows Server 2012 SE 64bit Japanese Version	No support
Windows Server 2016 SE 64bit Japanese Version	No support
Red Hat Enterprise Linux 6.x 64bit English Version (x is a number)	Limited Support
Red Hat Enterprise Linux 7.x 64bit English Version (x is a number)	Limited Support

Table 25: System Default Support Level Overview (
Software that Allows Changes to Support Options)

Software	Default Support Level
Microsoft SQL Server 2008 SE SP4 64bit Japanese Version	No support
Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version	No support
Microsoft SQL Server 2014 SE 64bit Japanese Version	No support
Microsoft SQL Server 2014 EE 64bit Japanese Version	No support
Microsoft SQL Server 2016 SE 64bit Japanese Version	No support
Interstage Application Server Standard-J Edition V11	24-hour support
Symfoware Server Lite Edition V12	24-hour support
Systemwalker Operation Manager Standard Edition V13	24-hour support
Systemwalker Centric Manager Standard Edition (for Managers) V15	24-hour support
Systemwalker Centric Manager Standard Edition (for Agents) V15	24-hour support

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

> **Tip** You can change the support level to any of the different support levels provided for the same software.

Table 26: Changing Support Options, List of Support Levels (OS)

OS	Support Levels that Allow Changes
Windows Server 2008 R2 SE SP1 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Windows Server 2008 R2 EE SP1 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Windows Server 2012 R2 SE 64bit Japanese	• No support • Support on weekdays • 24-hour support
Windows Server 2012 SE 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Windows Server 2016 SE 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Red Hat Enterprise Linux 6.x 64bit English Version (x is a number)	• Limited Support • Support on weekdays • 24-hour support

OS	Support Levels that Allow Changes
Red Hat Enterprise Linux 7.x 64bit English Version (x is a number)	• Limited Support • Support on weekdays • 24-hour support

Table 27: Changing Support Options, List of Support Levels (Software)

Software	Support Levels that Allow Changes
Microsoft SQL Server 2008 SE SP4 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Microsoft SQL Server 2014 SE 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Microsoft SQL Server 2014 EE 64bit Japanese Version	• No support • 24-hour support
Microsoft SQL Server 2016 SE 64bit Japanese Version	• No support • Support on weekdays • 24-hour support
Interstage Application Server Standard-J Edition V11	• 24-hour support
Symfoware Server Lite Edition V12	• 24-hour support
Systemwalker Operation Manager Standard Edition V13	• 24-hour support
Systemwalker Centric Manager Standard Edition (for Managers) V15	• 24-hour support
Systemwalker Centric Manager Standard Edition (for Agents) V15	• 24-hour 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 level 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 level 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 level.

> **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.
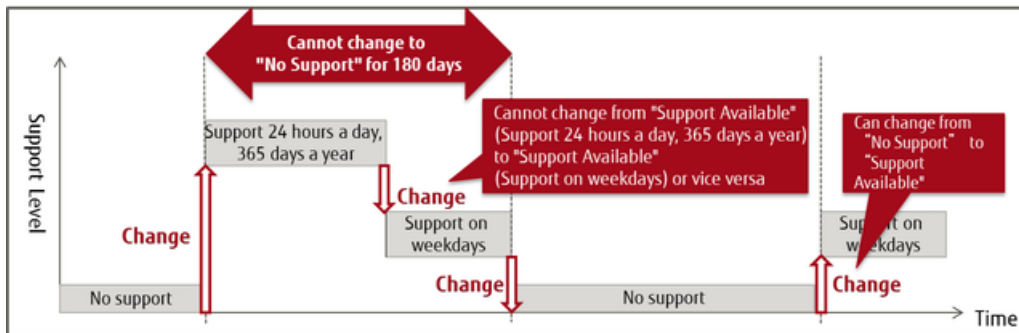
Related concepts
List of Software Support Service IDs

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.
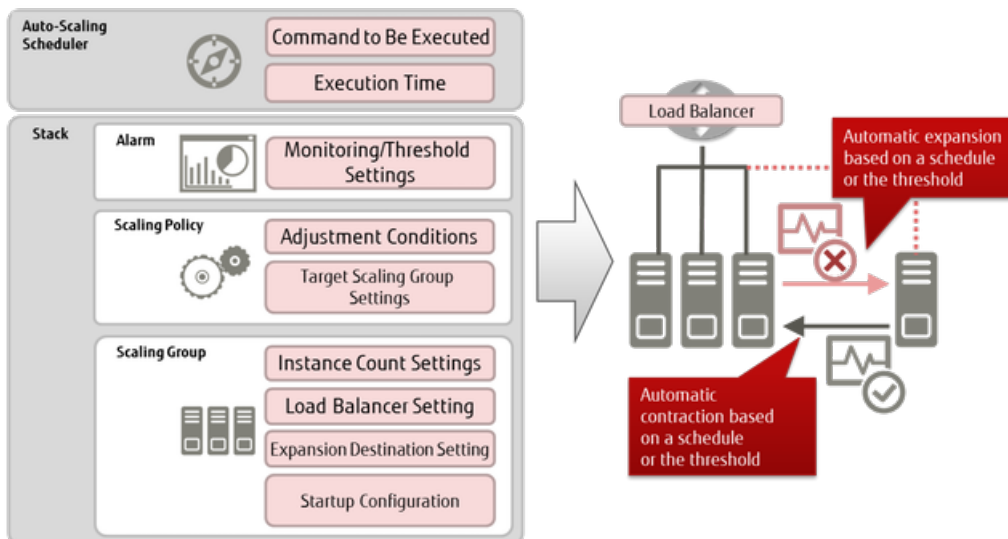
Figure 19: Overview of Auto-Scaling

> **Note** It is not possible to use auto-scaling between multiple availability zones.

> **Note** When a stack created using a template is updated, resources that have already been deployed are deleted and then rebuilt.

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 28: 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 starting 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
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 29: 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 starting 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.

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

Table 30: 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 settings so that the device will be attached as block storage 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

Example of 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
    default: 1234abcd-5678-ef90-9876-fedc5432dcba
  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
```

Related concepts

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.

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

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.

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
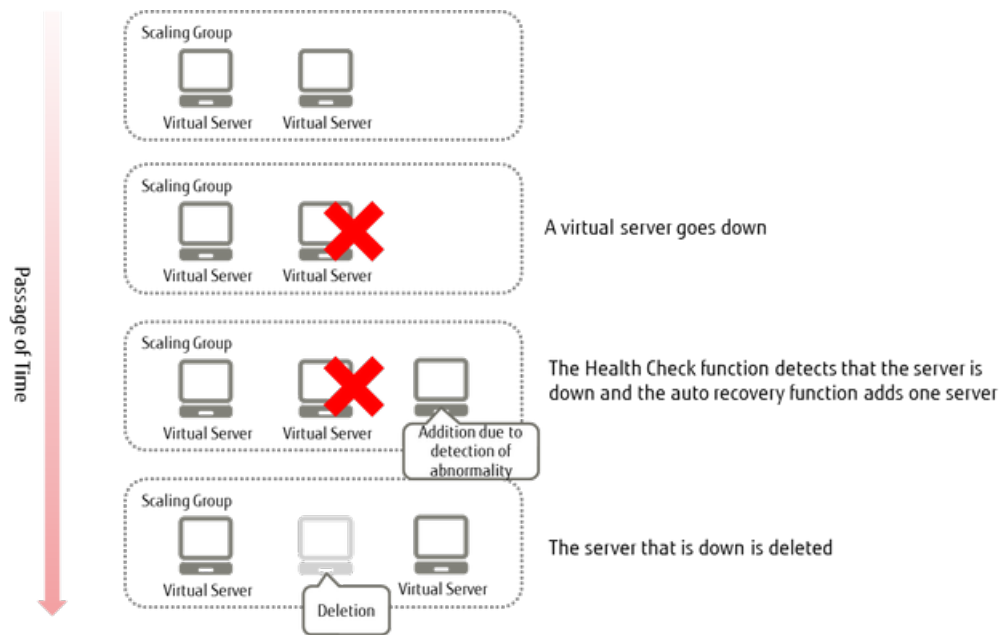
Figure 20: Operation of the Auto Recovery Function on a Virtual Server Where Abnormality Was Detected by the Health Check Function

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 31: 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 starting immediately after the previous scaling operation was completed (Formula for Estimating Cool Down Period after Auto-Scaling) **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 servers is not carried out, and only the deletion of virtual servers is carried out.	Yes

Item	Description	Required
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 32: 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 starting immediately after the previous scaling operation was completed (Formula for Estimating Cool Down Period after Auto-Scaling)	
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 33: 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 • "ne": Not equal	

Item	Description	Required
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 specified value.	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 34: 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 35: 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

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

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.
>
> Also, do not start the target virtual server until creation of an image has been completed. If you start the target virtual server while the image is being created, the content of the volume may be updated.

> **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**
>
> If there is a chance that the disk configuration has been changed between when a snapshot was created and when restoration is being performed, delete all volume information from the disk settings on the OS (for Linux, the /etc/fstab file, etc.), and then create a new snapshot. When there is unnecessary volume information remaining, starting of the OS may fail after restoration is performed.

> ⚠️ **Warning**
> Perform the following steps before creating an image of a virtual server whose OS is CentOS 6.x, Ubuntu, or Red Hat Enterprise Linux 6.x (x is a number). 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 38: 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 39: 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 an 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

How to Use This Service
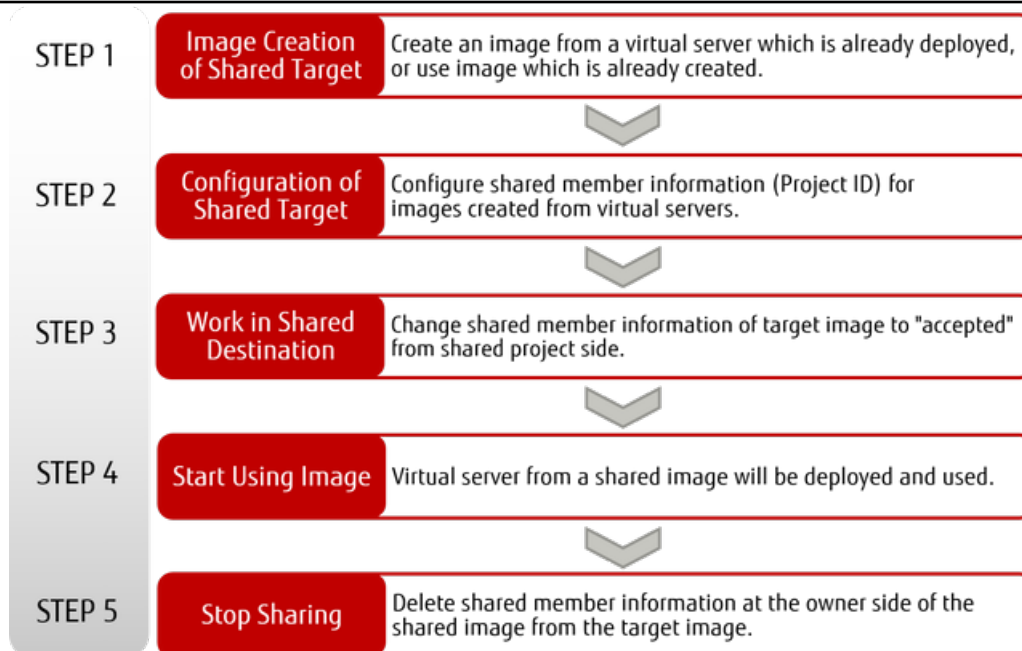
Figure 21: Procedure from Starting to Stopping the Sharing of a Virtual Server Image

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.

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 2016 SE / 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 2008 SE/EE

  From the Start menu, click [Control Panel] > [System and Security] > [Allow remote access], and then select one of the following in the dialog box:

  - [Allow connections from computers running any version of Remote Desktop (less secure) (L)]
  - [Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)(N)]

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 2016 SE

  C:\Windows\System32\Sysprep\ans_w2k16.xml

- For Windows 2012 SE

  C:\Windows\System32\Sysprep\ans_w2k12.xml

- For Windows 2008 SE

  C:\Windows\System32\Sysprep\ans_w2k8_se.xml

- For Windows 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 2016 SE / 2012 SE

     On the desktop screen, right-click the [Windows] logo button and click [Command Prompt (Admin)].
   - For Windows 2008 SE/EE
     a. Click the [Start] button.
     b. Click [All Programs] > [Accessories].
     c. 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
   ```

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

2.1.8.1 Overview of Functions

2.1.8.1.1 What is Virtual Server Import?

This function is used to migrate a virtual server running on your on-premises virtual environment to IaaS. This function allows you to register image files that you have captured as image files that can be used in IaaS.
The diagram below shows how this function is used.
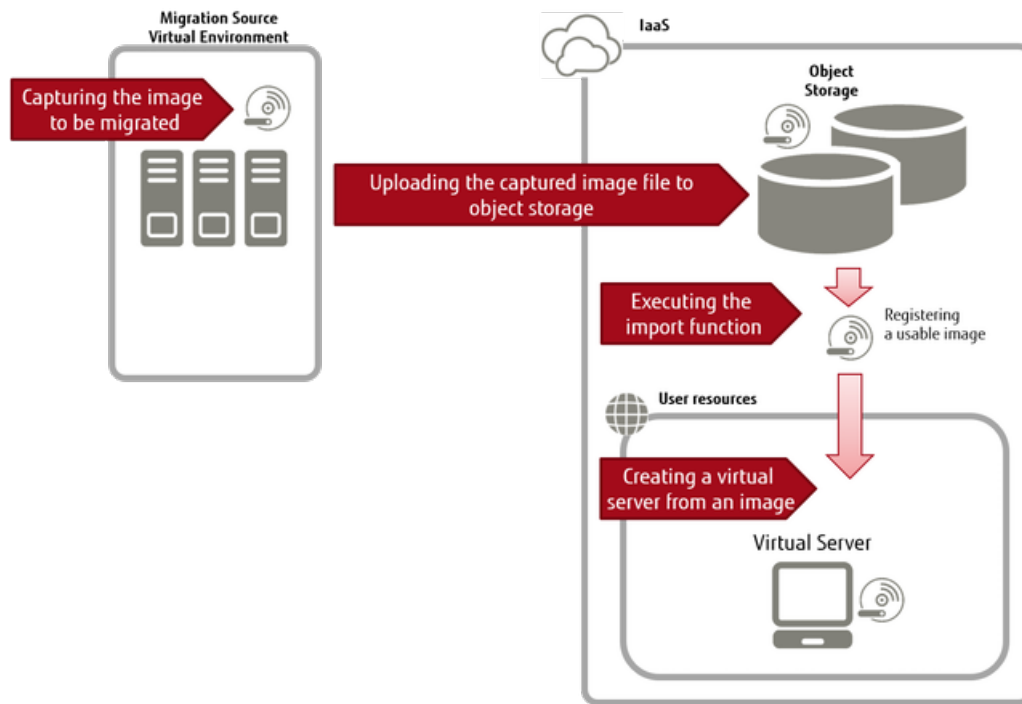
Figure 22: Using Virtual Server Import

Supported Migration Source Virtual Environments

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

Table 40: 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.

Migration Source Guest OS Types that Can Be Imported

A list of migration source guest OS types that can be imported is shown below.

> **Note**
> Appliance products are not supported.

Table 41: List of Migration Source Guest OS

---

[1] Hypervisors are supported for VMware only.

OS Type	Supported OS
Windows	• Windows 2008 R2 SE 64bit (Japanese Version, English Version) • Windows 2008 R2 EE 64bit (Japanese Version, English Version) • Windows 2012 SE 64bit (Japanese Version, English Version) • Windows 2012 R2 SE 64bit (Japanese Version, English Version) • Windows 2016 SE 64bit (Japanese Version, English Version)
Linux	• CentOS 6.5, 6.6, 6.7, 6.8 64bit • CentOS 7.1, 7.2 64bit • RHEL6 64bit • RHEL7 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.

In addition, no support is provided for any of the following:

- Dynamic disk (if the OS type is Windows)
- Formats other than NTFS/FAT32 (if the OS type is Windows)
- Disks encrypted with BitLocker (if the OS type is Windows)
- A Windows system of which the Windows folder has been renamed to anything other than the default 'Windows' (if the OS type is Windows)
- Volumes with the "NODEFAULTDRIVELETTER" attribute enabled (if the OS type is Windows)
- GPT format disks
- Multi-boot environments

• Network Interface

One network interface must be defined.

• Sysprep

When duplicating virtual servers, if the OS is Windows, do so using Sysprep on the migration source virtual environment or on the virtual server after import. For how to use Sysprep and response files, refer to Microsoft technical support.

> **Note**
> When executing Sysprep and importing an image on which Sysprep will be used when the OS starts, note the following points.
>
> - For Sysprep, only use OOBE (Out-of-box Experience) mode with generalized settings. At that time, prepare a response file.
> - In cases other than the above, the system wizard window is displayed the first time the server is started which means that the system wizard window cannot be operated as remote desktop connections are not possible.
> - When creating a virtual server using an imported image, the values for the following items in the response file will not be applied.
>   - Administrator password: The password specified using the portal or the API will used
>   - Machine name: The name configured in the system will be used

Handling of Licenses

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

Table 42: 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	• Red Hat Enterprise Linux Before importing the OS image, you need to register Cloud Access. For a virtual server that is created from an image that was imported, assign the Cloud Access from Red Hat or Fujitsu for the subscription that you have purchased. For IaaS, no charges apply. Your [Corporate Name], [Mail Address], and [Number of Virtual Servers Created from an Imported RHEL Image] will be reported to Red Hat on a monthly basis. Refer to the following URL for details about Cloud Access: https://www.redhat.com/en/technologies/cloud-computing/cloud-access **Note** • You cannot use RHUI provided by common network services. Do not install RHUI Agent. • You cannot receive IaaS software support service. Support service for your OS is provided from the source where you purchased your subscription. • To cancel your subscription to Cloud Access, contact Red Hat. • CentOS No license required. • Ubuntu No license required.

Tip Specify the following information when subscribing to Cloud Access.

Table 43: Settings Required to Specify for Cloud Access Subscription

Cloud Provider	FUJITSU Cloud Service for OSS
Cloud Provider Account Number	Contract number for FUJITSU Cloud Service for OSS
Product Name	Subscription name to be used for the RHEL that you intend to migrate
Quantity	Subscription types (not the number of cloud accounts assigned) to be used for the RHEL that you intend to migrate

How to Use This Service

Perform the following operations to import the image on the migration source virtual server to IaaS.
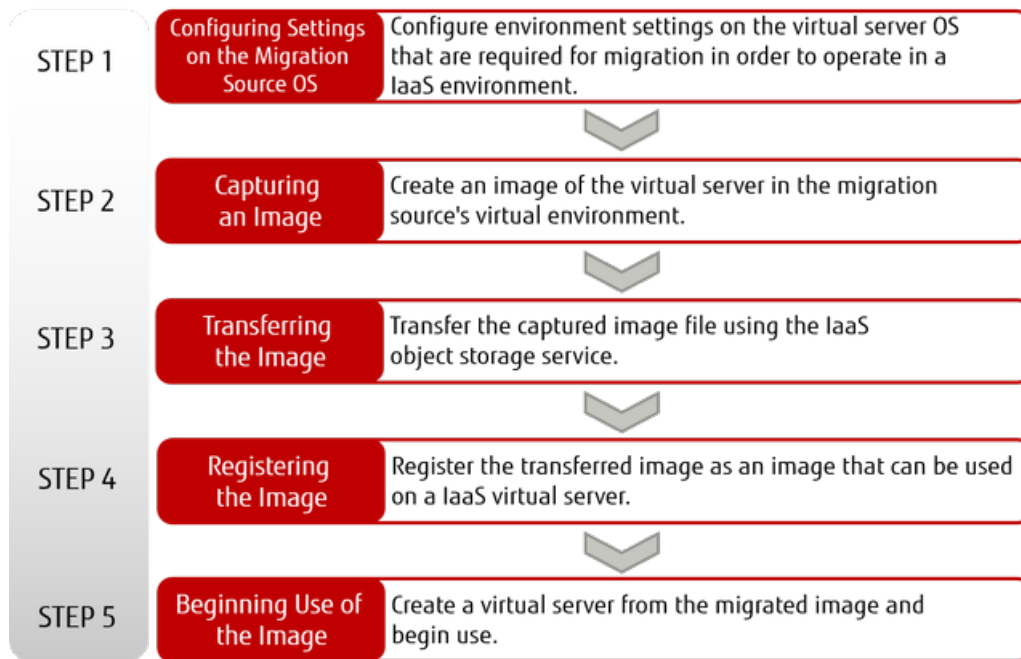
Figure 23: How to Use Virtual Server Import

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 IaaS environment when the OS of the virtual server that is operating in the virtual environment is Windows Server.

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

・Windows 2008 R2

・Windows 2012

・Windows 2012 R2

・Windows 2016

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. 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.

2. Uninstalling Cloudbase-Init
   If Cloudbase-Init is installed on the virtual server that you intend to migrate, uninstall it.

3. Shutting down the OS

Shut down the OS.

2.1.8.2.2 Migrating an Image of CentOS 6

The following explains the steps required for migrating an image to a IaaS environment when the OS of the virtual server that is operating in the migration source virtual environment is CentOS 6.

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

> **Important**
> - Each of the following procedures provides an example of the command operation. The operation method may vary slightly, depending on the user's environment. Perform each operation according to the user's environment at the responsibility and decision of the user.
> - 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.

   a. Obtaining cloud-init

      Obtain the cloud-init module provided by FUJITSU from the service desk. Use the latest package that is provided.

   b. Installation of cloud-init

      ```
      # yum install
      http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
      # yum -y install /var/tmp/cloud-init-0.7.5-10.el7.FJ.20160406.noarch.rpm
      cloud-utils-growpart
      # yum -y install dracut-modules-growroot
      ```

      > **Tip**
      > Replace the name of the storage destination of the cloud-init module and the file name with the names that are in use in your environment.

   c. Checking of cloud-init

      Check if cloud-init provided by Fujitsu is installed successfully.

      ```
      # rpm -qi cloud-init
      ```

      The following shows a display example that appears when cloud-init provided by Fujitsu is installed successfully.

      ```
      # rpm -qi cloud-init
      Name        : cloud-init          Relocations: (not relocatable)
      Version     : 0.7.5                    Vendor: FUJITSU LIMITED
      ```

```
            <--omitted-->
Packager    : FUJITSU LIMITED
            <--omitted-->
```

If cloud-init provided by Fujitsu is not installed, reinstall it, and then check whether the installation was successful.

```
# rpm -e cloud-init
# rpm -q cloud-init
# rm -rf /var/lib/cloud
# rpm -ivh /var/tmp/cloud-init-0.7.5-10.el7.FJ.20160406.noarch.rpm
# rpm -q cloud-init
```

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.

a. Save /boot/grub.grub.conf.

```
# cp -p /boot/grub/grub.conf /root/grub.conf.bak
```

b. 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.

a. Check the setting of /etc/sysconfig/network-scripts/ifcfg-<network interface name>.

```
ONBOOT=yes
BOOTPROTO=dhcp
```

Delete the following lines if they exist.

```
IPADDR=10.4.0.110
PREFIX=22
GATEWAY=10.4.0.220
```

* The above values are examples.

b. Restart the network.

```
# service network restart
```

6. Disabling Zeroconf

Disable Zeroconf so that the migrated virtual machine can acquire metadata.

```
# vi /etc/sysconfig/network
```

Add the following line.

```
NOZEROCONF=yes
```

* Delete the following line if it exists. The value is an example.

```
GATEWAY=10.4.0.220
```

7. Deletion of the MAC address

a. Save the configuration file.

If no configuration file exists, proceed to step 8.

```
# 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
```

b. 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
```

c. Delete the MAC address information (the line that starts with "HWADDR=") from /etc/sysconfig/network-scripts/ifcfg-<network interface name>.

d. Restart the OS.

* After the OS restarts, it may take several minutes until the login prompt appears.

```
# reboot
```

8. Disabling of the firewall

Disable the iptables service and the ipchains service.

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

9. Configuring cloud.cfg

Configure the settings of /etc/cloud/cloud.cfg.

Configure the operational settings of cloud-init in /etc/cloud/cloud.cfg. For details on the settings, refer to the support site of cloud-init.

10. Shutting down the OS

Shut down the OS.

```
# shutdown -h now
```

2.1.8.2.3 Migrating an Image of RHEL6 OS

The following explains the steps required for migrating an image to a IaaS environment when the OS of the virtual server that is operating in the migration source virtual environment is RHEL6.

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

> **Important**
> - Each of the following procedures provides an example of the command operation. The operation method may vary slightly, depending on the user's environment. Perform each operation according to the user's environment at the responsibility and decision of the user.
> - 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. Setting of the output destination of the boot log

Change the GRUB setting so that the Kernel can write the boot logs to the ttyS0 device.

a. Save /boot/grub/grub.conf.

```
# cp -p /boot/grub/grub.conf /boot/grub/grub.conf.bak
```

b. Edit /boot/grub/grub.conf and add the definition that enables the Kernel to write boot logs to the ttyS0 device.

```
# vi /boot/grub/grub.conf
```

Delete "rhgb quiet," and add "console=tty0 console=ttyS0,115200" as follows:

```
(Before) kernel /vmlinuz<string omitted> rhgb quiet
(After the change) kernel /vmlinuz<string omitted> console=tty0 console=ttyS0,115200n
```

Add or change the end to the following:

```
serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1
terminal --timeout=5 serial console
```

c. Restart the OS.

```
# reboot
```

3. Deletion of the MAC address

   Delete the udev rule file information and the MAC address information in the network interface settings file so that the settings for the network interface are set correctly for the virtual machine whose MAC address has been changed after migration.

   a. Save the definition file. If no definition file exists, this operation is not required.

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

   b. Replace the definition file with an empty file.

   ```
   # 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
   ```

   c. Delete the line with "HWADDR=" (the MAC address information) from /etc/sysconfig/network-scripts/ifcfg-<network interface name>.

   d. Restart the OS.

   ```
   # reboot
   ```

4. Assigning a subscription

   If you have not assigned a subscription to a virtual server, do the following:

   a. Register the server to the subscription service.

   After you have run the following command, enter the user name and password of your Red Hat account, then register the system to the subscription service.

   ```
   # subscription-manager register
   ```

   b. Check for a subscription that can be assigned.

   Check for a subscription that can be assigned which has been registered to the subscription service. After running the command shown below, take a note of the Pool ID of the subscription to be assigned.

   ```
   # subscription-manager list --available | less
   ```

   c. Assign a subscription.

   Specify the Pool ID that you took a note of in step 2, and assign a subscription to the virtual server.

   ```
   # subscription-manager subscribe --pool=<Pool ID>
   ```

5. Installation of an SSH server

   Install an SSH server by following the procedure below.

   ```
   # yum -y install openssh-server
   # chkconfig sshd on
   # service sshd start
   ```

   > Configure the SSH service settings as necessary.
   >
   > Tip

6. Installation of cloud-init

   Install cloud-init.

   ```
   # yum -y install cloud-init --enablerepo=rhel-6-server-rh-common-rpms
   ```

7. Unregistration of the subscription service

Unregister the system from the subscription service.

```
# subscription-manager unregister
```

8. Configuring cloud.cfg

Configure the settings of /etc/cloud/cloud.cfg.

Configure the operational settings of cloud-init in /etc/cloud/cloud.cfg. For details on the settings, refer to the support site of cloud-init.

9. 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.

a. Check the setting of /etc/sysconfig/network-scripts/ifcfg-<network interface name>.

```
ONBOOT=yes
BOOTPROTO=dhcp
```

Delete the following lines if they exist.

```
IPADDR=10.4.0.110
PREFIX=22
GATEWAY=10.4.0.220
```

* The above values are examples.

b. Restart the network.

```
# service network restart
```

10. Disabling Zeroconf

Disable Zeroconf so that the migrated virtual machine can acquire metadata.

```
# vi /etc/sysconfig/network
```

Add the following line.

```
NOZEROCONF=yes
```

* Delete the following line if it exists. The value is an example.

```
GATEWAY=10.4.0.220
```

11. Disabling of the firewall

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

12. Shutting down the OS

Shut down the OS.

```
# shutdown -h now
```

2.1.8.2.4 Migrating an Image of CentOS 7

The following explains the steps required for migrating an image to a IaaS environment when the OS of the virtual server that is operating in the migration source virtual environment is CentOS 7.

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

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. Installing cloud-init

   Install cloud-init by following the procedure below.

   a. Obtaining cloud-init

      Obtain the cloud-init module provided by FUJITSU from the service desk. Use the latest package that is provided.

   b. Installing cloud-init

      ```
      # yum -y install --enablerepo=* --disablerepo=c7-media
       /var/tmp/cloud-init-0.7.5-10.el7.FJ.20160406.noarch.rpm cloud-utils
      ```

      > **Tip**
      > Replace the name of the storage destination of the cloud-init module and the file name with the names that are in use in your environment.

   c. Checking of cloud-init

      Check if cloud-init provided by Fujitsu is installed successfully.

      ```
      # rpm -qi cloud-init
      ```

      The following shows a display example that appears when cloud-init provided by Fujitsu is installed successfully.

      ```
      # rpm -qi cloud-init
      Name        : cloud-init
               <--omitted-->
      Packager    : FUJITSU LIMITED
      Vendor      : FUJITSU LIMITED
               <--omitted-->
      ```

      If cloud-init provided by Fujitsu is not installed, reinstall it, and then check whether the installation was successful.

      ```
      # rpm -e cloud-init
      # rpm -q cloud-init
      # rm -rf /var/lib/cloud
      # rpm -ivh /var/tmp/cloud-init-0.7.5-10.el7.FJ.20160406.noarch.rpm
      # rpm -qi cloud-init
      ```

3. 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.

   a. Save /etc/default/grub.

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

   b. Edit /etc/default/grub and add the definition that enables the Kernel to write boot logs to the ttyS0 device to grub.

```
# vi /etc/default/grub
```

Append or change the definition as shown below:

```
GRUB_TERMINAL="serial console"
GRUB_CMDLINE_LINUX_DEFAULT="console=ttyS0"
GRUB_SAVEDEFAULT=true
GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1"
```

Change the value of GRUB_CMDLINE_LINUX as follows.

```
Before: GRUB_CMDLINE_LINUX="crashkernel=auto rhgb quiet"
After: GRUB_CMDLINE_LINUX="crashkernel=auto console=tty0 console=ttyS0,115200"
```

   c. Apply the changes to /boot/grub2/grub.cfg.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. 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.

   a. Enable NetworkManager.

```
# yum -y install NetworkManager
# systemctl enable NetworkManager
# systemctl start NetworkManager
```

   b. Modify the setting of /etc/sysconfig/network-scripts/ifcfg-*<network interface name>* as follows.

```
ONBOOT=yes
BOOTPROTO=dhcp
```

   c. Restart the network.

```
# systemctl restart NetworkManager
```

5. Changing the network interface name

   a. Copy the network interface configuration from /etc/sysconfig/network-scripts/ifcfg-*<network interface name>*.

```
# cd /etc/sysconfig/network-scripts
# cp ifcfg-eno16780032 ifcfg-eth0
```

   * The source file name (ifcfg-eno16780032) is an example and varies depending on the environment.

   b. Change the configuration name and the device name in the network interface configuration that you duplicated.

   Change the values in Ifcfg-eth0 to "NAME=eth0" and "DEVICE=eth0."

   * You can also write them in the format of "NAME="eth0"" and "DEVICE="eth0"."

   c. Edit /etc/default/grub.

```
# vi /etc/default/grub
```

   Change the value of GRUB_CMDLINE_LINUX as follows.

```
Before: GRUB_CMDLINE_LINUX="crashkernel=auto console=tty0 console=ttyS0,115200"
After: GRUB_CMDLINE_LINUX="crashkernel=auto console=tty0 console=ttyS0,115200
 net.ifnames=0"
```

   d. Apply the changes in /etc/default/grub to /boot/grub2/grub.cfg.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Deletion of the MAC address

   a. Delete the information specific to the network interface from /etc/sysconfig/network-scripts/ifcfg-eth0.

   Delete the lines with "UUID=" and "HWADDR=."

   b. Restart the OS.

```
# reboot
```

7. Disabling Zeroconf

   Disable Zeroconf so that the migrated virtual machine can acquire metadata.

   ```
   # vi /etc/sysconfig/network
   ```

   Add the following line.

   ```
   NOZEROCONF=yes
   ```

8. Disabling of the firewall

   ```
   # systemctl stop firewalld
   # systemctl disable firewalld
   ```

9. Enabling of the virtio driver

   Replace initramfs with the one in which the virtio driver required for the OS start after the migration is embedded.

   a. Make a backup of initramfs.

      ```
      # cd /boot
      # mv initramfs-3.10.0-327.el7.x86_64.img initramfs-3.10.0-327.el7.x86_64.img.bak
      ```

      * The above file name "initramfs-3.10.0-327.el7.x86_64.img" is an example.

   b. Create initramfs in which the virtio driver is embedded.

      ```
      # dracut --add-drivers 'virtio virtio_ring virtio_blk virtio_net virtio_pci'
      ```

   c. Make sure that initramfs was created successfully.

      ```
      # ls -l initramfs-3.10.0-327.el7.x86_64.img
      ```

10. Configuring cloud.cfg

    Configure the settings of /etc/cloud/cloud.cfg.

    Configure the operational settings of cloud-init in /etc/cloud/cloud.cfg. For details on the settings, refer to the support site of cloud-init.

11. Shutting down the OS

    Shut down the OS.

    ```
    # shutdown -h now
    ```

2.1.8.2.5 Migrating an Image of RHEL7 OS

The following explains the steps required for migrating an image to a IaaS environment when the OS of the virtual server that is operating in the migration source virtual environment is RHEL7.

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

> ⚠ Important
>
> - Each of the following procedures provides an example of the command operation. The operation method may vary slightly, depending on the user's environment. Perform each operation according to the user's environment at the responsibility and decision of the user.
> - 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. Enabling NetworkManager

Enable NetworkManager.

```
# systemctl enable NetworkManager
# systemctl start NetworkManager
```

3. Changing the network interface name

Change the name of the network interface so that the settings for the network are set correctly in the environment after migration.

a. Save /etc/default/grub.

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

b. Edit /etc/default/grub.

```
# vi /etc/default/grub
```

Change the value of Add GRUB_CMDLINE_LINUX as follows.

```
Before: GRUB_CMDLINE_LINUX="crashkernel=auto rhgb quiet"
After: GRUB_CMDLINE_LINUX="crashkernel=auto rhgb quiet net.ifnames=0 biosdevname=0"
```

c. Apply the changes to /boot/grub2/grub.cfg.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

d. Restart the OS.

```
# reboot
```

e. Check that the network interface "eth0" is displayed.

```
# ip addr show
```

f. Save the settings file for the network interface.

```
# cp -p /etc/sysconfig/network-scripts/ifcfg-eno16780032
/etc/sysconfig/network-scripts/org.ifcfg-eno16780032
```

* The file name (ifcfg-eno16780032) above is an example.

* Place "org." at the beginning of a file name to be saved.

g. Change the file name of the settings file for the network interface.

```
# mv /etc/sysconfig/network-scripts/ifcfg-eno16780032
/etc/sysconfig/network-scripts/ifcfg-eth0
```

h. Edit the settings file for the network interface.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Change it as follows:

```
NAME=eth0
DEVICE=eth0
```

Delete the following line if it exists.

```
HWADDR=00:0c:29:e6:f2:e9
```

* The above values are examples.

i. Restart the OS.

```
# reboot
```

j. Check that the changes are applied to the network interface "eth0."

```
# ip addr show
```

4. Setting of the output destination of the boot log

Change the GRUB setting so that the Kernel can write the boot logs to the ttyS0 device.

a. Edit /etc/default/grub.

```
# vi /etc/default/grub
```

Delete "rhgb quiet" from "GRUB_CMDLINE_LINUX," and add "console=tty0 console=ttyS0,115200."

```
Before: GRUB_CMDLINE_LINUX="crashkernel=auto rhgb quiet net.ifnames=0 biosdevname=0"
After: GRUB_CMDLINE_LINUX="crashkernel=auto console=tty0 console=ttyS0,115200
 net.ifnames=0 biosdevname=0"
```

Append or change the definition as shown below:

```
GRUB_TERMINAL="serial console"
GRUB_CMDLINE_LINUX_DEFAULT="console=ttyS0 modprobe.blacklist=floppy"
GRUB_SAVEDEFAULT=true
GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1"
```

b. Apply the changes in /etc/default/grub to /boot/grub2/grub.cfg.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

c. Restart the OS.

```
# reboot
```

5. Assigning a Subscription

If you have not assigned a subscription to a virtual server, do the following:

a. Register the server to the subscription service.

After you have run the following command, enter the user name and password of your Red Hat account, then register the system to the subscription service.

```
# subscription-manager register
```

b. Check for a subscription that can be assigned.

Check for a subscription that can be assigned which has been registered to the subscription service. After running the command shown below, take a note of the Pool ID of the subscription to be assigned.

```
# subscription-manager list --available | less
```

c. Assign a subscription.

Specify the Pool ID that you took a note of in step 2, and assign a subscription to the virtual server.

```
# subscription-manager subscribe --pool=<Pool ID>
```

6. Installation of an SSH server

Install an SSH server by following the procedure below.

```
# yum -y install openssh-server
# systemctl enable sshd.service
# systemctl start sshd.service
```

> **Tip** Configure the SSH service settings as necessary.

7. Installation of cloud-init

Install cloud-init.

```
# yum -y install cloud-init --enablerepo=rhel-7-server-rh-common-rpms
```

8. Unregistration of the subscription service

Unregister the system from the subscription service.

```
# subscription-manager unregister
```

9. Configuring cloud.cfg

Configure the settings of /etc/cloud/cloud.cfg.

Configure the operational settings of cloud-init in /etc/cloud/cloud.cfg. For details on the settings, refer to the support site of cloud-init.

10. 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.

a. Change the network setting to DHCP.

```
# nmcli connection modify eth0 ipv4.method auto
# nmcli connection modify eth0 ipv4.addresses "" ipv4.gateway ""
```

b. Restart the network interface.
```
# nmcli connection down eth0
# nmcli connection up eth0
```

c. Check that the network setting is applied to "eth0."
```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
```

Check the following:
- "BOOTPROTO=dhcp" is set
- "IPADDR=" does not exist
- "PREFIX=" does not exist
- "GATEWAY=" does not exist

11. Enabling of the virtio driver

Replace initramfs with the one in which the virtio driver required for the OS start after the migration is embedded.

a. Make a backup of initramfs.
```
# cd /boot
# mv initramfs-3.10.0-327.el7.x86_64.img initramfs-3.10.0-327.el7.x86_64.img.bak
```

* The above file name "initramfs-3.10.0-327.el7.x86_64.img" is an example.

b. Create initramfs in which the virtio driver is embedded.
```
# dracut --add-drivers 'virtio virtio_ring virtio_blk virtio_net virtio_pci'
```

c. Make sure that initramfs was created successfully.
```
# ls -l initramfs-3.10.0-327.el7.x86_64.img
```

12. Disabling Zeroconf

Disable Zeroconf so that the migrated virtual machine can acquire metadata.
```
# vi /etc/sysconfig/network
```

Add the following line.
```
NOZEROCONF=yes
```

13. Disabling of the firewall
```
# systemctl stop firewalld
# systemctl disable firewalld
```

14. Shutting down the OS

Shut down the OS.
```
# shutdown -h now
```

2.1.8.2.6 Migrating an Image of Ubuntu

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

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

> ⓘ **Important**
>
> - Each of the following procedures provides an example of the command operation. The operation method may vary slightly, depending on the user's environment. Perform each operation according to the user's environment at the responsibility and decision of the user.
> - 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
   ```

   > 💡 Configure the SSH service settings as necessary.
   > *Tip*

3. Installation of cloud-init
   Install cloud-init by following the procedure below.
   ```
   # apt-get install cloud-init
   # dpkg-reconfigure cloud-init
   ```
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.

   a. 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
   ```

   b. Execute the following command to apply the settings:
   ```
   # update-grub
   ```
5. Setting of network (DHCP connection)

   > 💡 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.
   > *Tip*

   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

   a. 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
   ```

   b. 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

   a. Install iptables-persistent with the following command:
   ```
   # apt-get install iptables-persistent
   ```

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

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

8. Configuring cloud.cfg

   Configure the settings of /etc/cloud/cloud.cfg.

   Configure the operational settings of cloud-init in /etc/cloud/cloud.cfg. For details on the settings, refer to the support site of cloud-init.

9. Shutting down the OS

   Shut down the OS.

   ```
   # shutdown -h
   ```

2.1.8.2.7 Capturing Images of a Virtual Server

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

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 IaaS Environment

2.1.8.3.1 Transferring Images

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

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

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 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 44: 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

Item	Description	Required
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	When you omit this parameter, a uuid is automatically assigned by IaaS service infrastructure. Users can specify this parameter in order to use an ID that they originally obtained. When you specify the uuid, be sure to use the one that is created by using a command, such as uuidgen, dedicated for creating uuid.	
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.	
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 • win2016SE_ja: Windows Server 2016 SE (Japanese Version) • win2016SE_en: Windows Server 2016 SE (English Version) • rhel6: Red Hat Enterprise Linux 6 • rhel7: Red Hat Enterprise Linux 7 • centos: CentOS • ubuntu: Ubuntu Note Be sure to specify an OS type that matches the OS in use from which the image will be imported. If you specify a type that is different from the one in use, the following problem may occur. • The virtual server does not start normally • You will not receive the correct OS support • You will be charged for the wrong OS support	Yes

Acquiring the Registration Status List for Virtual Server Images

Acquire a list of the image registration processes that have been requested for the system within a domain. The list is output 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

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

2.1.8.4 Working with Imported Virtual Server Images

2.1.8.4.1 Creating a Virtual Server

Run the virtual server creation API of the IaaS virtual server service by specifying the virtual server image. For details about the virtual server creation API (POST /v2/servers), refer to API Reference.

When you create a virtual server, note the following points:

- Obtain the password for the user that logs in for the first time or configure the public key settings.
- On the server to be created, create a security group that can be accessed from outside.

2.1.8.4.2 First Login to the Virtual Server

After creating a virtual server, perform the first login to each type of OS.

When the OS of the Created Virtual Server is Windows

Using a remote desktop connection, log in as the administrator and change the password.

> Tip
>
> Use the password obtained in Administrator Password for a Virtual Server when you created the virtual server.

After changing the password, check the event log to confirm that the migration agent was uninstalled.

1. Log in as an Administrator.
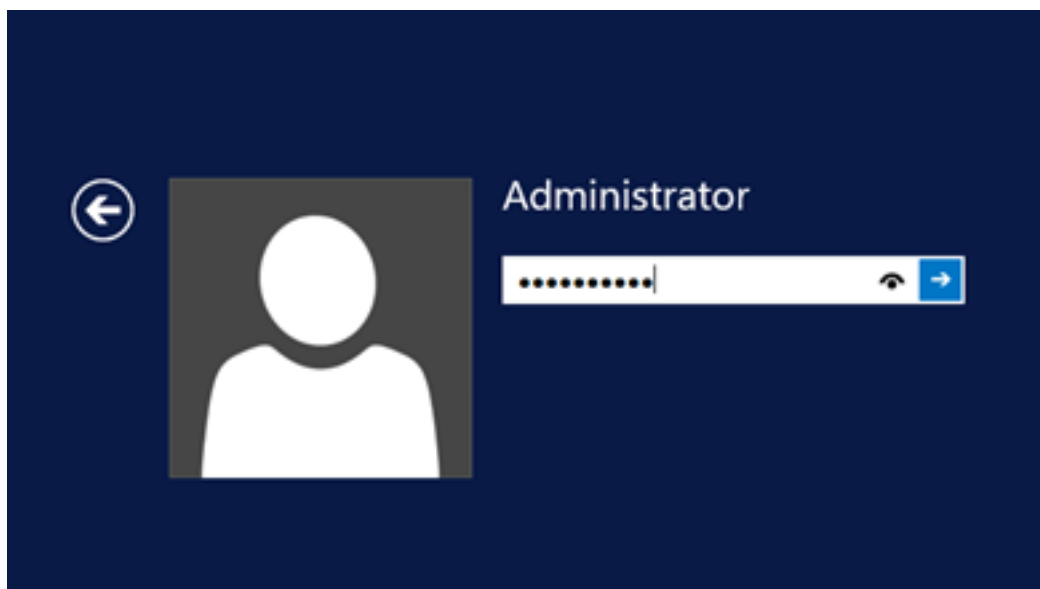
2. Change the password.
   If the password setting screen does not appear, disable the RDP temporarily and wait for a while.
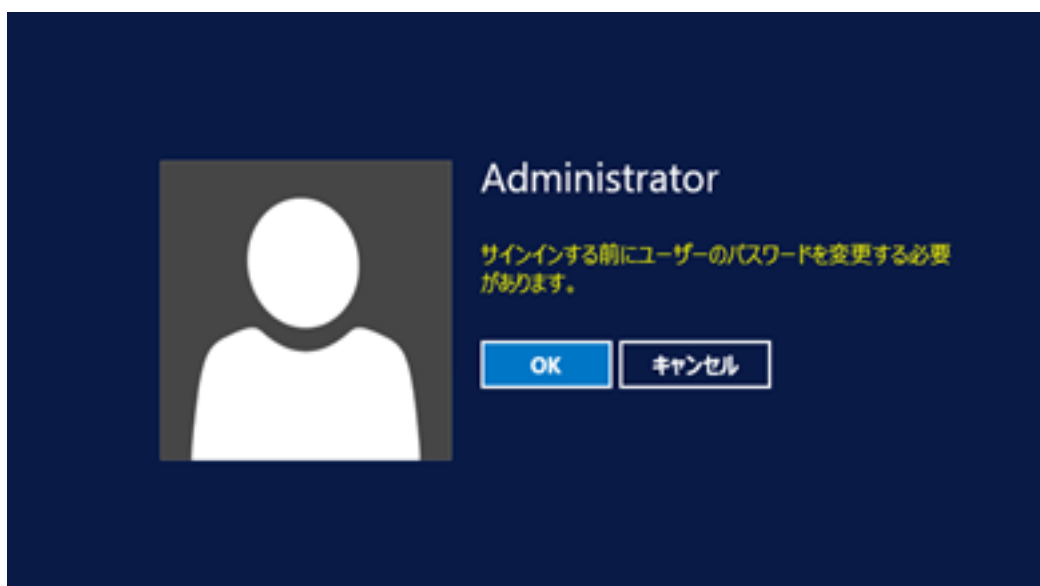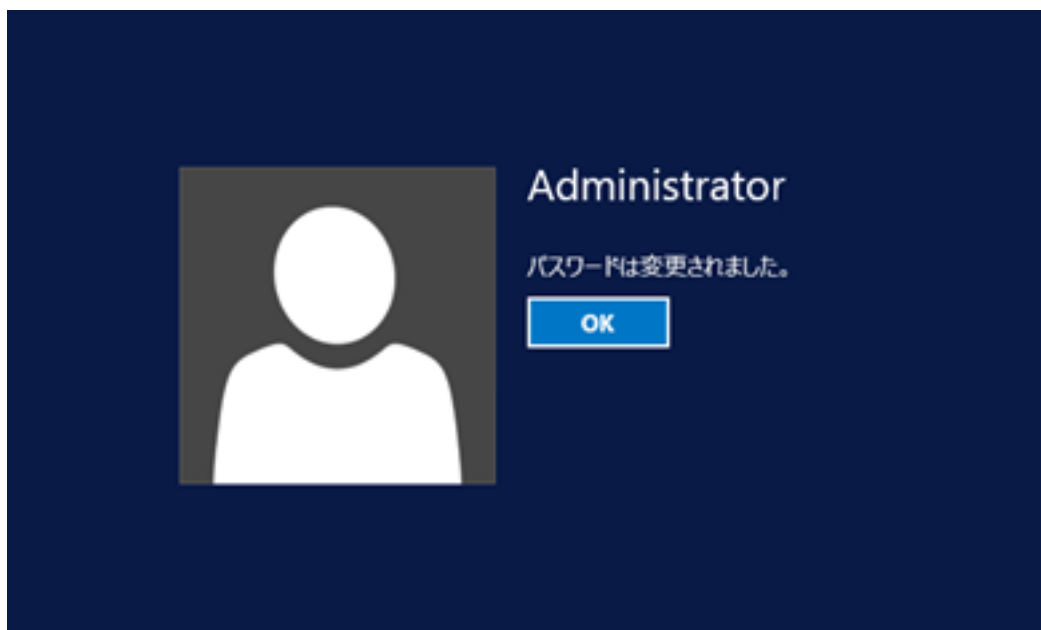
3. When you log in to the virtual server, refer to the event log.
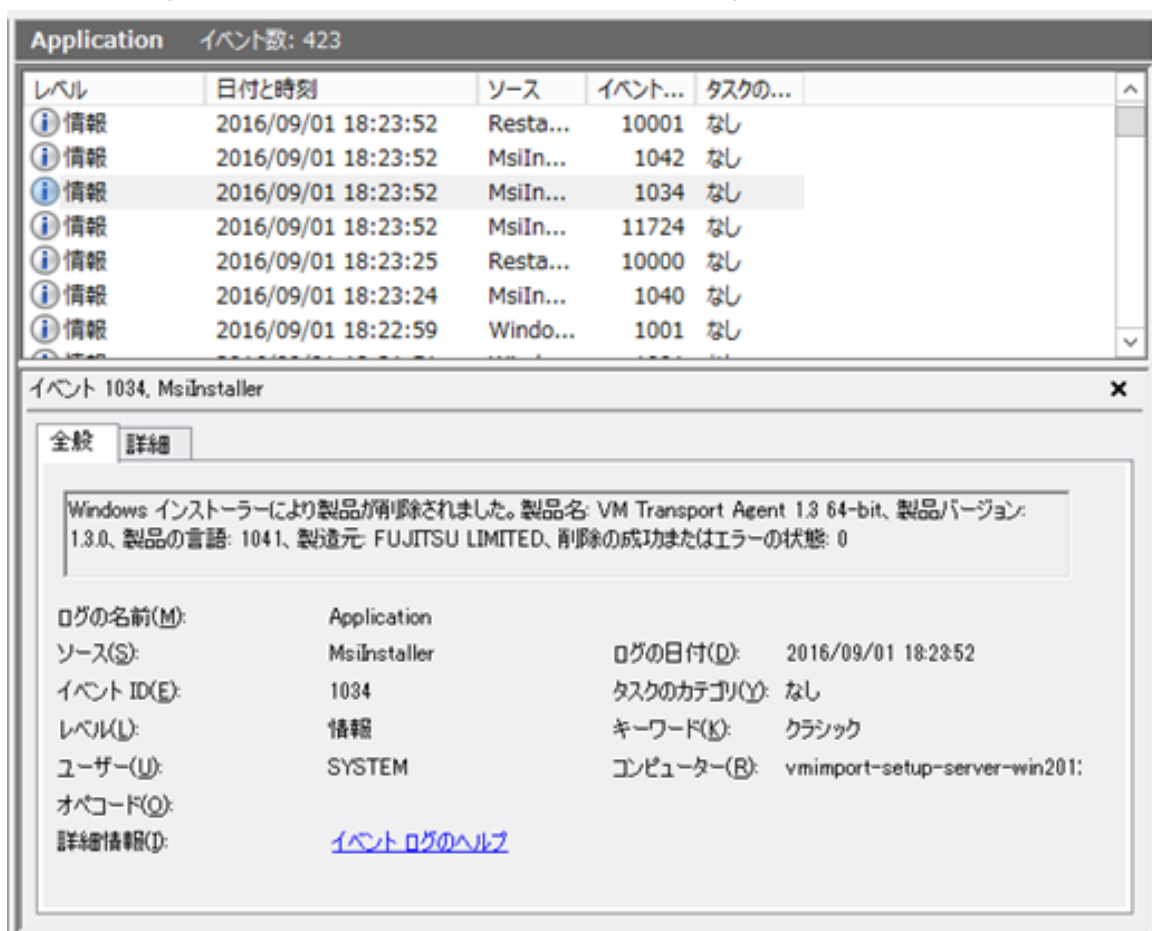
When the OS of the Created Virtual Server is Linux

Log in to the migration source image as the user that you configured for cloud-init. For the password, specify the password that you assigned with the user information when you created the virtual server or specify the private key that matches the configured public key.

2.1.8.4.3 KMS License Activation for the Virtual Server (Windows Only)

After starting a Windows server, you must configure KMS activation settings and perform activation as necessary. For details on KMS activation, contact the service desk.

You can also specify the automatic configuration of KMS activation settings when you execute the image registration API. When you specified automatic configuration, check if the settings are configured or the licenses are activated by performing the steps below.

Procedure for checking the KMS activation status

1. Start a command prompt with Administrator privileges.
2. Run the command "cscript %WINDIR%\system32\slmgr.vbs /dlv."

Table 45: List of Activation Methods for the KMS License Activation

Authentication Method	User Operation
Manual	Contact the service desk for assistance.
Automatic	Specify the request parameter 'kms' when you execute the image registration API. Set the 'activate' parameter in 'kms' content as shown below *1. (For details, refer to API Reference) • True: Automatically configures the activation settings and also performs activation *2

*1: When KMS activation settings are already configured in an on-premise environment, if you specify automatic configuration of KMS activation settings at the execution of the image registration API, the automatic activation overwrites the license information.

*2: If the automatic activation fails, perform the activation manually by following the instructions of the service desk.

2.1.9 Virtual Server Export

2.1.9.1 Overview of Functions

2.1.9.1.1 What is Virtual Server Export?

This function allows you to migrate a virtual server running in IaaS to your on-premises environment. Image files are stored in object storage based on the virtual server image that you have created.
The diagram below shows how this function is used.
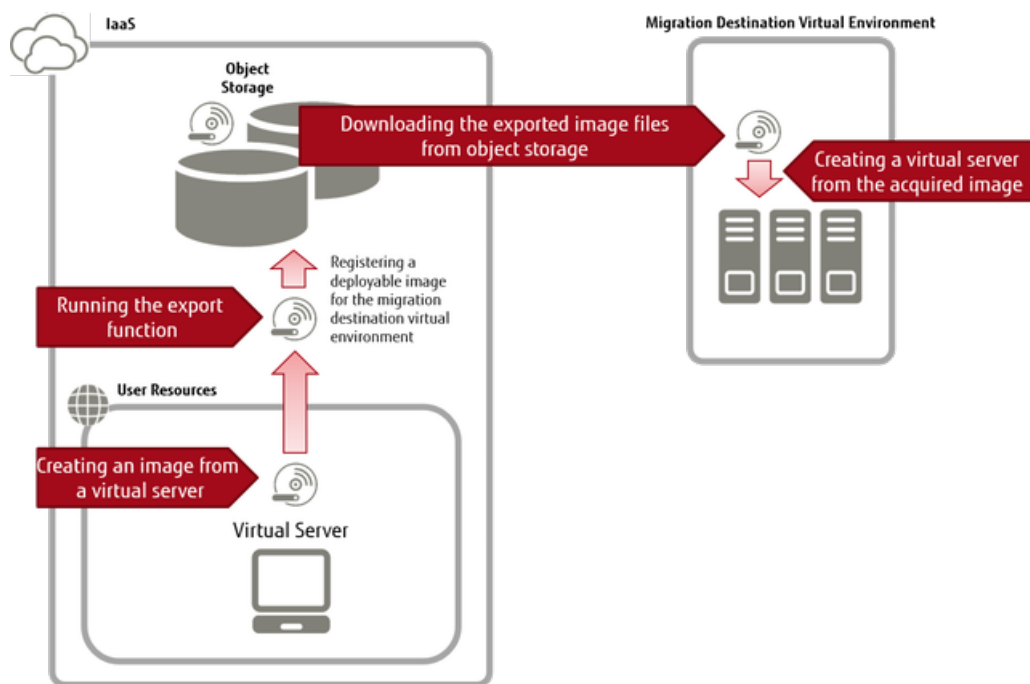
Figure 24: Using Virtual Server Export

Supported Migration Destination Virtual Environments

Table 46: List of Migration Destination 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

Supported Virtual Server Images

Table 47: Availability of Export Process

Type of Virtual Server Image to Be Exported	Availability of Export Process
Image imported by using virtual server import	✓
Derivative image of the virtual server deployed from an image that was imported by using virtual server import	✓
Image provided by the OS provision service	-
Derivative image of the virtual server deployed from an image that was provided by the OS provision service	-

Migration Source Guest OS Types that Can Be Exported

A list of migration source guest OS types that can be exported is shown below.

Table 48: List of Migration Source Guest OS

OS Type	Supported OS
Windows	• Windows 2008 R2 SE 64bit (Japanese Version, English Version) • Windows 2008 R2 EE 64bit (Japanese Version, English Version) • Windows 2012 SE 64bit (Japanese Version, English Version) • Windows 2012 R2 SE 64bit (Japanese Version, English Version) • Windows 2016 SE 64bit (Japanese Version, English Version)
Linux	• CentOS 6.5, 6.6, 6.7, 6.8 64bit • CentOS 7.1, 7.2 64bit • RHEL6 64bit • RHEL7 64bit • Ubuntu 14.04 LTS 64bit

Functions Included

The following functions are provided:

• Virtual Server Image Export Request

You can specify an image created from a virtual server, and make a request to the system for export processing.

> **Tip**
> An export request is immediately returned. You can use the "Acquire Export Status" function to determine if the requested export process has been completed.

• Acquire Export Status

You can specify the export ID that was issued during an export request to acquire the export status.

• Acquire Export Status List

You can acquire a list of export statuses.

> **Tip**
> • The most recent export requests are acquired first.
> • You can only acquire export requests that were made within the project for the token that is used.

• Cancel In-Progress Export Process

You can specify the export ID that was issued during an export request, and request the system to cancel the target export process.

> **Tip**
> An export process cancel request is immediately returned. You can use the "Acquire Export Status" function to determine if the requested export process has been canceled.

Limitations on Migration Source Virtual Server Configurations

• Disk Configuration

Only system storage that is on the startup disk can be exported. Additional storage cannot be exported.

Handling of Licenses

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

Table 49: Handling of Licenses by Type of Exported OS

Type of Exported OS	Handling of Licenses
Windows	After exporting is complete, you must remove the SPLA license. Modify the KMS authentication settings according to your environment, and then perform authentication again.
Linux	• Red Hat Enterprise Linux Check the subscription requirements of the RHEL that you use in the migration destination virtual environment. • CentOS No license required. • Ubuntu No license required.

How to Use This Service

Use the following procedure to export a virtual server image on IaaS.

STEP 1	Configuring OS settings for the Migration Source Virtual Server	Configure environment settings required for export on the virtual server OS that is operating in a IaaS environment.
STEP 2	Terminating virtual servers	Terminate the virtual server in the migration source's virtual environment.
STEP 3	Creating an Image	Create a virtual server image from the system storage of the terminated virtual server.
STEP 4	Requesting Export	Specify the created virtual server image, and request an image export.
STEP 5	Transferring Image Files	Confirm that the export request was completed, and then transfer the image files from object storage to your environment.
STEP 6	Beginning Use of the Image	Deploy a virtual server from the image files for use in your environment.

Figure 25: How to Use Virtual Server Export

2.1.9.2 Procedure on the Migration Source Virtual Server

2.1.9.2.1 Configuring Settings on a Virtual Server in Advance

This section describes the settings that must be configured in advance on the virtual server that is targeted for export.

Use the following procedure for the virtual server targeted for export.

Procedure

1. Logging in to a Virtual Server
   Log in to the virtual server to configure the required settings on the guest OS.
2. Configuring Settings by Guest OS in Advance
   • When the Guest OS is Windows
     If Cloudbase-init is installed, uninstall it.

- When the Guest OS is Linux

  If Cloud-init is installed, uninstall it.

  > 💡 **Tip** You may need to replace the initial RAM disk with the embedded driver that is compatible in the migration destination virtual environment.

3. Terminating virtual servers

   Use one of the following methods to terminate the virtual server.
   - Run the shutdown command on the guest OS.
   - Run "Termination of Virtual Server" on the portal or API.

2.1.9.3 Procedure on the IaaS Environment

2.1.9.3.1 Creating Virtual Server Images

This section describes how to create a virtual server image in order to use the Virtual Server Image Export function for export processes.

Complete the Configuring Settings on a Virtual Server in Advance.

Use the following procedure to create a virtual server image to be exported.

Procedure

1. Specify the system storage for the target virtual server.
2. Specify the following parameters and create a virtual server image from the system storage.

Table 50: Parameters Specified when Creating a Virtual Server Image

Item	Description	Required
Image Name	Specify a name that identifies the virtual server image 💡 **Tip** The specified name is also applied to the virtual server image files after exporting is completed.	✓
Disk Format	Specify "raw"	
Container Format	Specify "bare"	
Force Option	Specify "true"	

Export processing is possible if the status of the created virtual server image is "ACTIVE."

> ⚠ **Important** Do not delete the created virtual server image until the export process is completed and the virtual server image is stored in object storage as virtual server image files.

2.1.9.3.2 Virtual Server Image Export Function

This function allows you to specify a virtual server image created from a virtual server, and make a request to the system for export processing. Further, there is a function for checking the status of the requested export process.

Virtual Server Image Export Request Function

To request the export of a virtual server image, specify the following items. If the request is successful, an export ID is issued.

Table 51: Exporting a Virtual Server Image (List of Items)

Item	Description	Required
Image ID	Specify the image ID assigned to the export source virtual server.	✓
Export Destination Container for Object Storage	Specify the object storage container where exported virtual server images are stored. Use the following format: `/v1/AUTH_<Project ID>/<Container Name>`	✓

> **Note**
> - Image IDs other than for projects registered by the user operating this function cannot be specified.
> - You cannot specify the same image ID and the same export destination object storage container when making multiple export requests.
> - If image files (including separated files) with image names identical to the ones set for the image ID already exist in the object storage container that is the export destination, an export request is not possible.

Acquire Export Status List Function

This function acquires a list of virtual server image export processing that can be referenced in the project scope of the token. You can specify the following items and make changes to the range of acquisition.

Table 52: List of Virtual Server Image Export Statuses (List of Setting Items)

Item	Description	Required
Start Position	Specify the first index where list acquisition starts. **Tip** If this setting is omitted, the most recently requested export process is returned.	
Number Acquired	Specify the number of records acquired in the list. **Tip** If this setting is omitted, all export processes are returned. (Maximum 200 records)	

You can also acquire basic status information for each export process.
- succeeded

  This status indicates that the export process was completed successfully.
- failed

  This status indicates that the export process failed.
- processing

  This status indicates that the export is being processed.
- queued

  This status indicates that the export process is queued.
- canceling

  This status indicates that the export is being canceled.
- canceled

  This status indicates that the export has been canceled.

Acquire Export Status Function

You can specify an export ID and acquire detailed information regarding the export processing status for a single virtual server image export process.

- Information about the status of the export process
- Progress rate (from 0 to 100%)
- Information about the settings when the export process was requested
- Date/time when the export process request was received

Cancel In-Progress Export Process Function

You can specify an export ID and request the cancellation of a single virtual server image export process.

> **Note**
> - Cancellation can be requested only if the status of the export process is incomplete.
> - You cannot register multiple cancellation requests for the same export ID.
> - Once a cancellation request has been registered, it cannot be canceled.

You can use the Acquire Export Status function to check the cancel status of an export process. However, this function operates as indicated below, depending on the status and progress rate of the export process.

Table 53: Cancel Request Status and Estimated Standby Time until Cancellation is Completed

Cancel Request Status	Estimated Standby Time until Cancellation is Completed
Status: queued	5 minutes
Status: processing Progress rate: 0 - 10	20 minutes
Status: processing Progress rate: 11 - 40	Varies based on image size (approximately 6 hours for 300 GB) **Tip** Canceled when the progress rate reaches 40.
Status: processing Progress rate: 41 - 70	Varies based on image size (approximately 1 hour for 300 GB) **Tip** Canceled when the progress rate reaches 70.
Status: processing Progress rate: 71 - 95	Varies based on image size (approximately 2 hours for 300 GB) **Tip** Canceled when the progress rate reaches 95.

2.1.9.3.3 Transferring Image Files

Image files for which the export process is completed are stored in object storage. In order to use them in your environment, acquire the image files from object storage and transfer them to the migration destination environment.

Image files are stored in object storage under the following conditions.

- Image files (objects) are stored with the "Image Name" + ".vmdk." Image Name is a name specified when the image was created from the virtual server system storage.
- An ".ovf" file and an ".mf" file are also stored in the same container where the image files (objects) are stored.
- Image files (objects) are divided and uploaded separately.
- Divided files are stored in a different container with the name "Container Name" + "_segments."

> **Note** If one or more divided files are deleted by accident, you will be unable to use the corresponding image files.

Use the following procedure to acquire exported image files.

Procedure

1. Receive authorization to access the object storage where image files are stored.
2. Specify the following parameters to acquire image files from object storage.
   - Project ID
   - Container name where exported image files are stored
   - Names of exported image files
3. Acquire the ".ovf" file and the ".mf" file at the same time.

Confirm that all image files, the ".ovf" file, and the ".mf" file were acquired successfully. At this time, the ".ovf" file is configured to start the virtual server with the minimal settings. Therefore, make the necessary modifications before transferring the files to your environment.

- Configuring the number of CPUs (Changing the VirtualQuantity value)

```
<Item>
  <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
  <rasd:Description>Number of Virtual CPUs</rasd:Description>
  <rasd:ElementName>1 virtual CPU(s)</rasd:ElementName>
  <rasd:InstanceID>1</rasd:InstanceID>
  <rasd:ResourceType>3</rasd:ResourceType>
  <rasd:VirtualQuantity>1</rasd:VirtualQuantity>
</Item>
```

- Configuring the memory size (Changing the VirtualQuantity value)

```
<Item>
  <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
  <rasd:Description>Memory Size</rasd:Description>
  <rasd:ElementName>512MB of memory</rasd:ElementName>
  <rasd:InstanceID>2</rasd:InstanceID>
  <rasd:ResourceType>4</rasd:ResourceType>
  <rasd:VirtualQuantity>512</rasd:VirtualQuantity>
</Item>
```

> **Tip**
>
> Table 54: List of OS Configured in ".ovf" Files
>
> | OS Type | Settings |
> | --- | --- |
> | Windows 2008 R2 | <OperatingSystemSection ovf:id="1" vmw:osType="windows7Server64Guest"> |
> | Windows 2012 R2 | <OperatingSystemSection ovf:id="1" vmw:osType="windows8Server64Guest"> |
> | Windows 2016 | <OperatingSystemSection ovf:id="1" vmw:osType="windows9Server64Guest"> |
> | Other than Windows | <OperatingSystemSection ovf:id="1" vmw:osType="otherGuest"> |

When the acquisition of image files and the acquisition and editing of ".ovf" and ".mf" files are completed, transfer them to your virtual environment.

Billing continues based on the amount of use of images created as export sources registered in the image archiving service, and image files that have been exported. After confirming that normal operation occurs in your environment, do not forget to delete any files that are no longer needed.

2.1.9.4 Procedure on the Migration Destination Customer's Environment

2.1.9.4.1 Deploying Virtual Server Images

Use OVF image files (.vmdk, .ovf, .mf) acquired from a IaaS environment to deploy a virtual server in your virtual environment.

For more information about how to deploy a virtual server, refer to the VMware manuals.

Example: Deploying a virtual machine by using VMware VSphere Client

1. Select [File] > [Deploy OVF Template] from the menu.
2. Specify the acquired OVF image files, and click the [OK] button.

The setting status for the deployed virtual server is as indicated below.

Table 55: Setting Status for a Virtual Server Deployed to a VMware Environment

Settings	Status
Account	The account that was set during virtual server import can be used (including the root user).
Network	DHCP enabled, MAC address not set
Firewall	Disabled

> The above items are set automatically when importing. Adjust these settings as required when exporting.
>
> Tip

2.2 Services for SAP

Virtual servers that can be used for SAP applications, and a function for deploying them in a dedicated physical host pool are provided.

> **Note** This function is only provided in the Eastern Japan Region 1 and Western Japan Region 2.

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.
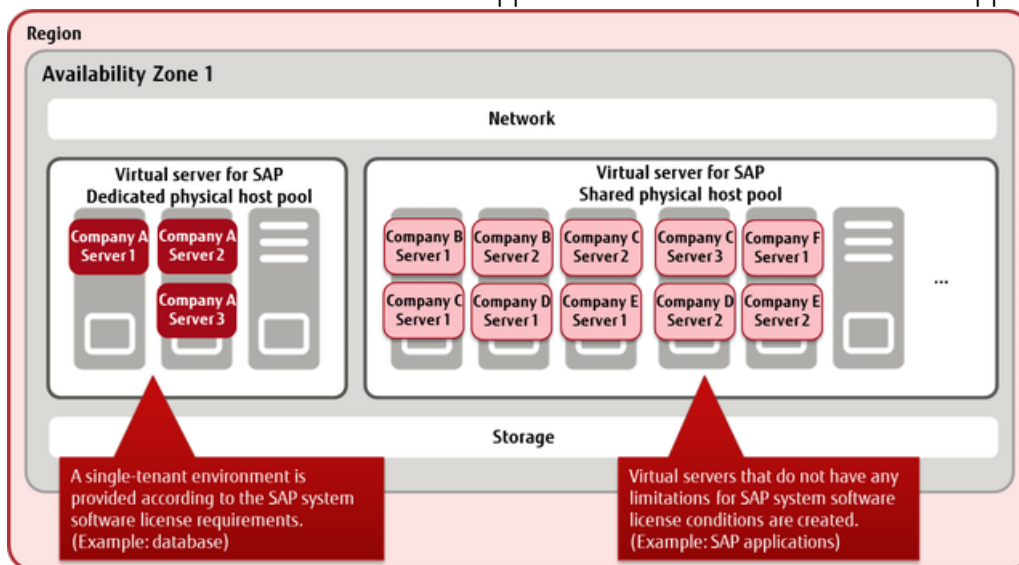
Functions Included

- 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

    Use the images provided in List of Available OS of Virtual Server for SAP 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 servers (Automatic failover)

  If the server stops during an operation due to issues such as failure of the physical host machine at the data center, the virtual server that was operating on that host machine is automatically moved to a different host machine and the server operates there.

  > **Note**
  > - The automatic failover (automatic recovery) function is always enabled (it cannot be disabled). When automatic failover is completed, a notification email is sent to the overall administrator of the project the target resource belongs to. For details on notification emails, refer to Automatic Failover Notification Messages.
  > - If Auto-Failover is performed while virtual servers are being started or stopped, they may have a different power status from the assumed status.
  >
  >   In such cases, manually perform the power operation for the virtual server. If the power status does not change within around 10 minutes, perform the power operation again.

- Image management

  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.

  Choose to disclose a created private image either within the project or within the domain.

- Storage
  - Storage Type

    There are the following types of storage.

Table 56: List of Storage Types

Class	Storage Type
Standard Type	M1
High Performance Type	H2

> **Note**
> The storage type can be selected when adding a disk to a virtual server. You cannot change the storage type after a disk has been added.

  - Standard Type

    The standard type is efficient in cost performance.

Table 57: Purposes and Disk Sizes of the Standard Type

Storage Type	Purpose	Disk Size
M1	• When you deploy application data that requires frequent file access (reading and writing) • When you handle a lot of large data files	0.1 - 2047 GB (in units of 0.1 GB)

  - High Performance Type

    For high performance type, the performance of the storage improves, as the disk size increases.

Table 58: Purposes and Disk Sizes of the High Performance Type

Storage Type	Purpose	Maximum IOPS/ GB	Disk Size
H2	For small-scale or medium-scale DBs, when storing application data that requires data throughput.	5 IOPS/GB *1	512 - 2047 GB (in units of 1 GB)

*1: IOPS is calculated with a block size of 16 KB. Performance varies depending on the operating environment and other factors. There is no guarantee for a certain level of performance.

> **Note**
> - The high performance type cannot be specified for the following. These are fixed as standard type.
>   - System storage
>   - Additional storage created when creating a virtual server
> - Storage performance varies in proportion to the disk size. Therefore, a disk with a small storage size may not produce enough storage performance.

- System Storage

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

  Standard type storage is used for system storage.

Table 59: List of System Storage Sizes (Eastern Japan Region 1, Western Japan Region 2)

OS Type	OS Provided	Size
Windows	Windows Server 2016 SE 64bit English Version	180 GB
	Windows Server 2012 R2 SE 64bit English Version	180 GB
	Windows Server 2008 R2 SE SP1 64bit English Version	180 GB
	Windows Server 2016 SE 64bit Japanese Version	80 GB
	Windows Server 2012 R2 SE 64bit Japanese Version	80 GB
	Windows Server 2008 R2 SE SP1 64bit Japanese Version	80 GB

- Additional storage

  Additional storage is provided for data archiving.

  When adding storage to a virtual server, it is possible to select the storage type.

Table 60: Selectable Additional Storage Types and Sizes

Storage Type	Size
Standard Type	0.1 - 2047 GB
High Performance Type	512 - 2047 GB

Table 61: List of Limiting Values Related to Additional Storage

Item	Limiting Values
Number of Storage Systems	1 - 55

- Snapshot function

  This function is used to 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 62: 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 63: 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 26: How to Use a Virtual Server for SAP

STEP 1	Enabling an Environment	Enable an environment for a project in which you want to use a virtual server for SAP.
STEP 2	Building a Network	Create a virtual router, network, and subnet in the project, in the same way as a normal virtual server.
STEP 3	Assigning Network Resources	Assign network resources (such as private IP addresses) to the subnet in STEP2 for the virtual server for SAP environment.
STEP 4	Preparing a Virtual Server for Logging In	Provide a virtual server on a different subnet that is connected via a virtual router to the subnet on which steps 1 through 3 have been completed.
STEP 5	Creating a Virtual Server for SAP	Specify the required information, such as server type, OS image, and Administrator password, to create a virtual server for SAP.
STEP 6	Using a Virtual Server for SAP	From the virtual server you created in STEP 4, log into the created virtual server for SAP via remote desktop.

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 normal virtual server cannot be created.
- A virtual server for SAP 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 64: 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 by the system.	

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)

Virtual Router

Network A

Subnet Name: fcx_subnet-w:....
Network Address: 192.168.1.0/24

IP Address Range:
192.168.1.2–192.168.1.50

Port

Assign an IP address to the virtual server for SAP that is within the specified network address range, but that is outside the specified IP address range.
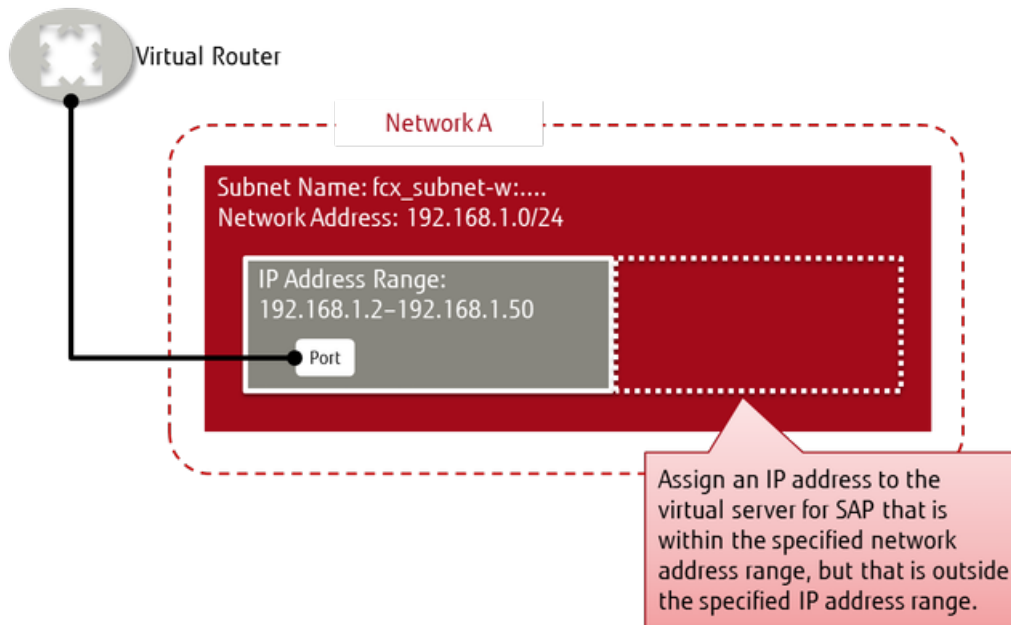
Creating a Network Resource

Create a network resource by assigning the subnet that has been created for the virtual server for SAP environment.
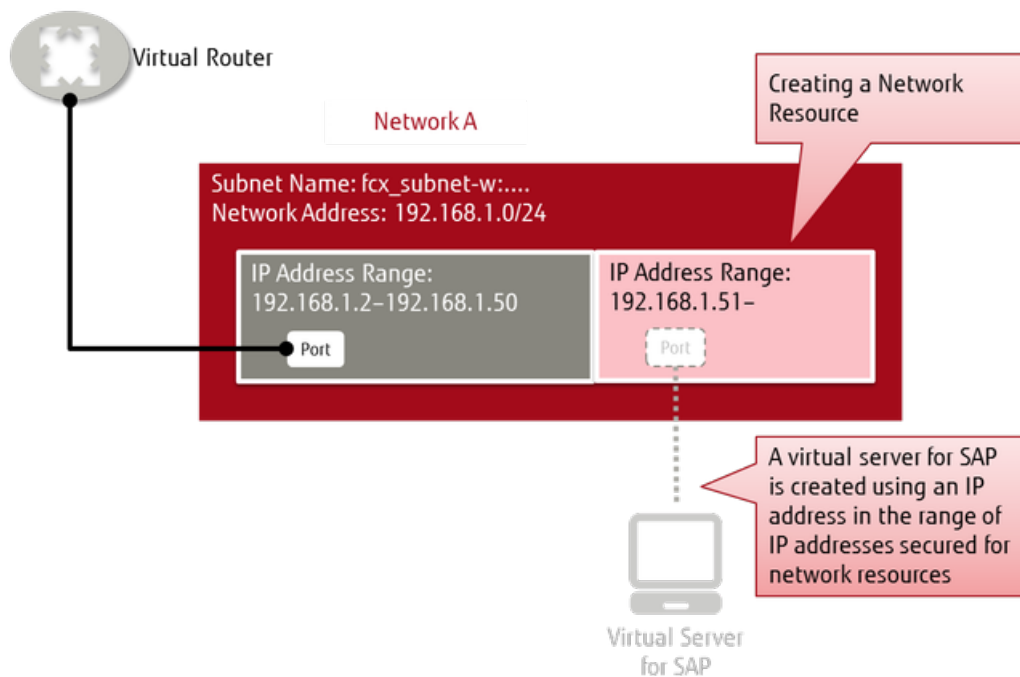
Preparing a Virtual Server Used for Logging In

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.
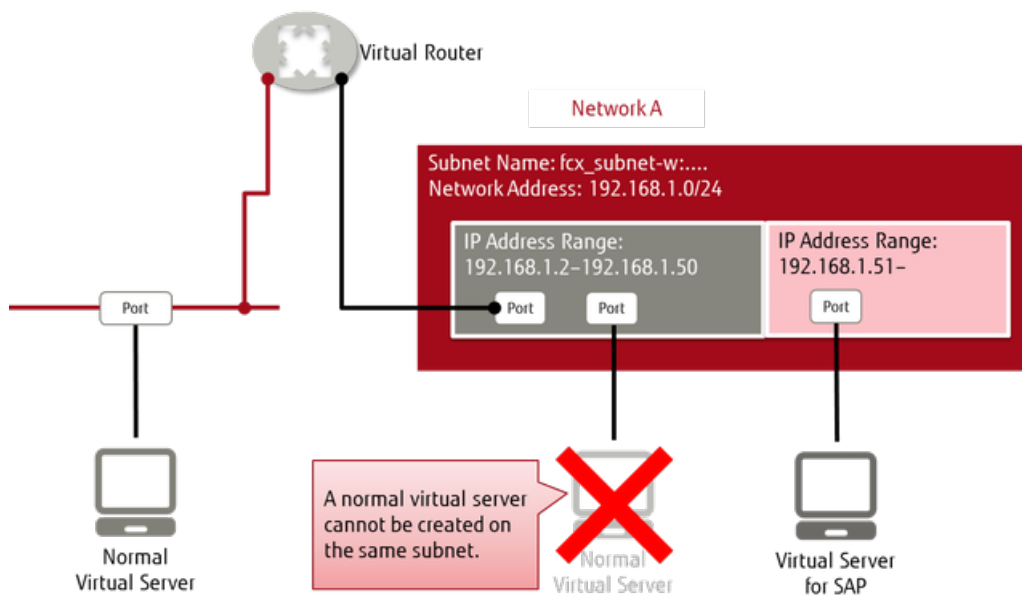
2.2.1.3 Creating/Deleting a Virtual Server for SAP

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 List of Available OS of Virtual Server for SAP
- 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 65: 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
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.	

Item	Description	Required
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.	
Creation in the Dedicated Area	Specify "true" to create a virtual server for SAP in the dedicated area Note: To create a virtual server for SAP in the dedicated area, 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 66: List of Types of Virtual Server for SAP (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
WS-2	2	8
WS-4	4	16
WS-8	8	32
WS-16	16	64
WS-32	32	128

List of Available OS

Table 67: List of Available OS of Virtual Server for SAP

OS Type	OS Provided
Windows	• Windows Server 2016 SE 64bit English Version • Windows Server 2012 R2 SE 64bit English Version • Windows Server 2008 R2 SE SP1 64bit English Version • Windows Server 2016 SE 64bit Japanese Version • Windows Server 2012 R2 SE 64bit Japanese Version • Windows Server 2008 R2 SE SP1 64bit Japanese Version

2.2.1.4 Operations on a Virtual Server for SAP

Carry out the following operations on a virtual server for SAP that has been created in an SAP service 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**
> When a virtual server for SAP starts up, there is no waiting for its OS to start up.

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

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

Item	Description
Resource ID	Obtain the resource ID of the target virtual server for SAP.
Power Status	Obtain the power status information of the virtual server for SAP. • on • off • unknown
Snapshot Generations	Obtain the number of snapshot generations taken for the virtual server for SAP.
Snapshot Date and Time	Obtain the date and time of when snapshots were taken for the virtual server for SAP.

Item	Description
Snapshot ID	Obtain the ID of the snapshots taken for the virtual server for SAP.
Storage Name	Obtain the name of the storage system attached to the virtual server for SAP.
Storage ID	Obtain the ID of the storage system attached to the virtual server for SAP.
Storage Capacity	Obtain the capacity (in GB) of the storage system attached to the virtual server for SAP.
Device Path	Obtain the path or identifier of the device connected to the storage system.
MAC Address	Obtain the MAC address of the network interface connected to the virtual server for SAP.
Status	Obtain the status information of the virtual server for SAP. • normal • warning • stop • error • fatal • unknown

Attaching Additional Storage

To attach additional storage, specify the following items:

Table 69: 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.

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

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

Adding a Port

To add a port, specify the following items.

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

	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.
Tip	

Table 70: 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 Tip: If this setting is omitted, an IP address is automatically assigned from the IP address 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.

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

Table 71: 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

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

Creation of a snapshot

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

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

	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.
Note	

<div align="center">Table 72: Taking a Snapshot (List of Items That Can Be Set)</div>

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.

<div align="center">Table 73: Deleting a Snapshot (List of Items That Can Be Set)</div>

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	

<div align="center">Table 74: Restoring from a Snapshot (List of Items That Can Be Set)</div>

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 Cloning Images (Private Images)

Create private images from 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.

<div align="center">Table 75: Creating a Private Image (List of Items That Can Be Set)</div>

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

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

2.2.1.6 Managing Virtual Server for SAP Backup Images

Create a backup image from an existing virtual server for SAP. Also, delete an already created backup image.
When a backup image has been created for a virtual server for SAP, if the system stops operating properly for some reason, it is possible to restore the virtual server for SAP from the backup image.

> **Tip**
> When it is necessary to temporarily maintain the status of a system due to updating of an application, etc., use the snapshot function. Backup images should be used when it is necessary to create a regular backup for a system that will be retained for a long time.

Creating a Backup Image

To create a backup image from a virtual server for SAP that has been created, specify the following items.

Table 76: Creating a Backup Image (List of Items That Can Be Set)

Item	Description	Required
Name	Specify a name for the backup 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 "backup."	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 backup image	Yes
Comment	Specify a comment (character string) to set for the backup 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	
Disk	Specify whether to back up only the system disk, or to also back up all of the data disks	

> 🔜 • As a target for which you want to create a backup image, specify a virtual server for SAP that has been started before.
>
> **Note** • When creating a backup image, stop the target virtual server for SAP in advance.

Re-creating a Virtual Server Using a Backup Image

When a virtual server for SAP stops operating correctly, re-create the virtual server for SAP from a backup image. To re-create a virtual server for SAP, specify the following items.

> ⓘ When a virtual server for SAP has been re-created from a backup image, the re-created
>
> **Important** virtual server for SAP is considered to be a different virtual server from the one used to create the backup. Be careful, as an additional charge from the OS provision service will be incurred for the re-created virtual server.

> 💡 After re-creating a virtual server for SAP from a backup image, delete the original virtual server for SAP that was used as the source for backup image creation. Immediately after
>
> **Tip** a virtual server for SAP is created, it will be in the "stopped" state. Start the virtual server for SAP as necessary.

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 alphanumeric characters, hyphens (-), underscores (_), and periods (.) • Specify at least 1 character, and no more than 64 characters. • Use an alphanumeric character as the first character	Yes
Creation Method	Specify "restore".	Yes
Disk	Specify whether to create only the system disk, or to also create all of the data disks	

Deleting a Backup Image

Specify the name of an unnecessary backup image to delete it.

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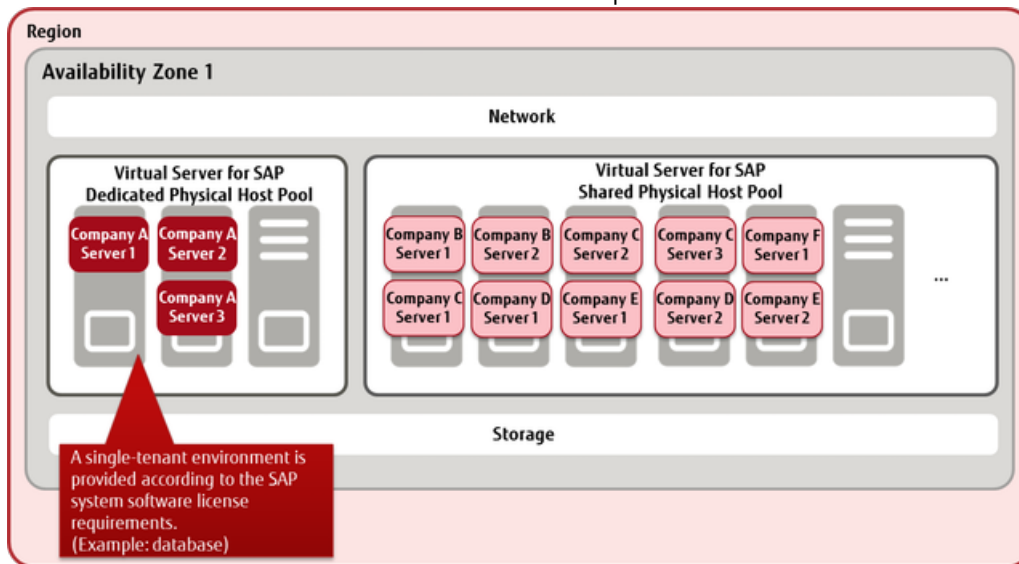
This server can be used for environments that must be separate from other users (single tenant), as required in the license for SAP system software.

> ⓘ **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 78: List of Types of Virtual Server for SAP (Flavors)

Type Name	Number of Virtual CPUs	Memory (GB)
WS-2	2	8
WS-4	4	16
WS-8	8	32
WS-16	16	64
WS-32	32	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 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.
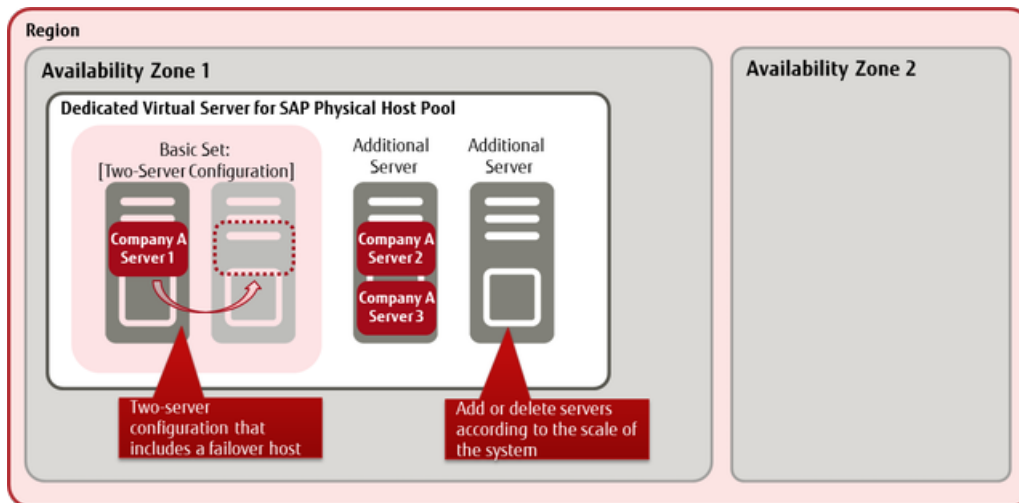
Figure 27: Using the Physical Host Pool Menu

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 (Automatic failover)
  - Image management

The same functions as normal virtual servers for SAP are also provided for the following:

- Storage
- Network

How to Use This Service

STEP 1	Application for Starting Usage	Apply for the number of physical hosts required to run the dedicated virtual servers for SAP by using a combination of options on the host pool menu.
STEP 2	Notification of Availability for Use	The service provider will inform you when the dedicated virtual server for SAP environment is available.
STEP 3	Execution of Operations on the Dedicated Virtual Servers for SAP	Create dedicated virtual servers for SAP and start system operation.
STEP 4	Application for Changes	Apply for additional physical hosts from the physical host pool menu if the capacity of the host pool ceases to be sufficient during operation.
STEP 5	Application for Stopping Usage	Apply to stop usage of the system when it is no longer needed.

Figure 28: 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:

- Block Storage
- Snapshot
- Object Storage
- Network Attached Storage (NAS)

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

3.1 Block Storage

3.1.1 Storage Type

A block storage can be used for two purposes: as a system storage that stores the OS and as an additional storage that stores data. When you create a new block storage, select a type for the block storage from the following.

Table 79: List of Storage Types

Class	Storage Type
Standard Type	M1
High Performance Type	H2

> **Note** A storage type can be selected when it is created. You cannot change the storage type after it is created.

Standard Type

The standard type is efficient in cost performance. You can specify this for both the system storage and additional storage.

Table 80: List of Storage Types (Standard Type)

Storage Type	Purpose	Disk Size
M1	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	1 GB or more (specified in GB)

High Performance Type

For high performance type, the performance of the storage improves, as the disk size increases. You can use this as additional storage to store application data.

Table 81: List of Storage Types (High Performance Type)

Storage Type	Purpose	Maximum IOPS/ GB	Disk Size
H2	For small-scale or medium-scale DBs, when storing application data that requires data throughput.	5 IOPS/GB *1	1000 GB to 3000 GB (specified in GB)

*1: IOPS is calculated with a block size of 16 KB. Performance varies depending on the operating environment and other factors. There is no guarantee for a certain level of performance.

> **Note**
> - Do not use a high performance type storage as a system storage. If you use it as a system storage, the creation of virtual servers may become delayed or may fail.
> - The storage performance is indicated at its maximum. In addition, the storage performance varies in proportion to the disk size. Therefore, a disk with a small storage size may not produce enough storage performance.
> - The amount of usable storage space within a project is limited. For details, refer to Limiting Values.

3.1.2 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 82: OS Image and System Storage Size

OS	Size of System Storage Specified
Windows 2008 R2 SP1	80 GB or more
Windows 2012 R2	80 GB or more
Windows 2012	80 GB or more
Windows 2016	80 GB or more
Red Hat Enterprise Linux 6.x (x is a number)	40 GB
Red Hat Enterprise Linux 7.x (x is a number)	40 GB
CentOS 6.x (x is a number)	30 GB or more
CentOS 7.x (x is a number)	30 GB or more
Ubuntu Server 14.04 LTS	3 GB or more
Ubuntu Server 16.04 LTS	3 GB or more
Red Hat OpenShift Container Platform 3.x (Node) (x is a number)	70 GB or more
Red Hat OpenShift Container Platform 3.x (Master) (x is a number)	70 GB or more

> **Tip**
> - When you create a virtual server, specify whether to retain the system storage of the server upon deletion.
> - 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.
> - Do not use a high performance type storage as a system storage. If you use it as a system storage, the creation of virtual servers may become delayed or may fail.

- Existing block storage

Attach existing bootable block storage to create a virtual server.

- 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 83: 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** 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.	

Item	Description	Required
Volume Type	Specify the type name of a block storage. 📤 **Note** The notes for each source type specified are as follows: ・When you have specified "image": You can select a storage type (only M1). If you omit this field, M1 is selected. ・When you have specified "volume": The storage type cannot be changed. Even if you specify a value, it is ignored. ・When you have specified "snapshot": The storage is created with the volume type of the volume in the snapshot source. Even if you specify a value, it is ignored.	
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.	

Points to Note
・You cannot detach the system storage from the virtual server.

3.1.3 Additional Storage

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

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

📤 **Note** Take care to ensure that block storage is not deleted while it is being used.

📤 **Note** If you create a block storage by restoring it from an existing volume or a snapshot, you cannot change the storage type.

> **Tip**
>
> When adding or deleting storage to Windows virtual servers of the standard service, make the following changes to the SAN policy. If these changes are not made, it may not be possible for virtual servers to correctly recognize storage after they are rebooted.
>
> 1. Start a command prompt with Administrator privileges.
> 2. Enter "DISKPART" and then press the Enter key.
> 3. Enter "san", and then press the Enter key. Check that "san policy=Offline Shared" is displayed.
> 4. Enter "san policy=OnlineAll", and then press the Enter key.
> 5. Enter "san", and then press the Enter key. Confirm that display has changed to "san policy=OnlineAll".
> 6. Enter "exit", press the Enter key, and finish DISKPART.
> 7. Close the command prompt.

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

Restores block storage from a snapshot. The block storage to be restored can be specified from among the following:

・The block storage from which the snapshot was taken
・Newly created block storage

> **Note**
> ・It is not possible to specify existing block storage that is not the source of the snapshot as the destination for snapshot restoration.
> ・To reuse it for system storage, the block storage that you use as the snapshot source must be bootable.
> ・If you create a block storage by restoring it from a snapshot, you cannot select the storage type.

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 (ACL)
- Versioning
- Custom Metadata Management

Deleting a Container

Delete a container.

> **Important**
> Containers with objects cannot be deleted.

3.3.3 Container Management

Change the settings of an existing container.
The items that you can change are as follows:

- Access Policy Settings (ACL)
- Versioning
- Addition of custom metadata

3.3.4 Access Policy Settings (ACL)

It is possible to set an access policy for a container and allow access to the container or objects. Access policies can be set using the two following methods.

- Policy settings for each user and project
- Policy settings for the referer headers included in HTTP requests

Policy Settings for each User and Project

It is possible to set access policies for each project or each user.

Configurable access permissions

・Reading of containers or objects

・Writing to containers or objects

Policy Settings for the Referer Headers Included in HTTP Requests

It is possible to set access policies for the hosts or domains that are notified in referers. For example, set access policies when allowing reading of objects from websites.

Configurable access permissions

・Reading of containers (acquisition of object lists)

・Reading of objects

> **Note**
> Setting permissions for referers makes it possible to read without performing token authentication. As this setting lowers the level of security, it is not recommended to use it.

For details, refer to the "API Reference - Foundation Service".

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.

<div align="center">Table 84: List of Object Settings</div>

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.	

> ⓘ **Important** When a very large number of objects are created in a container, the response when obtaining the list may be delayed. To prevent lowered performance, limit the maximum number of objects registered in a single container to 1,000,000.

Deleting an Object

Delete objects stored in a container.

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.

<div align="center">Table 85: List of Object Settings</div>

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.	

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 86: NAS Software Image Information

Image Name	FJK5-NAS-V03
Image OS	CentOS 7.2 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 following virtual servers cannot be used because they do not meet the operating requirements of NAS software.
>   ・P-1 / P2-1
>   ・T-1 / T2-1
>   ・LM-1 / LM2-1
>   ・LM-2 / LM2-2
>   ・LM-4 / LM2-4
>   ・LM-8 / LM2-8
>   ・L-12 / L2-12
>   ・L-24 / L2-24
> ・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.

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, and firewall 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

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.
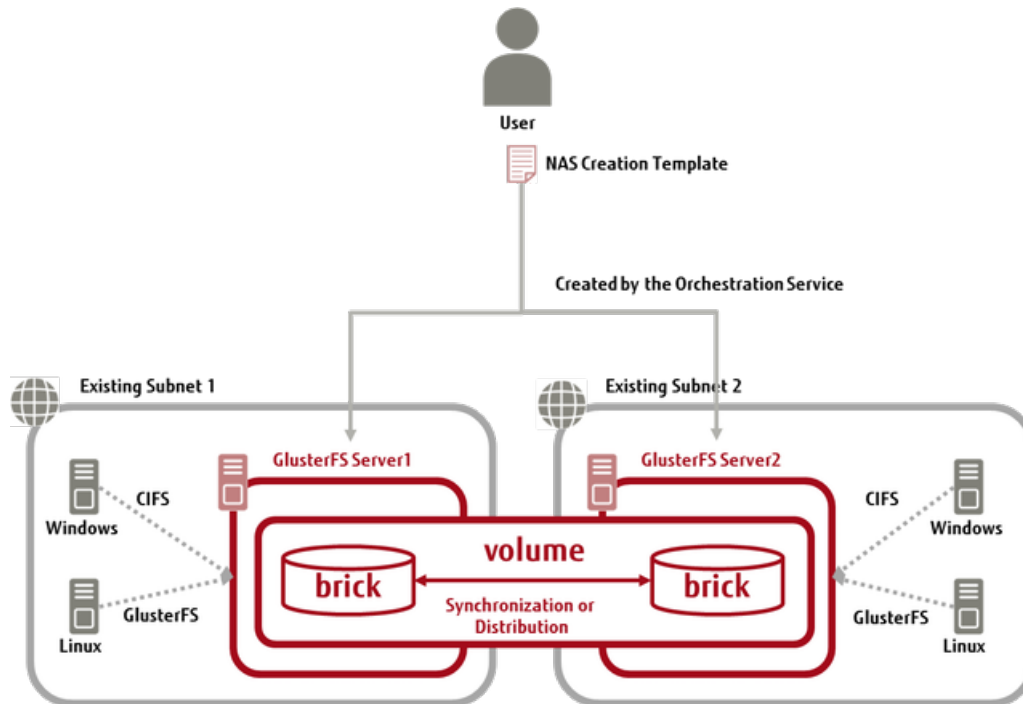
Figure 29: Creation of a NAS Image by Using the Template

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 desk.

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, 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 87: 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)

Parameter	Contents Specified (Value)
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
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 GlusterFS 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
```

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.
> - The host names defined in the NAS deployment template file (nas1, nas2) cannot be changed.

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 3.7.X (X represents 13 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.

   > **Note**
   > The following is an example of command execution. Depending on the version of GlusterFS being installed, the URL of the repository differs.

   ```
   # wget https://download.gluster.org/pub/gluster/glusterfs/old-releases/3.7/LATEST/
   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].

> **Note** If you stop two synchronized NAS servers at the same time, and then start them up again, the client may not be able to connect to one of the NAS servers. If this happens, reboot the NAS server that the client cannot connect to.

---

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, 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 88: 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.
> - Do not connect two or more virtual routers that are connected to external networks to a single 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.

Related concepts

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.

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.

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 89: 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
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 Note: Do not specify the ISP shared address (100.64.0.0/10, or any subnet addresses divided off from that subnet) Note: Do not specify 192.168.122.0/24. Tip: IP addresses outside the above ranges can also be used. However, in that case the user is responsible for the settings and verification of the operation.	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 90: 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.	

Default Rules

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

Table 91: Default Rules When a Security Group Is Created

Direction	Communication Partner	Protocol	IP Version
Outbound (Egress)	All	All	IPv4
Outbound (Egress)	All	All	IPv6

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 92: 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.	

Item	Description	Required
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** When a security group is specified, the following is set for the communication partner. • The IP address that is set for the specified security group However, when "Allowed Address Pairs" are configured for a port, the IP addresses specified as the address pair are also set as the communication partner.	
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. **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 30: 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.

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

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

> 💡 You can add rules to the default security group.
> Tip

Table 93: 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.
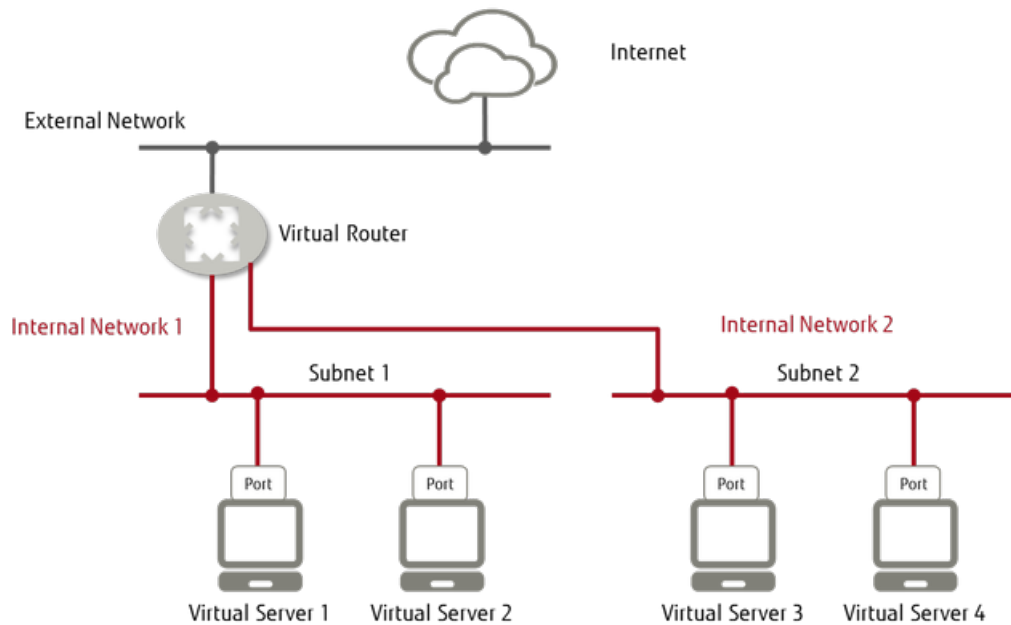
Figure 31: Relationship between an External Network, Internal Networks, and a Virtual Router

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. Otherwise, communication to the Internet will not be possible. In order to specify an external network, use the function for modifying the information of a virtual router after it has been created.

Table 94: 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 95: 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. 💡 **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.

  The SNAT function is only enabled for transmission from resources in the subnets of virtual routers that are connected to external networks. However, for the Eastern Japan Region 2, communication is also possible from resources in the subnets of internal virtual routers that have 2 or more tiers.

  > **Note**
  > - Use of SNAT for IP addresses that are not managed using the IaaS service of FUJITSU Cloud Service for OSS is not supported (For example, IP addresses on a customer's on-premises network that is connected to using the Private Connection function).
  > - When it is necessary to communicate from an unsupported IP address like the one explained above to an external network via a virtual router on the IaaS, it is necessary to prepare a virtual server that has either proxy or NAT functionality, place it in the project, and use it to perform conversion of addresses.

- 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

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 96: 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 97: 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 assignment with DHCP, first create a port at that IP address in advance, and then assign it to a virtual server.
> - With DHCP, IP addresses that were used for ports will be unavailable for use with other ports for a set period of time after the original port has been deleted.

> **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.

> **Note**
> When all of the following conditions are met, an inconsistency will occur in the network interface due to functional restrictions:
> - The OS of a virtual server is CentOS 7.x, RHEL 7.x, or Windows
> - A port is attached after a virtual server is deployed
> - A port is attached while a virtual server is operating
> - A virtual server is restarted (stopped and then started)
>
> If an inconsistency occurs, reconfigure the network from the OS. Also, when attaching an added port, attach it after stopping the virtual server.

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**
> You can assign an IP address only when you create a new port. To change the IP address, use the following procedure:
> 1. Delete the port assigned to the existing IP address.
> 2. Restart the virtual server.
> 3. Specify a new IP address, and re-create the port.
> 4. Assign the re-created port to resources.

> 💡 **Tip**
>
> For a Red Hat Enterprise Linux virtual server or a CentOS virtual server, the network interface is not configured automatically if you add multiple ports when creating a virtual server or if you create an additional port. If necessary, create a network interface settings file on your OS.
>
> Create the settings file according to the following steps.
>
> 1. Log in to the virtual server as an Administrator.
> 2. Create the settings file for the network interface.
> 3. Restart the network services.

<u>Table 98: Creating a Port (List of Items That Can Be Set)</u>

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.	
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 IaaS network.	
List of Security Group IDs	Specify as a list the security groups to be applied to the port.	

---

[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.

Item	Description	Required
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.	

4.3 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 99: List of Global IP Address Settings

Item	Description	Required
External Network ID	Specify the external network ID issued by the system 💡 You can confirm the ID in the list of subnet IDs. Tip	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	

> 🔜 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.
> Note

Changing the Assignment of a Global IP Address

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

Table 100: 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.
The IPsec VPN function is composed of the VPN service and an IPsec site connection.
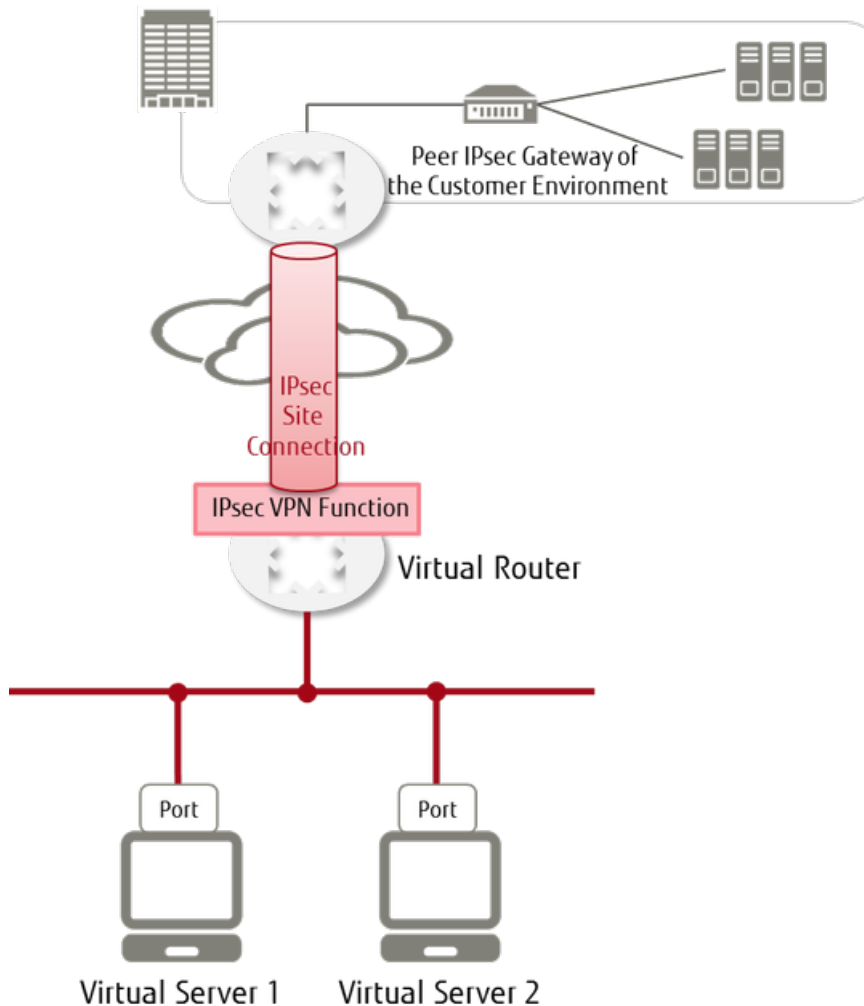
Figure 32: Network Connections Using the IPsec VPN Function

> **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 IPsec gateway.

> **Note** Only one VPN service can be created for a single virtual router. If you want to create multiple IPsec VPN tunnels, create multiple IPsec site connections on a single VPN service.

> **Tip**   Set the global IP address for the port of the virtual router specified when creating the VPN service. The virtual router will use the set global IP address to execute communication for the IPsec site connection.
>
> However, with virtual routers in the Eastern Japan Region 2, it is also possible to use the global IP address of the port used for connection with an external network for communication using an IPsec site connection.

Settings

Table 101: Settings Related to VPN Connections

Item	Supported Methods
Authentication Method	Pre-shared key method
Action When Dead Peer Is Detected	hold, restart
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 102: 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 103: 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. However, firewalls between virtual routers and the peer IPsec gateway must use the same rule settings.

Table 104: List of Allowed Communication Rules

Protocol	Port No.	Description
UDP	500	Internet Security Association and Key Management Protocol (ISAKMP)
UDP	4500	IPsec NAT Traversal

4.5 VPN (SSL-VPN)

4.5.1 SSL-VPN Connection

The SSL-VPN connection function allows you to make secure connections to a virtual environment built on the system, and to log in to the virtual server to perform management operations.
To connect with SSL-VPN, add an SSL-VPN Connection resource to your system maintenance network.

For the procedure for building SSL-VPN connection environments, refer to Connecting to a Virtual Server OS through an SSL-VPN Connection.

> **Important**
> Do not specify the following network addresses in the client address pool for SSL-VPN. If the following network addresses are specified, communication may not be possible.
> - Network addresses that are being used
> - Local network addresses that client PCs are connected to
>
> If communication is not possible, please contact the help desk.

> **Important**
> To connect to the SSL-VPN Connection resource, you need to install an OpenVPN client and configure the settings for SSL-VPN connection.

> **Note**
> - Only one VPN service can be created for a single virtual router. When you establish SSL-VPN connections to multiple subnets, create a virtual router and configure the SSL-VPN function (VPN service and SSL-VPN Connection) for each separate subnet.
> - Configure the gateway address for the subnets that use SSL-VPN connections. Do not delete the configured gateway address while using SSL-VPN.
> - Do not configure a route that would block communication with the gateway address for the host route of the subnets that use SSL-VPN connections.
> - When a virtual server is connected to multiple subnets, including those connected to using SSL-VPN, configure the appropriate route on the virtual server.
>   - In the settings for the default gateway on the OS of the virtual server, configure the gateway of the appropriate subnet.
>   - In the route settings to the subnet configured in the client address pool for SSL-VPN, configure the host route settings so the gateway specified in the subnet of the customer's network for system maintenance is passed through.
> - When creating an SSL-VPN connection, do not delete the static router setting (Nexthop: 192.168.80.4, Destination: Client address pool) automatically added to the virtual router.
> - When updating the certificate for an SSL-VPN Connection resource, update the key metadata container and then create the SSL-VPN Connection resource again.
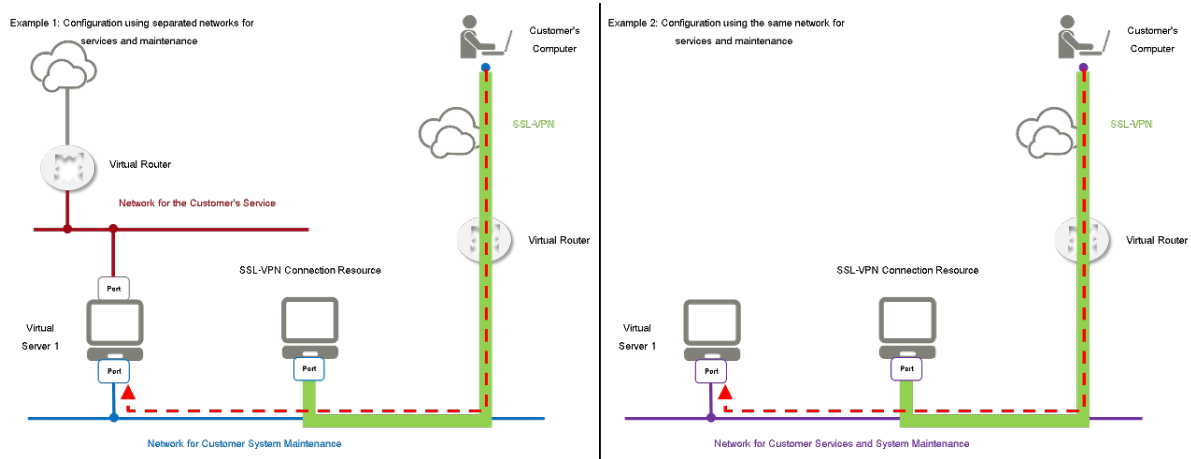
Figure 33: Using SSL-VPN Connection

Related tasks
Setup of an OpenVPN Client (Windows)
Setup of an OpenVPN Client (CentOS)

4.5.2 Relationships with the Firewall Service and Security Group Function

If a firewall is enabled on a virtual router, the relationship with the firewall is as shown below. Although the Allow rules for the SSL-VPN connection are automatically added, you must explicitly configure the firewall service to allow communication such as SSH communication for logging in to a virtual server.

> **Tip**
> - You can configure security group settings for SSL-VPN Connection resources. If you do not configure a security group, the service will automatically use a security group that does not block communication.
> - For "Example 2: Configuration using the same network for services and maintenance", set rules allowing communication from both networks on the firewall and security groups.

An image of the configuration when using the firewall service and the security group function is shown below.
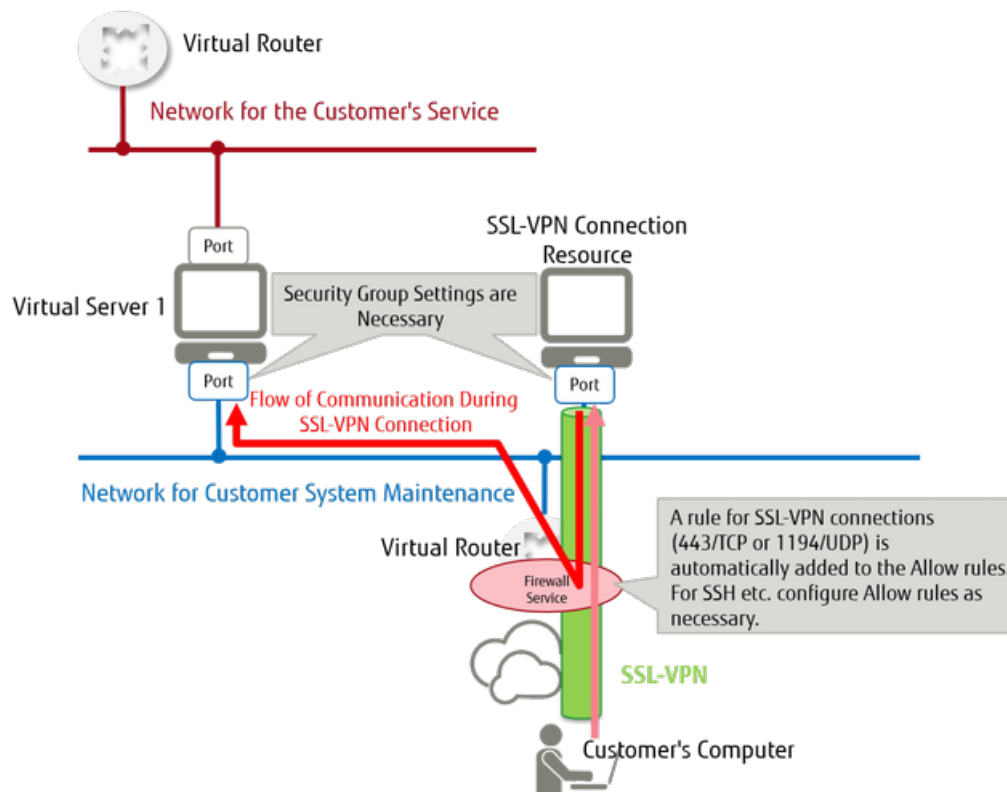
Figure 34: Image of SSL-VPN Communication

When using the firewall service, the following Allow rules are necessary.
- Firewall Rules for an SSL-VPN Connection
- Firewall Rule for Communication after It Passed an SSL-VPN Connection

Firewall Rules for an SSL-VPN Connection

If you create the SSL-VPN Connection resource when a firewall service has already been created, a firewall rule (443/TCP or 1194/UDP) where 'Source IP Address' is set to 'Omit' will automatically be added.

If you create a firewall service after creating an SSL-VPN Connection resource, add this rule manually.

Table 105: Firewall Rules for an SSL-VPN Connection

Source IP Address	Source Port Number	Destination IP Address	Destination Port Number	Protocol
Your computer's IP address (SSL-VPN client)	Omit	IP address of SSL-VPN Connection resources *1	443 or 1194 *2	tcp or udp *2

*1: This is the value specified for 'internal_gateway' on the SSL-VPN Connection resource.

*2: Selected according to the protocol type specified for the SSL-VPN Connection. When setting this manually, set according to the protocol type.
- If the protocol type is 'tcp'
  - Destination Port Number: 443
  - Protocol: tcp
- If the protocol type is 'udp'
  - Destination Port Number: 1194
  - Protocol: udp

> **Tip**: If you want to change a firewall rule, you can do so after creating the SSL-VPN Connection resource.

Firewall Rule for Communication after It Passed an SSL-VPN Connection

Add a rule to explicitly permit communication after it passed an SSL-VPN Connection.

Table 106: Firewall Rule for Communication after It Passed an SSL-VPN Connection

Source IP Address	Source Port Number	Destination IP Address	Destination Port Number	Protocol
Client Address Pool CIDR for SSL-VPN *3	Omit	Virtual server (connection destination server)	Communication protocol used for communication after it passed an SSL-VPN Connection *4	Communication port number used for communication after it passed an SSL-VPN Connection *4

*3: The virtual network CIDR (client_address_pool_cidr) used by the SSL-VPN client of the SSL-VPN Connection resource. For details, refer to "Create SSL VPN V2 Connection" in the "API Reference - Network".

*4: For example, to make an SSH connection to a virtual server, specify the following:
- Destination Port Number: 22
- Protocol: tcp

Security Group Rule for the SSL-VPN Connection

When you configure a security group, the following Allow rule is necessary.

Table 107: Security Group Rule for the SSL-VPN Connection

Direction	Communication Partner	Protocol	Starting Port No.	Ending Port No.
Inbound (Ingress)	Your computer (SSL-VPN client)	tcp or udp *1	443 or 1194 *1	Same value as the one that you specified for the starting port number
Outbound (Egress) *2	Virtual server (connection destination server)	Communication protocol for communication after it passed the SSL-VPN Connection	Communication port number for communication after it passed the SSL-VPN Connection	Same value as the one that you specified for the starting port number

*1: Select according to the protocol type specified for the SSL-VPN Connection.
- If the protocol type is 'tcp'
  - Protocol: tcp
  - Starting Port Number: 443
  - Ending Port Number: 443
- If the protocol type is 'udp'
  - Protocol: udp

- Starting Port Number: 1194
- Ending Port Number: 1194

*2: According to the default rule that is created at the time when you create a security group, all communication in the outbound direction is allowed. To explicitly restrict communication in the outbound direction, delete the default rule and add this rule.

*3: For example, to make an SSH connection to a virtual server, specify the following:

- Protocol: tcp
- Starting Port Number: 22
- Ending Port Number: 22

Related tasks

Setup of an OpenVPN Client (Windows)
Setup of an OpenVPN Client (CentOS)

4.6 Firewall

4.6.1 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.
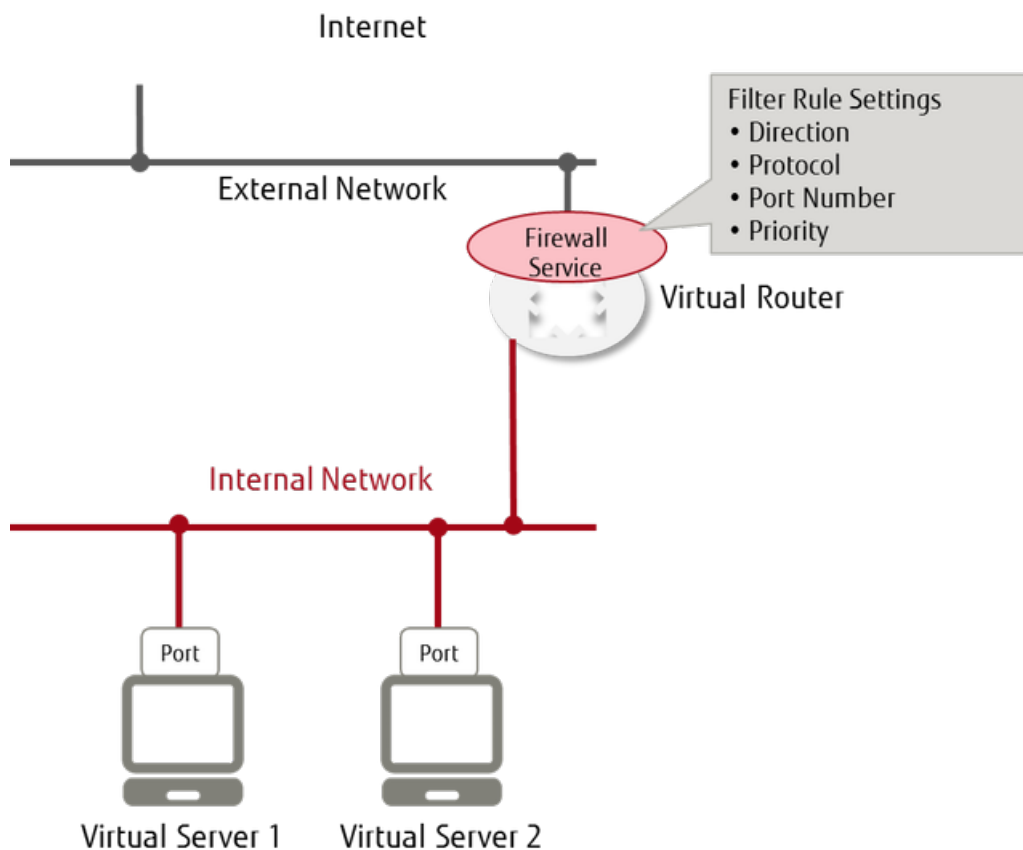
Figure 35: Using the Firewall Service

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 108: List of Firewall Rule Settings

Item	Description	Required
Rule Name	Specify a name for the rule.	
Description	Enter a description.	
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.	

> **Tip**
> • The firewall service provides a stateful firewall.
>   • Only configure allow rules for request packets.
>   It is not necessary to configure allow rules for response packets.
>   • Configure the same communication route of request packets and response packets.
>   If the communication route is not the same, communication will not be possible.
> • When using a combination of a firewall and the NAT function of a virtual router, specify the private IP address corresponding to the global IP address for the IP address
>   The firewall is applied at the following timings:
>   • When communicating from an internal network to the Internet: Before execution of SNAT
>   • When communicating from the Internet to an internal network: After execution of DNAT

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 109: 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 110: 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.	

4.7 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**
> Access the load balancer using the notified FQDN. There is a possibility that the IP address may be changed.

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

Table 111: 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 **Tip** When you create an internal load balancer, the FQDN is registered with the public DNS server (see Appendix), which is provided by one of the common network services. You do not need to manually register the FQDN with the DNS server.	Yes
List of Load Distribution Condition Settings	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.	

Item	Description	Required
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. **Note:** If the host_routes of the subnet has been changed, you must re-create the load balancer. The settings after changing will be reflected after the load balancer has been re-created.	Yes
Grade	Specify one of the following levels of performance for the load balancer: ・ Standard: Standard performance (290 TPS*) ・ Middle: Intermediate performance (580 TPS*) ・ High: High performance (870 TPS*) * Note: The processing performance during SSL communication (2048-bit key length) (The unit is TPS: Transactions Per Second). These performance values were measured in the Fujitsu evaluation environment. Performance varies depending on the operating environment and other factors. There is no guarantee for a certain level of performance. **Note:** Based on the grade of the load balancer performance, the following numbers of IP addresses are necessary for each subnet. Perform configuration so the necessary number of IP addresses can be secured. ・ Standard: 4 ・ Middle: 8 ・ High: 12	

Operations on a Load Balancer

・ Adding/Deleting a Target for Load Distribution
・ Multi-Availability Zone Distribution
・ Monitoring for Abnormality on a Load Distribution Target

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 112: 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 Policies to be Created	100 per load balancer

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.

It is possible to specify the SSL certificate used for HTTPs communication and SSL communication in a listener.

> **Note**
> To use an SSL certificate, you must use the Key Management Function or the Registering Server Certificates Used by Load Balancers to register the certificate in advance.
>
> For the private key, register the key decrypted using a passphrase.

Table 113: List of Listener Settings

Item	Description	Required
Protocol	Specify the front-end and back-end communication protocols. **Tip** Only the following combinations can be specified: • HTTP - HTTP *1 • HTTPS - HTTP *1, *2 • HTTPS - HTTPS *1, *2 • TCP - TCP • SSL - TCP *2 • SSL - SSL *2 *1: The HTTP keep-alive time is one second. *2: For information about supported SSL protocols and SSL cipher suites, refer to Appendix "Predefined Security Policies".	Yes
Front-end Port No.	Specify the front-end port number (1 - 65535).	Yes

Item	Description	Required
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. **Tip** For the method for registering the server certificate of the load balancer with the key management function, refer to Registering Server Certificates Used by Load Balancers.	

Managing Listener Policies

You can register, modify, and delete the policies that are applied to a listener. You can create a maximum of 100 policies per load balancer. 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.
> - You can specify a single policy per load balancer.

Specify the following settings to register the session persistence policy:

Table 114: 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 there is no virtual server that is available for load distribution.

> **Note**
> This policy can be applied only if an HTTP/HTTPS listener is specified.

Specify the following settings to register the sorry page redirect policy:

Table 115: 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. > **Note** > The name must be unique in the load balancer.	Yes
Redirect Destination URI	Specify the URI for the redirect destination. > **Tip** > This is set as the Location information for redirect responses.	Yes

・Security policy

This policy specifies the SSL protocol that is applied when HTTPS or SSL is specified as a protocol in the Listener Settings.

> **Note**
> You can specify a single policy per load balancer.

Specify the following settings to register or to modify a security policy:

Table 116: List of Security Policy Settings

Item	Description	Required
Load Balancer Name	Specify the name of the load balancer for which to configure the security policy.	Yes
Enable SSL Protocol (list of attributes related to policy name)	Enable (true) or disable (false) SSL separately for each protocol. The SSL protocols that can be configured are as follows: ・SSL 3.0 (default setting: disabled) ・TLS 1.0 (default setting: disabled) ・TLS 1.1 (default setting: enabled) ・TLS 1.2 (default setting: enabled) > **Tip** > ・Specify whether to enable (true) or disable (false) SSL for each SSL cipher suite. For information about the SSL cipher suites that can be specified for each SSL protocol, refer to Appendix Predefined Security Policies. > ・The DH private key length used when performing TLS communication is 1024 bit.	Yes

Item	Description	Required
Policy Name	Specify the name of the security policy to create. **Note** The name must be unique in the load balancer.	Yes
Policy Type	Specify the following policy type: • SSLNegotiationPolicyType A policy related to the SSL encryption protocol. This policy can be set to listeners where the protocol that is set to "Protocol" begins with HTTPS or SSL.	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.

Important The load distribution algorithm for virtual servers is the "less connections" algorithm.

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.

Important Before you add a virtual server to target for load distribution, the virtual server must be in an operating state.

Warning 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. When operations which involve changing of the IP address of a virtual server targeted for load distribution such as the examples below are performed, delete the target virtual server from the load distribution targets, and register it again.

Operation Examples:

• Rebooting of a virtual server targeted for load distribution while DHCP is enabled
• Manual changing of the IP address, by a user, of a virtual server targeted for load distribution while DHCP is enabled

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.

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.
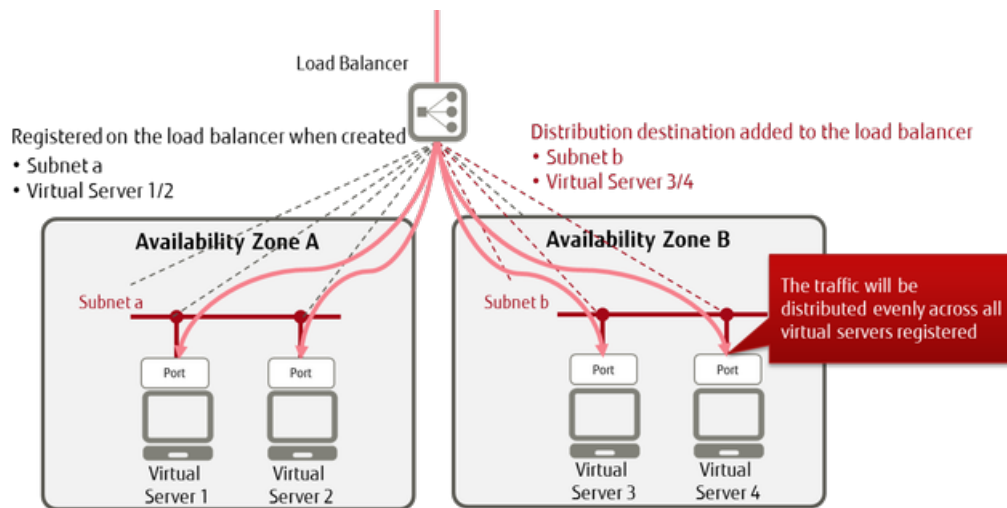
Figure 36: Load Distribution when Connecting Multiple Availability Zones

---

| ⓘ Important | Resolving the name of the FQDN of a load balancer that can handle multi-availability zone distribution returns the IP addresses of all load balancers in both of the availability zones. |
| | When a failure occurs in one of the availability zones, it will not be possible to connect to the load balancer of the availability zone where the failure has occurred. It is necessary to take preventative action such as using a library on the client side that processes retrying of http connections, so that when a failure occurs the connection destination is switched to the load balancer of the unaffected availability zone. |

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 117: 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 one of TCP, HTTP, HTTPS, and SSL • 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

💡 **Tip** The health monitor function of load distribution performs health checks at the specified interval. If a request returns an error even before a failure is determined using a health check, the request will be resent to another virtual server that is the target of load balancing.

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 desk for assistance.
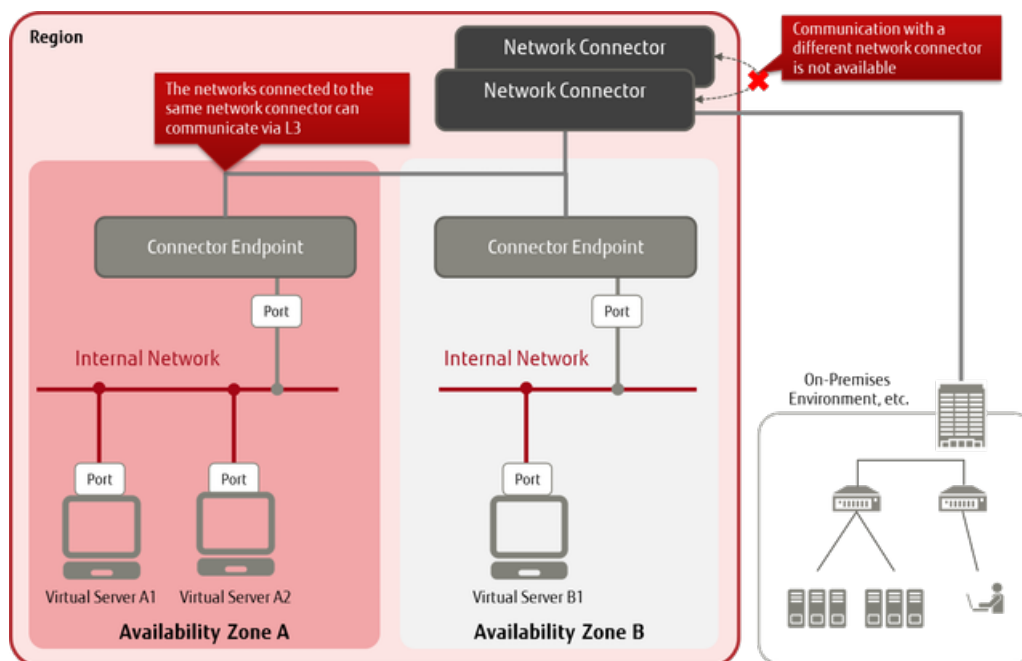
Figure 37: Using the Network Connector Service

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 118: 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

Item	Description	Required
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 119: 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 120: 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 IaaS network	Yes
Creation Destination Information	Specify the following values according to the type specified above. • For "availability_zone": Specify the name of the availability zone where the network to which the connector endpoint connects exists.	Yes
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 121: 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:

- Overview of Functions
- Building a Database
- Managing a Database

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.
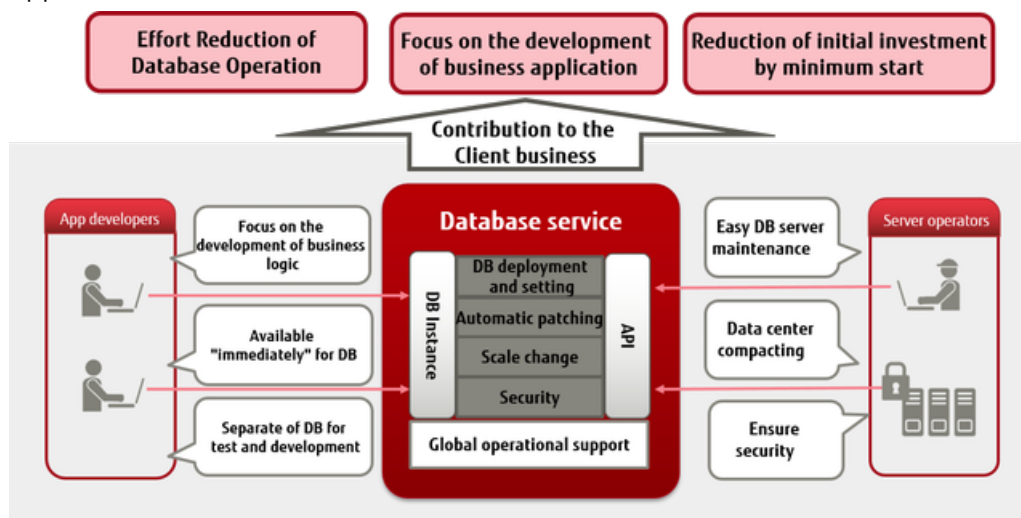
Figure 38: Value Provided By Database as a Service

Available Database Engines

Shown below is the compatibility information from the application perspective regarding database engines that are provided by this service. Use this service with applications intended for the products of the version levels included in the following table.

Table 122: Compatibility Information for Database Engines

Product Name	Version / Level	Remarks
Enterprise Postgres	9.6	Equivalent to PostgreSQL 9.6
Symfoware Server	12.1	Equivalent to PostgreSQL 9.2

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.
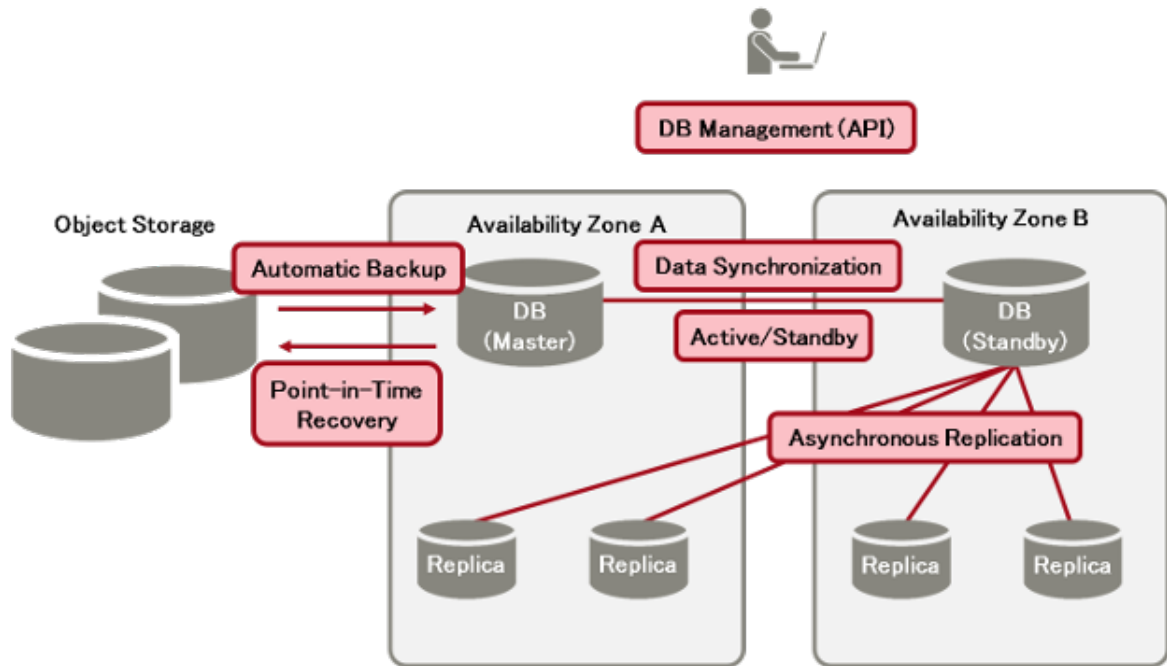
Figure 39: Overall Layout of Database as a Service

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 123: List of Provided Virtual Server Types (Flavors) (Standard CPU)

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

Type Name	Number of Virtual CPUs	Memory (GB)
M-1	1	8
M-2	2	16
M-4	4	32
M-8	8	64
M-16	16	128
XM-4	4	128
LM-1	1	16
LM-2	2	32
LM-4	4	64
LM-8	8	128
L-12	12	128
L-24	24	128

Table 124: List of Provided Virtual Server Types (Flavors) (High-Speed CPU)

Type Name	Number of Virtual CPUs	Memory (GB)
C2-2	2	4
C2-4	4	8
C2-8	8	16
C2-16	16	32
S2-1	1	4
S2-2	2	8
S2-4	4	16
S2-8	8	32
S2-16	16	64
M2-1	1	8
M2-2	2	16
M2-4	4	32
M2-8	8	64
M2-16	16	128
XM2-4	4	128
LM2-1	1	16
LM2-2	2	32
LM2-4	4	64
LM2-8	8	128
L2-12	12	128
L2-24	24	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 125: List of Disk Types

Type	Purpose
Standard (type M1)	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

> **Tip** The following are included in the disk capacity used as the data area.
> - The user data area of the PostgreSQL database
> - The system data area of the PostgreSQL database
> - The engine log area
> - The transaction log area
> - Temporary files such as sorts

Redundancy Settings

- Multi-DB option (Enable or Disable)
- Multi-AZ option (Enable or Disable)

Table 126: Combination of Redundancy Settings

		Multi-DB Option		Note
		Disable	Enable	
Multi-AZ Option	Disable	✓	✓	The standby virtual database server is created within the same availability zone, according to the multi-DB option setting. **Important** If the region has only one availability zone, be sure to specify "Disable".
	Enable	-	✓	The standby virtual database server is created within another availability zone. **Important** If "Enable" is specified for the multi-AZ option, be sure to specify "Enable" for the multi-DB option as well.

After the standby virtual database server is created, data is duplicated from the active server to the standby server synchronously, which ensures data redundancy.

> **Note**
> - Data is duplicated from the data area connected to the virtual database server, on a per-data area basis.
> - Data cannot be read from the standby server.
> - As data is duplicated synchronously, write performance may be affected compared to when the redundancy settings are disabled.

Automatic Backup Settings

Configure automatic backup settings to perform a daily full backup of data and configuration files on the virtual database server. Items that you can specify are as follows.

Table 127: 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

If automatic maintenance is set, maintenance (setting modifications of the database virtual server that require restarting) will 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 128: 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

However, in automatic maintenance, updating of security and application of software patches are not performed. When performing application of patches, refer to Applying Patches to Database Virtual Servers.

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 129: Database Settings

Item	Description
Master user name	Specify the database management user name
Master user password	Specify the password for the database management user

Item	Description
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.
- The TCP timeout value of virtual database servers is one hour. This value cannot be changed.
- In the database service, the checksum functions of database engines are enabled.

5.2.2 DB Subnet Groups

Create the network information that is used to create and control virtual database servers 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 130: 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 - 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

Item	Description	Required
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 131: 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 ➡ **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	

Item	Description	Required
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 virtual database server.
Since the parameters you can specify depend 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 132: 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: • enterprisepostgres_v9.6 • symfoware_v12.1	Yes

Item	Description	Required
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 133: Each Parameter Item That Can Be Checked

Item	Description
Parameter name	Check the parameter names that can be specified.
Parameter value	Check the current setting value that corresponds to the parameter name.
Parameter value range	Check the range of values that can be parameter values.
Parameter application method	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 virtual database server is restarted.
Parameter data type	Check the data type of the parameter value (example: Integer, String).

Item	Description
Description	Check the description of the parameter.
Flags that indicate changeability	Check whether or not the parameter value can be changed. "FALSE" indicates that it cannot be changed
Lowest version that supports the parameter	Check what the lowest version that supports the parameter in the parameter group family is.
Source of the default value	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 IaaS system

Changing a DB Parameter Value

In order to change the parameter value to be set on the database, include in the DB parameter group the parameter that you want to modify, and modify the DB parameter group information. You cannot modify parameter values by specifying only individual parameters.

Table 134: 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 timing are available: • immediate: The value is applied immediately • pending-reboot: The value is applied when the virtual database server 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

The settings specified when virtual database servers are created can be changed later. As shown in the following table, you may need to restart the virtual database servers in order to apply the changed settings.

Table 135: Settings That Can Be Changed

Settings	Description	Restarting of Virtual Database Servers
Database engine version	Changes the version of the database engine	Necessary
Virtual database server type	Changes the virtual database server type	Necessary
Database capacity expansion, or changing of disk type	Increases the data block storage capacity, or changes the disk type	Necessary
Redundancy settings	Changes the redundancy settings of virtual database servers	Not necessary
Security group settings	Changes the security group information that is set on virtual database servers	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 **Note** Restarting is not necessary when you change the setting, but restarting is carried out when you perform maintenance.

Settings	Description	Restarting of Virtual Database Servers
Automatic minor version upgrade	Changes whether or not to perform a minor version upgrade of the database engine automatically	Not necessary Note Restarting is not necessary when you change the setting, but restarting is carried out when you upgrade.

Starting/Terminating/Restarting a Virtual Database Server

You can start up, terminate, or restart a virtual database server. When you restart a virtual database server, the operation varies depending on whether the redundancy settings are "Enable" or "Disable."

・When the redundancy settings are "Enable"

Failover takes place, then restarting is carried out.

・When the redundancy settings are "Disable"

Normal restarting is carried out. (The server stops for approximately 10 minutes.)

Applying Patches to Database Virtual Servers

When patches are database engine patches or security updates are released, it is possible to apply patches. It is necessary to reboot database virtual servers in order to apply patches. For the parameters, etc. when rebooting, refer to "Restart virtual database server" in the "API Reference - Application Platform Service".

Deleting a Virtual Database Server

Take one of the following actions and then delete the virtual database server:

・Create a DB snapshot before deletion

Tip If you create a DB snapshot before you delete a database server, you can create a new database server by restoring the DB snapshot that contains the database 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 136: Settings for Monitoring

Item		Description
Check interval		10 minutes
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

Item	Description
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 refer to PostgreSQL engine logs.

> **Note** Log files are rotated every day. 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 statement for reference.

DB Snapshot Management

You can create a DB snapshot of a virtual database server at a specific point in time, and create a new virtual database server by using the DB snapshot. Following functions related to DB snapshots are provided:

· Creation of a DB snapshot
· List display of a DB snapshot
· Information display of a DB snapshot
· Duplication of a DB snapshot
· Deletion of a DB 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.

<div align="center">Table 137: List of Events</div>

Source Type	Event Types	Description
db-instance	availability	Starting/termination/restarting of a database virtual server (includes restarting due to the failover option)

Source Type	Event Types	Description
	backup	Creation of a DB snapshot, Starting or stopping of an automatic backup
	configuration change	Modification of a database virtual server
	creation	Creating a virtual database server
	deletion	Deleting a virtual database server
	failover	Start and completion of failover
	failure	When the status of a parameter value of a DB parameter group is abnormal
	low storage	When over 80% of the allocated storage is being used
	maintenance	When performing security updates or minor version updates of database virtual servers
	recovery	Restoration of virtual database servers
	restoration	When restoring a database virtual server from a point-in-time or a DB snapshot
	read replica	Reading of a replica
db-snapshot	creation	Creation of a DB snapshot, Creation of an automatic backup
	deletion	Deletion of a DB snapshot
	notification	Duplication of a DB snapshot
	restoration	Restoration of a database virtual server from a DB snapshot

Transparent Data Encryption

Using the transparent data encryption function makes it possible to encrypt the data stored in databases. For details, refer to the Database Service User Guide.

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 138: 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_isready	Checks the connection status of a server (*1)
pg_recvlogical	Controls the logical decoding of a stream (*1)
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

Note 1: Not usable when the database engine is Symfoware Server.

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 139: 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 EVENT TRIGGER	Changes the definition of an event trigger (*2)
ALTER EXTENSION	Changes the definition of an extension
ALTER FOREIGN TABLE	Changes the definition of an external table (*2) (*3)

SQL Statement	Purpose
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 MATERIALIZED VIEW	Changes the definition of a materialized view (*2)
ALTER OPERATOR	Changes the definition of an operator
ALTER OPERATOR CLASS	Changes the definition of an operator class
ALTER OPERATOR FAMILY	Changes the definition of an operator family
ALTER POLICY	Changes rows of the definition of a security policy (*2)
ALTER ROLE	Changes a database role (Note 1)
ALTER RULE	Changes the definition of a rule (*2)
ALTER SCHEMA	Changes the definition of a schema
ALTER SEQUENCE	Changes the definition of a sequence generator
ALTER SERVER	Changes the definition of an external server (*2) (*3)
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 USER MAPPING	Changes the definition of a user map (*2) (*3)
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

SQL Statement	Purpose
COMMIT PREPARED	Commits a transaction that was earlier prepared for two-phase commit
COPY	Copies data between a client and a database table (Note 4)
CREATE AGGREGATE	Defines a new aggregate function (Note 5)
CREATE CAST	Defines a new cast (Note 5)
CREATE COLLATION	Defines a new collation
CREATE CONVERSION	Defines a new encoding conversion (Note 5)
CREATE DATABASE	Creates a new database (Note 6)
CREATE DOMAIN	Defines a new domain
CREATE EVENT TRIGGER	Defines a new event trigger (*2)
CREATE EXTENSION	Installs an extension
CREATE FOREIGN TABLE	Defines a new external table (*2) (*3)
CREATE FUNCTION	Defines a new function (Note 1) (Note 7)
CREATE GROUP	Defines a new database role
CREATE INDEX	Defines a new index
CREATE MATERIALIZED VIEW	Defines a new materialized view (*2)
CREATE OPERATOR	Defines a new operator (Note 5)
CREATE OPERATOR CLASS	Defines a new operator class (Note 5)
CREATE OPERATOR FAMILY	Defines a new operator family
CREATE POLICY	Defines new rows of a security policy in a table (*2)
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 SERVER	Defines a new external server (*2) (*3)
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 8)
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 5)
CREATE TEXT SEARCH TEMPLATE	Defines a new text search template (Note 5)

SQL Statement	Purpose
CREATE TRIGGER	Defines a new trigger (Note 5)
CREATE TYPE	Defines a new data type (Note 5)
CREATE USER	Defines a new database role
CREATE USER MAPPING	Defines a new user map of an external server (*2) (*3)
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 EVENT TRIGGER	Removes a defined event trigger (*2)
DROP EXTENSION	Removes a defined extension
DROP FOREIGN TABLE	Removes a defined external table (*2) (*3)
DROP FUNCTION	Removes a defined function
DROP GROUP	Removes a defined database role
DROP INDEX	Removes a defined index
DROP MATERIALIZED VIEW	Removes a defined materialized view (*2)
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 POLICY	Deletes rows of a security policy from a table (*2)
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 SERVER	Deletes the descriptor of an external server (*2) (*3)
DROP TABLE	Removes a defined table

SQL Statement	Purpose
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 USER MAPPING	Removes the user map of an external server (*2) (*3)
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
IMPORT FOREIGN SCHEMA	Imports a table definition from an external server (*2)
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
REFRESH MATERIALIZED VIEW	Converts the content of a materialized view (*2)
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

SQL Statement	Purpose
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: Not usable when the database engine is Symfoware Server.

Note 3: You can only use postgres_fdw as an external wrapper.

Note 4: You cannot specify any file names for FROM and TO. Specify STDIN or STDOUT.

Note 5: If you specify a function, you can only specify a function that is implemented in SQL or the plpgsql language.

Note 6: You cannot specify the ENCODING clause.

Note 7: You can only specify the languages SQL, internal, or plpgsql for LANGUAGE.

Note 8: 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.

- You cannot use the following SQL statements that are available in PostgreSQL:
  - ALTER FOREIGN DATA WRAPPER
  - ALTER LANGUAGE
  - ALTER SYSTEM
  - CREATE FOREIGN DATA WRAPPER
  - CREATE LANGUAGE
  - DROP FOREIGN DATA WRAPPER
  - DROP LANGUAGE
  - LOAD
- The operation for parallel searches of the database service is the same as for PostgreSQL.
  - In the database service it is not possible to use the "CPU resource availability checking" function provided by the product version of Enterprise Postgres.

    The "CPU resource availability checking" function is the function that controls server slowdown due to excessive parallel searches.

5.3.3 Database User

When you create a virtual database server, create the database management user and the system user as well.

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

When changing the password for the database management user, use the API for changing database virtual servers. If the database management user is deleted or modified without using the API, there will be serious effects on operation. Do not perform deletion or modification.

System User

When you create a virtual database server, a system user (cloud-user) is created to enable operation from the system. The following privileges are granted to the system user:

- superuser
- create role
- create db
- replication

The system user cannot be used to connect to databases of the virtual database server from a DB client.

If the system user is deleted or modified, there will be serious effects on operation. Do not perform deletion or modification.

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 virtual database 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:

・DB Snapshot

Snapshot of a database virtual server that was taken at a point in time chosen by the user. The following data is included in snapshots.

・The entire backup data of the database virtual server at the point in time when the snapshot was created
・The transaction logs output between the start and end of the backup process

DB snapshots are retained until deleted by the user.

> **Tip**
> DB snapshots are taken in the hot backup format.

・Automatic Backup

The following data that was acquired based on the automatic backup conditions that you set when you created the database virtual server:

・The entire backup data of the database virtual server that was acquired at the time set for automatic backup
・Transaction logs, which are backed up at 5-minute intervals (fixed)

Automatic backup data is retained for the set retention period. When the retention period is exceeded, automatic backup data is automatically deleted.

> **Tip**
> ・The automatic backup data is given a name that complies with the following naming conventions:
> ```
> auto-snapshot-<virtual database server ID>-<year>-<month>-<day>-<hour>-
> <minute>-<second>
> ```
> ・Automatic backups are taken in the hot backup format.
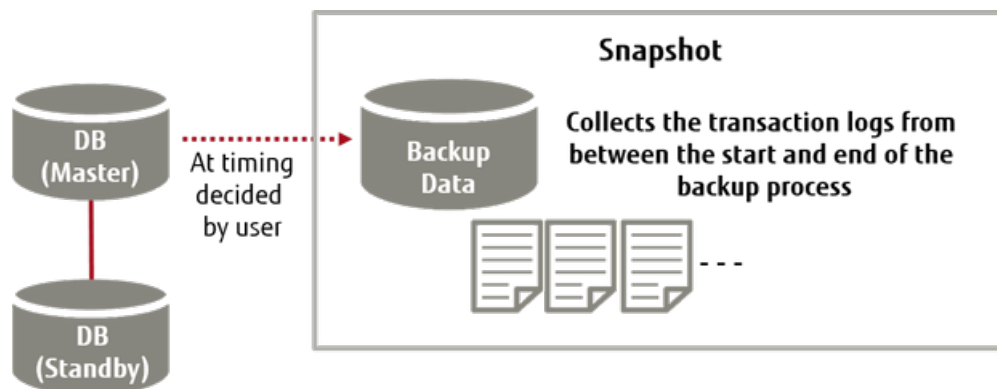
Figure 40: Snapshot
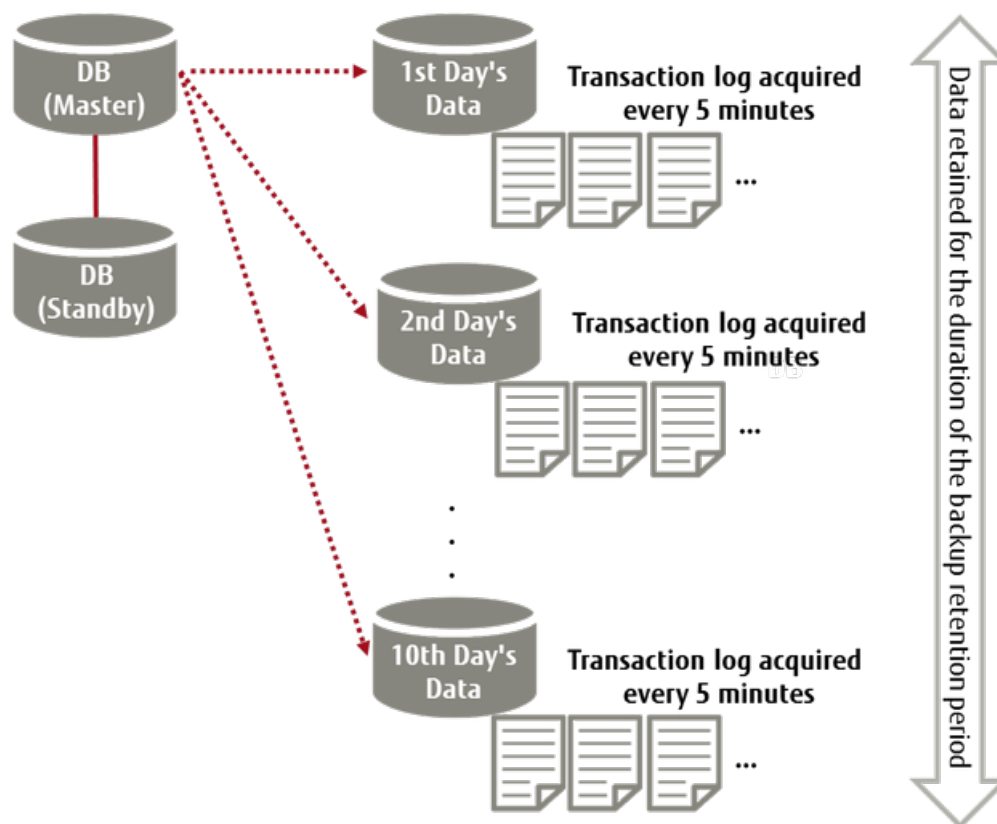
Figure 41: Automatic Backup

Database Recovery Method

There are two methods of recovering databases, as shown below:

- Restoring from a DB Snapshot

  Recover the database by using a DB snapshot that was acquired at a specific point in time.

- Point-in-time recovery

  Recover the database by using automatic backup data. It is possible to specify any "date and time" in the period between when the backup was created (a maximum of 10 days earlier) and when the latest transaction log was obtained (at maximum 5 minutes prior).

> **Important**
> The restoration destination will be a new virtual database server. Confirm that there is no problem with the recovered data before you delete the old virtual database server.

- 181 -

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. • You can recover the database only in the same region where the data that will be used for recovery exists.

Part 6: DNS Service

Topics:

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.
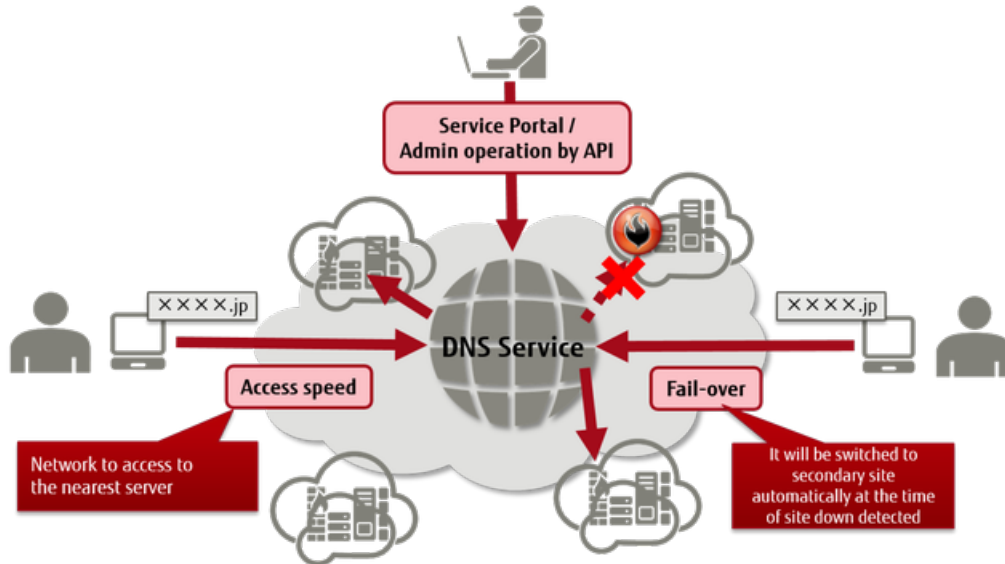
Figure 42: Overall Layout of the Functions Provided by the DNS Service

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.

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.

> **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 140: 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 141: 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

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)
- PTR
- SRV

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

Limiting Values

Table 142: 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, LBR, PTR, SRV
Record Type with Wildcard Support	A, AAAA, MX, CNAME, TXT

Table 143: List of Limiting Values for DNS Record Entries

Record Type	Item	Limitations	Required
A	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Available character type: Alphanumeric characters and dots (.) Must be a valid IPv4 address	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	

Record Type	Item	Limitations	Required
	Weight	0 - 100 Available character type: Numeric characters	*1
	Health Check IP Address	Length: 1 - 32 characters Alphanumeric characters and dots (.)	*2
	Health Check Port No.	Length: 1 - 5 characters Available character type: Numeric characters	*2
	Health Check Host Name	Length: 0 - 255 characters Available character type: Single-byte characters	*3
	Health Check Path	Available character type: Single-byte characters Only omittable when failover is selected in the policy	*3
AAAA	Record Name	Length: 1 - 63 characters Alphanumeric characters, hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Alphanumeric characters and colons (:) Must be a valid IPv6 address	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
	Weight	0 - 100 Available character type: Numeric characters	*1
	Health Check IP Address	Length: 1 - 32 characters Available character type: Alphanumeric characters and dots (.)	*2
	Health Check Port No.	Length: 1 - 5 characters Available character type: Numeric characters	*2
	Health Check Host Name	Length: No more than 255 characters Available character type: Single-byte characters	*3
	Health Check Path	Available character type: Single-byte characters	*3
CNAME	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, hyphens (-), and wildcards (*)	Yes

Record Type	Item	Limitations	Required
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
MX	Record Name	Length: 1 - 63 characters Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)	Yes
	Priority	0 - 64000 Available character type: Numeric characters	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
TXT	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, underscores (_), hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Alphanumeric characters, single-byte spaces, and single-byte symbols other than double quotation marks (")	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
NS	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters and hyphens (-)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	

Record Type	Item	Limitations			Required
	Value	Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)			Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters			
LBR	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters and hyphens (-)			Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters			
PTR	Record Name	Character type: Alphanumeric characters, dots (.), and hyphens (-)			
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority			
	Value	Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)			Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters			
SRV	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), and underscores (_) Specify using the "_<Service Name>._<Protocol Name>" format (Example: _ftp._tcp)			Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority			
	Value	Specify the priority, the weight, the port number, and the target in this order, separating the values with blank spaces			Yes
		Priority	0 - 64000 Available character type: Numeric characters		Yes
		Weight	0 - 65535 Available character type: Numeric characters		Yes
		Port No.	0 - 65535 Available character type: Numeric characters		Yes

Record Type	Item	Limitations		Required
		Target	Length: 1 - 255 characters	Yes
			Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)	
			Specify using the format "<Record name of A record>.<Domain name>"	
			Tip — When the record name of the A record is "ftp-server-01" and the domain name is "example.com": Set it as "ftp-server-01.example.com"	
	Memo	Length: No more than 255 characters		
		Available character type: Double-byte characters		

*1: A required item when weighting has been selected using the policy.

*2: A required item when failover has been selected using the policy.

*3: An optional item when failover has been selected using the policy.

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.
- Only the global IP (FloatingIP) provided by this service can be set as the record name for PTR. When setting a record name it is necessary to obtain the global IP in advance.
- For details on reverse DNS lookup, refer to How to Use Reverse DNS Lookup.
- For the target value of the SRV record, specify the record name of the A record in the same zone and the domain name.
- The weighting in SRV records is not handled as the weighting of weighted round robin functions.

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 the abnormality occurred is blocked.

Table 144: 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 145: 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 HTTPS is selected for the protocol. This cannot be changed.

Health Check Rules

- The individual health checks that are specified for each record are run.
- Health check is performed at 5-minute intervals.
- During a health check, a check of whether packets can be sent to the target server via the Internet is performed.
- When a failover occurs, a host switches over to the other host in the group that has the same Name tag and same Type tag.
- Ensure that all the same record name is used for all records in the same group.
- Set a global IP address as the target IP address.
- Configure the network and OS (firewall service, security group rules, OS firewall, etc.) so that packets reach the target IP address.
- If multiple records are specified for [Secondary], priority is given to the record that was registered first.
- Health checks are normally only performed for primary servers.
- If an abnormality occurs in a health check for [Primary], health checks will be performed for both [Primary] and [Secondary].
- The relationships of the server statuses of [Primary] and [Secondary] and the allocation destinations are as follows.

Table 146: Relationships of the Statuses of [Primary]
and [Secondary] and the Allocation Destinations

Statuses of [Primary] and [Secondary]		Allocation Destination
Primary	Secondary	
✓	✓	Primary
✓	-	Primary
-	✓	Secondary
-	-	Depends on the statuses of both before health check abnormalities
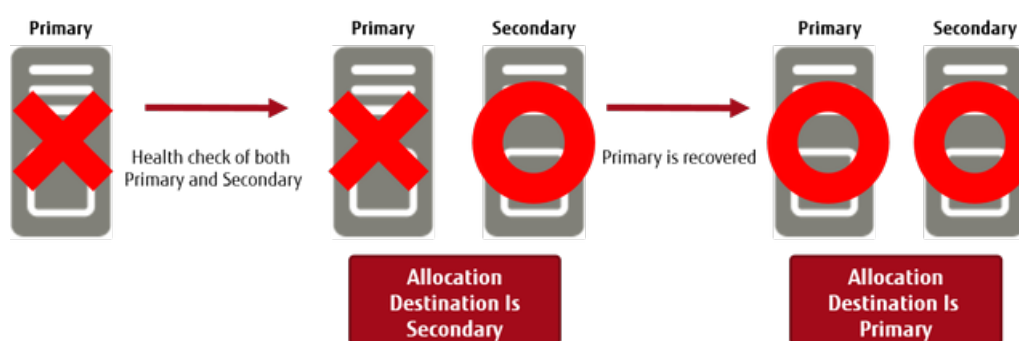
Figure 43: Allocation Destinations of Health Checks

- When abnormalities occur in health checks of both the primary and the secondary, the allocation used before the abnormality will continue to be used until either of them is recovered.
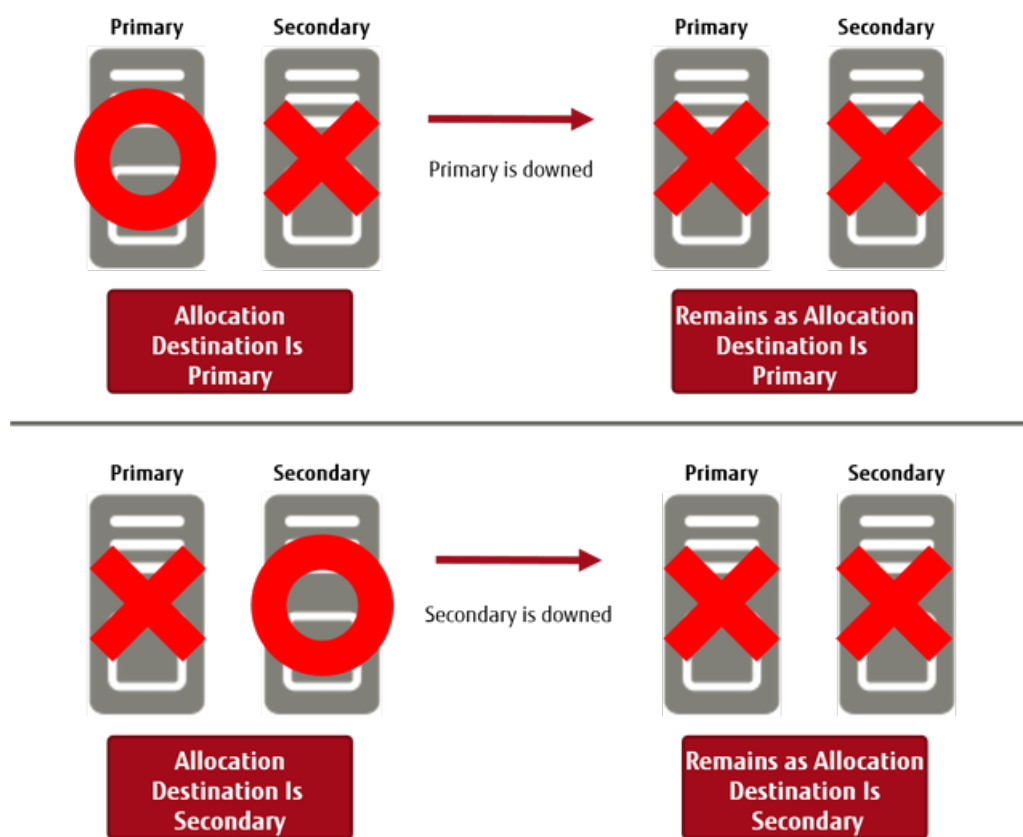
Figure 44: Allocation During Abnormality on Primary or Secondary

Points to Note

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

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.

<div align="center">Table 147: Latency-Based Routing Settings</div>

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.

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 148: 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.

Part 7: Email Delivery Service

Topics:

IaaS provides an email delivery service.

7.1 Overview of Functions

7.1.1 Email Delivery Service

FUJITSU Cloud Service for OSS 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.
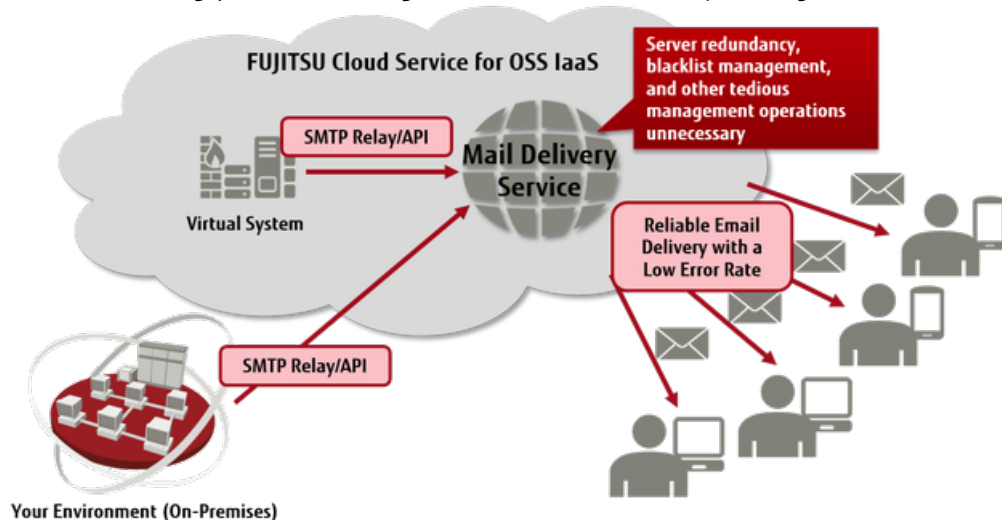
Figure 45: Overall Layout of the Email Delivery Service

Usage Value

The following can be realized using the email delivery service.

- Email is stored temporarily by the email delivery service and then sent asynchronously. Unlike when a mail server has been configured, the act of sending is completed when the email delivery service receives the email, and the sender does not need to wait until email has been sent to all of the target addresses. This is particularly useful when sending large amounts of email.
- There are two interfaces for sending email: SMTP relay and APIs. It is possible to select the interface that best suits the customer's environment.
- As optimum and efficient sending control is performed, it is possible to reduce the number of errors related to the sending method.

Functions Included

- Sending settings
  - Sender domain registration
  - Sender email address settings
- 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

7.2 Settings

7.2.1 Sending Settings

There are the two following methods for registering users with the email delivery service.
- Register a sender domain
- Register email addresses of senders

For the registration methods, refer to "Verify domain (POST /)" and "Verify email address (POST /)" in the "API Reference - Application Platform Service".

> **Tip**
> If a sender domain is registered, it is not necessary to register individual email addresses belonging to that domain.

You can specify only registered domains and email addresses as the From address (Envelope From and Header From).

Table 149: 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)

> **Note**
> • When registering a sender domain, registration is completed by configuring the value of the authentication token included in responses in the TXT record of the DNS server. At that time, use "_niftycloudess.<name_of_the_domain_to_register>" as the name of the TXT record to register.
> • Domains normally become usable approximately 10 minutes after being registered.

7.3 Mail Delivery

7.3.1 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.

<div align="center">Table 150: Connection Information</div>

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.

For details, refer to Email delivery service in the IaaS API Reference.

7.3.2 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 must be specified in 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.

7.4 Email Certificate

7.4.1 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 151: Settings for SPF Records

Setting Target	Settings
Record Type	TXT
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"

7.5 Monitoring

7.5.1 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 152: Items That Can Be Monitored

Item	Description
Emails Sent	This is the total number of emails that have been sent.
Bounces	This is the total number of emails that were not delivered and returned to the sender.
Emails Refused	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.
- 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
- The number of emails refused is the number of emails for which 400 or 500 error codes were returned from the incoming mail server at the destination.

Part 8: Content Delivery Service

Topics:

This service uses edge servers provided by AKAMAI to deliver content around the world.

8.1 Overview of Functions

8.1.1 Content Delivery 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. Users configure an origin server, and then perform settings for content delivery. It is possible to specify a virtual server, a load balancer, object storage, and other computing resources as an origin server.
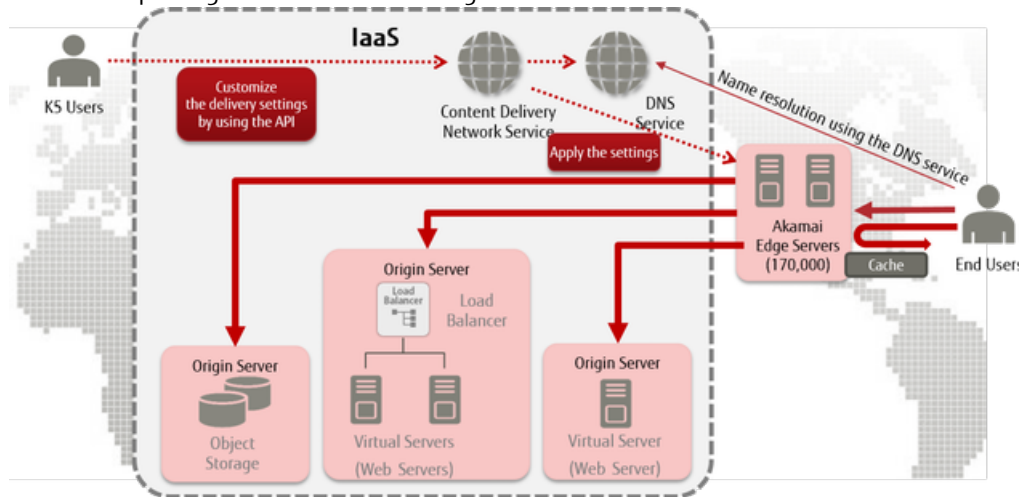
Figure 46: Overall Image of Content Delivery Service

Functions Included

- Acquiring the Delivery Settings List

  Acquire a list of delivery settings that can be set for your project.

- Creating Delivery Settings

  Create delivery settings to start content delivery.

- Acquiring Delivery Settings

  Specify the ID of the delivery settings you have created, to acquire the content for those delivery settings.

- Editing Delivery Settings

  Specify the ID of the delivery settings you have created, to edit the content for those delivery settings.

- Deleting Delivery Settings

  Specify the ID of the delivery settings you have created, to delete those delivery settings.

- Purging Cache

  Specify a delivery settings ID that you have created to purge cached content from an edge server.

- Access Control

  By requiring verification (authorization) for cache content it is possible to restrict delivery to users. Specifically, by distinguishing between IP addresses, Cookie referers, User-Agents, and regions (countries) and configuring authorization tokens, it is possible to restrict access and also determine whether to approve or deny access.

- Creating a Report

  Create statistical information from the total amount for each of the delivery settings that have been created within the range of your project.

- Acquiring a Report

  Acquire statistical information that was created with the Create Report function in json format.
- Acquiring an Access Log

  Store edge server access logs in a container that you created in object storage.

Content That Can Be Delivered

Table 153: 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 caching behavior control rules that follow the cache settings to control whether cache is allowed on the origin server. For details, refer to the API Reference Manual.
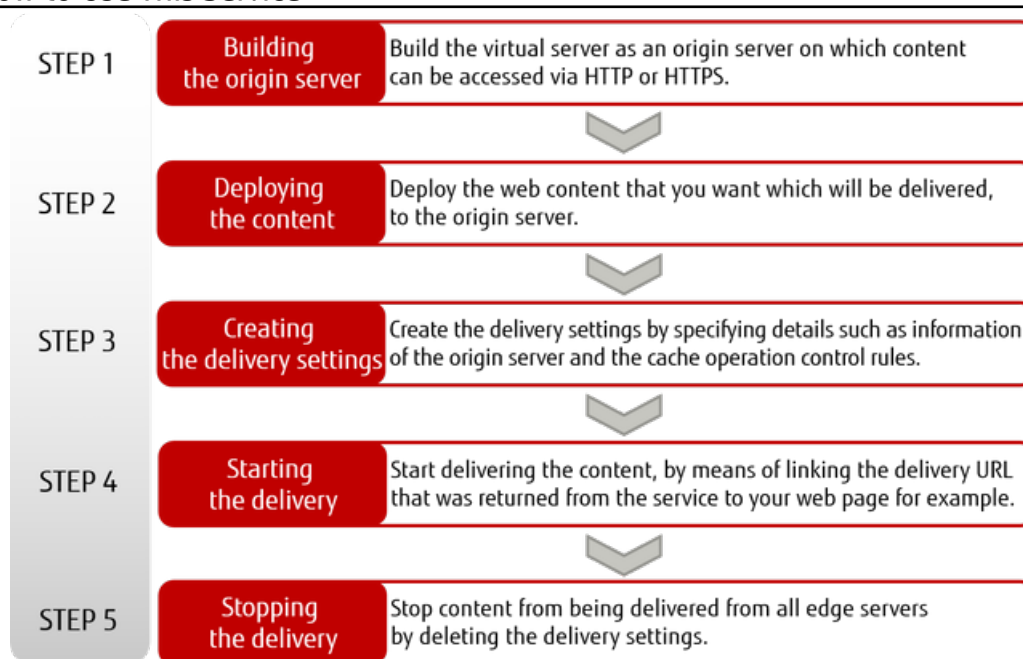
How to Use This Service

STEP 1	**Building the origin server**	Build the virtual server as an origin server on which content can be accessed via HTTP or HTTPS.
STEP 2	**Deploying the content**	Deploy the web content that you want which will be delivered, to the origin server.
STEP 3	**Creating the delivery settings**	Create the delivery settings by specifying details such as information of the origin server and the cache operation control rules.
STEP 4	**Starting the delivery**	Start delivering the content, by means of linking the delivery URL that was returned from the service to your web page for example.
STEP 5	**Stopping the delivery**	Stop content from being delivered from all edge servers by deleting the delivery settings.

Figure 47: How to Start the Content Delivery Service

Points to Note

・You can use only port 80 for access via HTTP, and only port 443 for access via HTTPS.

・When securely delivering content on a unique domain, it is necessary to submit an application before performing the delivery settings in step 3. Refer to "When Using a Unique Domain".

・Charges for content delivery service are due 2 months after the end of the billing period.

・DNS-related operations for the content delivery 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 will continue during maintenance.

8.1.2 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 a unique domain (assigned domain)

A URL that includes an assigned domain provided by the content delivery service is used as the delivery URL. The configuration of the delivery URL for both http and https is shown below.

```
http:// [prefix]random characters.cdn-edge.cloud.global.fujitsu.com/
https://[prefix]random characters.cdn-edge-s.cloud.global.fujitsu.com/
```

Delivery FQDN

Delivery URL

If you have a unique domain

If you have a unique domain, use that domain to deliver content. In addition to creating the delivery settings for the content delivery service, it is also necessary to set the CNAME on a DNS server. The CNAME destination varies depending on whether http or https is used.
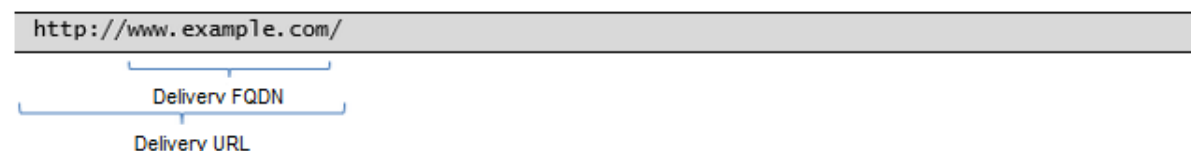
・For http

  common-http.cdn-edge.cloud.global.fujitsu.com

・For https

  You will receive notification when the application is complete.

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 below.

8.1.3 Secure Delivery

Use HTTPS to securely deliver content from an edge server to the end user.

> **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.

Certificates for Origin Servers

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 154: 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

Common Name	Expiry Date	SHA-1 Fingerprint
Certum CA	June 11 2027	6252dc40f71143a22fde9ef7348e064251b18118
Class 2 Primary CA	July 7 2019	74207441729cdd92ec7931d823108dc28192e2bb
COMODO Certification Authority	January 1 2030	6631bf9ef74f9eb6c9d5a60cba6abed1f7bdef7b
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

Common Name	Expiry Date	SHA-1 Fingerprint
SecureTrust CA	January 1 2030	8782c6c304353bcfd29692d2593e7d44d934ff11
StartCom Certification Authority	September 18 2036	3e2bf7f2031b96f38ce6c4d8a85d3e2d58476a0f
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 created by the user are not supported.
> - An unlimited license is not required.
> - If you already have the certificate for a domain name that will be used on an application (example: www.company.com), it can be used as the certificate for the origin server. If you do not have a certificate, prepare one for only the origin server (example: origin.company.com).

When Using a Unique Domain

When using a unique domain, it is necessary to register the server certificate on the edge server. It is necessary to apply using an application form. Obtain the "Content Delivery Service Unique Domain Secure Delivery Form" application form from customer service.

- We apply for the certificate on your behalf, and arrange and manage it on the edge server.
  - It is not possible to use a certificate that you already have.
  - It is not possible to download the private key for your certificate.
  - The certificate is a Subject Alternative Name (SAN) certificate.
  - It is not possible to use wildcard certificates.
  - The TLS Version and Cipher Set are automatically updated.

- Use is not possible in China and Russia.
- It is not possible to change a domain name that has been applied for to another domain name.
- The updating of certificates is performed automatically.
  - The Certificate Authority regularly authenticates domain names.
  - When updating is successful, the limit of the certificate is automatically extended.
  - When update fails due to a reason such as communication not being possible, there is a possibility that the certificate for the relevant domain has expired.
- It is also necessary to apply using an application form when deleting a certificate. Charges will be incurred for the certificate until the application is processed.
- The types of certificates are DV (Domain Validated) and SNI (Server Name Indication).
- A single certificate is shared with other customers. The name of the customer's domain is stored in the DNS Name field of the certificate.
- Signing is performed by Let's Encrypt.
- It is usually possible to start use within five working days.
- As domain validation is performed during authentication, build an accessible origin server in the domain name that will be applied for. At that time, open TCP port 80, and configure redirection as below. As updating will be performed on the edge server side, port 80 can be closed if so desired.

Table 155: Redirect Settings

Item	Value
Access destination	Under "http://Application_domain/.well-known/acme-challenge/"
Redirect destination	http://dcv.akamai.com/.well-known/acme-challenge/

8.2 Delivery Settings

8.2.1 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

This function acquires 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 156: Creating Delivery Settings (List of Items That Can Be Set)

Item	Description	Required
FQDN Information	Specify either of the following formats for the FQDN information that will be delivered: • When using a unique domain: FQDN > ➡ **Note** You must set CNAME on the DNS server. • When not using a unique domain: Prefix	
Delivery Protocol Scheme	Specify either of the following: > 💡 **Tip** If this setting is omitted, "http" will be specified. • 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 this setting is omitted, "activate" will be specified. • To enable content delivery immediately: activate • To disable content delivery: deactivate	

Item	Description	Required
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. ➡️ **Note** You can store access logs only in a container on object storage in Eastern Japan Region 1 (jp-east-1).	
Access Log Prefix	Specify the prefix to assign to the object name of the access log.	
Public Key Encryption of Access Log	Specify the save directory of the public key to use to encrypt 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.	Yes

Caching behavior control rules are used to implement an action specified as a "behavior" (for example, specification of TTL) when the conditions specified in "match" (for example, the condition that the extension is .jpg) are met.

💡 **Tip** Refer to Example Usage Scenarios and Caching Behavior Control Rules for examples of "matches" and "behaviors." For description formats, refer to API Reference Manual.

The items that can be set to "matches" and "behaviors" are shown below.

<div align="center">

Table 157: Match (List of Items That Can Be Set)

</div>

Item	Description
URL	Set a character string that identifies the URL to be accessed by the end user. Examples: jpg, index.html, /img/*, /*
Method	Set the HTTP methods to be accessed by the end user. (Example: "GET, POST") • GET • POST • PUT • DELETE • HEAD • PATCH
Scheme	Set the scheme to be accessed by the end user. • HTTP • HTTPS
Header	Set whether there is a header to be accessed by the end user. Example: "User-Agent: xxx yyy zzz"

<div align="center">Table 158: Behavior (List of Items That Can Be Set)</div>

Item	Description
Origin Settings	Specify FQDN and accompanying information for the origin server. As accompanying information, specify information for the origin server to determine if access is via the content delivery service. Examples of accompanying information: ・ Host header ・ Cache key that affects cache conditions
Cache TTL Settings	Specify cache TTL as a fixed value, dependent on the origin, etc.
Query Strings Used by Cache Keys	For dynamic pages that can be cached, specify behaviors that identify cache keys. Example: Exclude a query string that includes a session ID
Invalidate Cache	Invalidate the cache on an edge server at a specified time (including "immediately").
IP Address Restriction	Restrict end users who are allowed to access based on their IP addresses.
Region Restriction	Restrict end users who are allowed to access based on the region where they originally accessed.
Referer Restriction	Restrict end users who are allowed to access based on the referer information .
Token Verification	Restrict end users who are allowed to access based on the referer information.
Failover	If the originally specified origin server goes down, acquire content from a different origin server.

Acquiring Delivery Settings

You can specify the ID of the delivery setting to acquire the following content for the delivery setting:
・ Caching behavior control rules
・ Delivery URL
・ Delivery protocol
・ Delivery status
・ Access log storage destination
・ Access log status
・ Public key encryption of access log

Editing Delivery Settings

You can specify the ID of the delivery setting to edit the following content for the delivery setting:
・ Caching behavior control rules
・ Delivery status
・ Start/stop storing access logs, access log storage destination, change encryption settings and public key encryption

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.

Purging Cache

Purge the cache for content that matches a specific delivery URL from an edge server when replacing the files on an origin server or when incorrect files have been delivered.

There are the following two ways to purge the cache.

- Delete the cache

  Delete the cache on edge servers. If you delete the cache, and then an end user accesses the content, edge servers will need to fetch (obtain) it from the origin server.

  Use this when it is necessary to ensure cache deletion, such as when an incorrect image has been published.

- Invalidate the cache

  Invalidate the cache on edge servers. If you invalidate the cache and then an end user accesses the content, edge servers will need to fetch (obtain) it from the origin server only if the content is updated.

  From the viewpoint of increased load on the origin server and consumption of network bandwidth, it is recommended to invalidate the cache.

Access Log Function

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. Access logs can be encrypted when they are stored (The default is unencrypted).

Specify the following information for the storage destination for access logs.

- Name of container for object storage

  Example: "container"

  > **Note**
  > You can store access logs only in a container on object storage in Eastern Japan Region 1 (jp-east-1).

- 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 12 MB 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 159: 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.)
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
```

8.2.2 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 service.

- Website Content Delivery
- Content Delivery with a Unique Domain
- Secure Content Delivery
- Secure Content Delivery with a Unique Domain
- Replacing Content
- Reconsidering the Content Update Frequency
- Conditional Access Restrictions
- Stopping Content Delivery

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. Use a browser to confirm that you can access the origin server.
  5. Use the content delivery 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. Enter the delivery URL in a browser and confirm that you can access the delivery URL.
- 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 a Unique Domain

- Example building procedure

> 💡 **Tip** If you are using the DNS service for the name resolution of a unique 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 DNS service.

1. Create delivery settings using the procedures described in Website Content Delivery, to acquire the delivery URL.

   At this time, specify a unique domain (example: www.example.com) for delivery FQDN in the API parameters.

2. Enter the delivery URL in a browser and confirm that you can access the delivery URL.

3. Use the DNS service to create a CNAME record.

   At this time, create the CNAME settings so that the unique domain points to common-http.cdn-edge.cloud.global.fujitsu.com.

4. Use a browser to confirm that you can access the unique domain.

- 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 certificates you can use, refer to Secure Delivery.

2. Create delivery settings using the procedures described in Website Content Delivery.

   At this time, specify https for the delivery protocol in the API parameters. In addition, for the edge server to accept 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. Enter the delivery URL in a browser and confirm that you can access the delivery URL.

- 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"
        }
      ]
    }
  ]
}
```

Secure Content Delivery with a Unique Domain

- Example building procedure

Assume that the name of the unique domain for content delivery is "www.example.com", and the domain name of the origin server is "origin.example.com".

1. First of all, build the origin server (origin.example.com). If the origin server is a virtual server or a load balancer, prepare an SSL certificate and install it yourself. For details about what certificates you can use, refer to Secure Delivery.

2. For authentication (to confirm the existence of the domain), temporarily assign origin.example.com to www.example.com in the DNS CNAME record. Also, it is necessary to open http port 80 as well as https port 443. Then configure the path for the directory used for authentication in http as the target of redirection of the edge server. A sample is given below.

3. Apply for www.example.com using an application form. For details, refer to Secure Delivery.

4. Check the content displayed when the application is complete, and create delivery settings with the API. At this time, specify https for the delivery protocol and www.example.com in the FQDN information in the API parameters.

5. Use a browser to confirm that you can access the unique domain.

- Example of addition to the Apache httpd setting file

```
<Directory "(DocumentRoot)">
(omitted)
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/.well-known/acme-challenge/ [NC]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule . http://dcv.akamai.com%{REQUEST_URI} [L]
</Directory>
```

- Example of caching behavior control rules

```
{
  "rules": [
    {
      "matches": [
        {
          "name": "url-wildcard",
          "value": "/*"
        },
        {
          "name": "url-scheme",
          "value": "HTTPS"
        }
      ],
      "behaviors": [
        {
          "name": "origin",
          "value": "-",
          "params": {
            "digitalProperty": "-",
            "originDomain": "origin.example.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.

- Example operation procedure

1. Replace image files, PDF files and so on stored in the origin server.

2. Perform "Purge 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.

- 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.

- 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 a unique 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.

8.3 Reporting

8.3.1 Report Functions

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. Users can also acquire reporting information in units of delivery and region.

Create Report Function

Create statistical information 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 160: Creating a Report (List of Items That Can Be Set)

Item	Description	Required
Granularity	Specify the granularity of the information from either 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 only • all: Combined total (default)	
Target	Specify the target of the information from either of the following: • Combined total for delivery setting (default) Specific delivery setting	
Output per Region	Specify whether to output per region: • true: Output per region false: Combined total (default)	

Item	Description	Required
List of Metrics to Be Acquired	Specify the names of the metrics that you want to output from Table 161: List of Metrics That Can Be Acquired with a Report, separated by commas.	Yes

Table 161: List of Metrics That Can Be Acquired with a Report

Name	Description
IncompleteDownloadCount	Number of incomplete downloads
200Count	Number of Status Code 200 responses
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 of the content delivery until about 8am on January 1. To acquire reports from all edge servers, 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"],
    }
}
```

8.4 Access Control

8.4.1 Access Control

It is possible to restrict delivery of cache contents to only some end users. For instance, as well as it being possible to restrict access to cache contents based on regions, IP addresses, and referers of browsers, it is also possible to restrict access to content requiring verification (authorization) based on whether an authorization token is approved or denied.
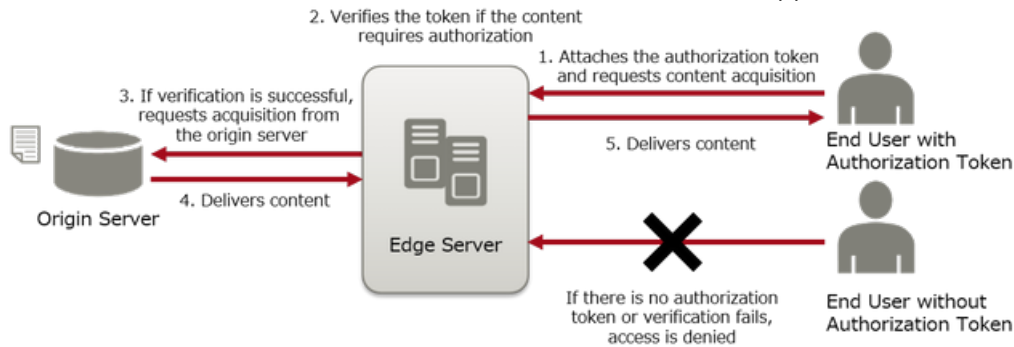
Figure 48: Access Control in the Content Delivery Service

Part 9: Template

Topics:

- **Orchestration**

IaaS provides this function to create a template of the resources built by the user.

9.1 Orchestration

9.1.1 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 virtual database server.

The orchestration function handles system groups like the one described below as one "stack."

Figure 49: 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 50: Diagram of Use of the Orchestration Function

9.1.2 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.

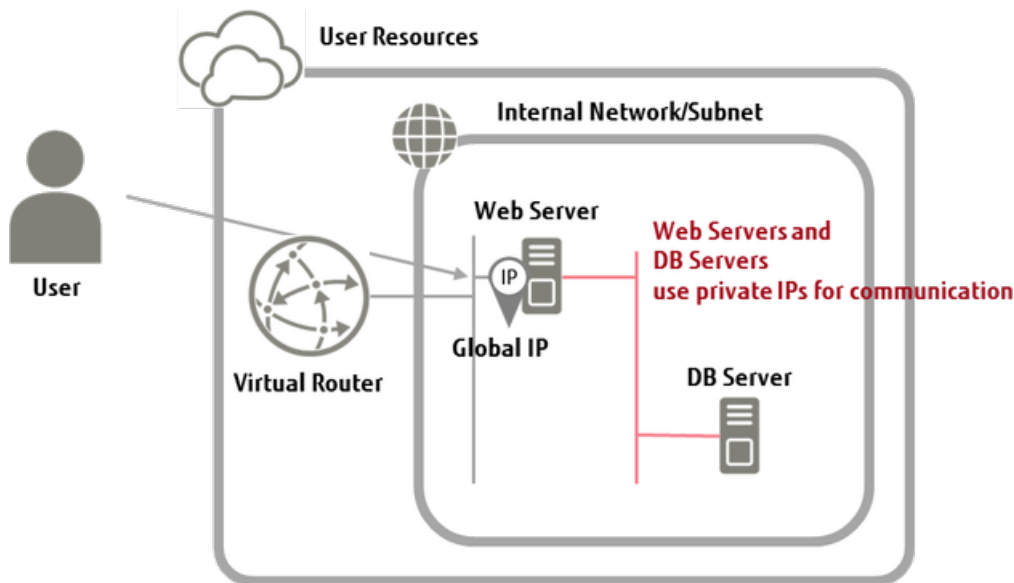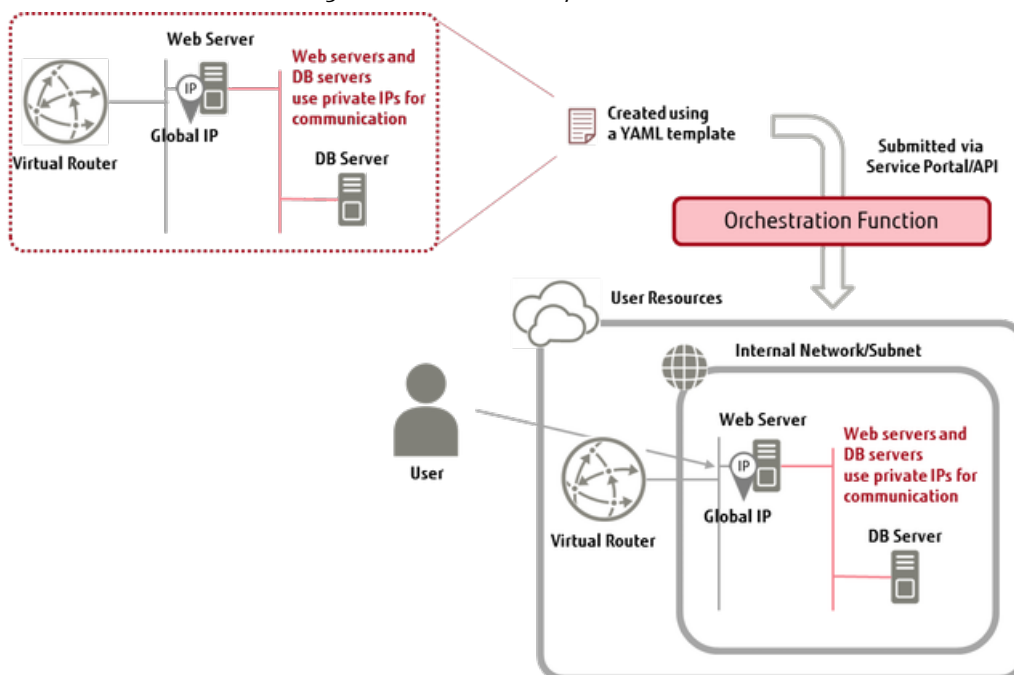> **Note** To build a stack, the "System Owner role (cpf_systemowner)" of the project where you want to build the stack must be assigned in advance to the user of this function.

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 162: 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
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.	

Item	Description	Required
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	

⮕ **Note** When deployment of virtual servers fails, ports may not be deleted even if rollback is performed.

Creating a Template

For details, refer to Example of Setting Auto-Scaling.

9.1.3 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 10: Monitoring Service

Topics:

- Overview of Functions
- Monitoring of Resources
- Alarms

IaaS provides a monitoring function for the resources built by the user and for the applications executed by the user on the resources.

10.1 Overview of Functions

10.1.1 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 virtual database servers. 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
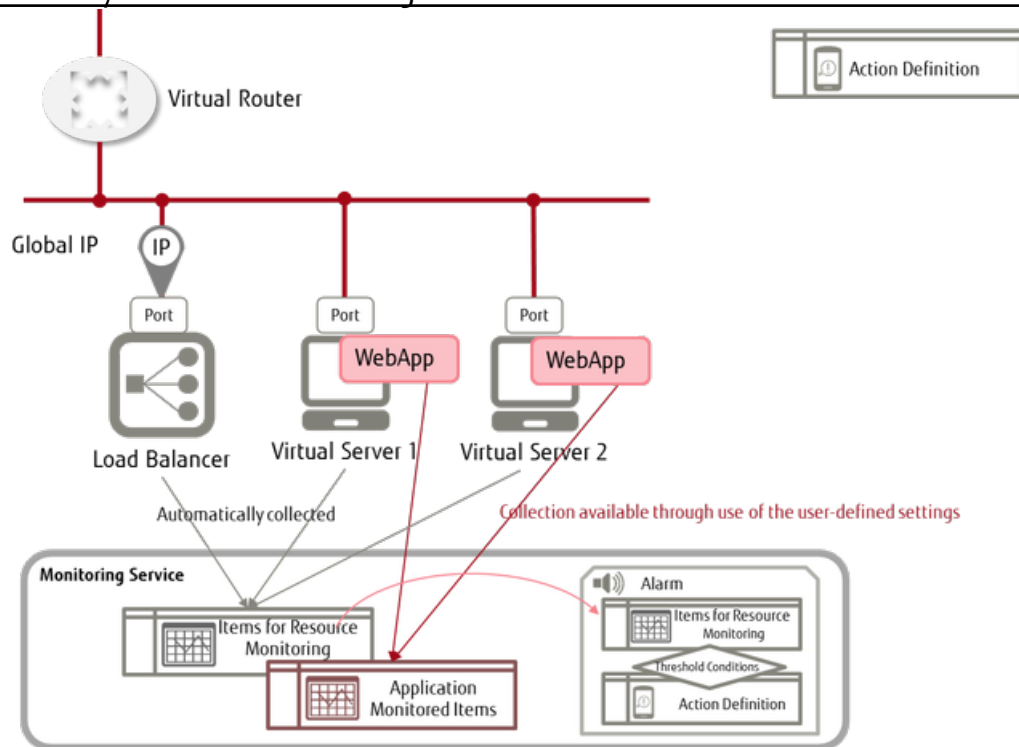
Figure 51: Overview of the Monitoring Service

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.
Dashboard	The dashboard displays graphs and statistics for all monitored items from the management console. You can also view all alarms and their history.

Function	Overview
API	All operations and the acquisition of monitored items are performed by using an API (compatible with Ceilometer from OpenStack).

10.2 Monitoring of Resources

10.2.1 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:

> **Tip** For information about the items to be monitored, refer to Lists of Monitored Items.

- 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.

10.2.2 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.

> **Tip** For details about creating a custom meter, refer to the section about new monitoring items and sample registration in API Reference Manual.

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

10.3 Alarms

10.3.1 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
  - Statistics calculation period

    1 minute (minimum) to 1 day (maximum)
- Action settings

  Define actions for each alarm status shown below.

> **Note**   Actions are performed only when the status changes.

Table 163: 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 164: 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 11: Security

Topics:

- IPS/IDS

IaaS provides security solutions for virtual servers.

11.1 IPS/IDS

11.1.1 Trend Micro Deep Security as a Service Option

We have provided the Deep Security as a Service option, which allows you to carry out centralized management of the security functions for your created virtual server, by using the management server provided in the cloud by Trend Micro.
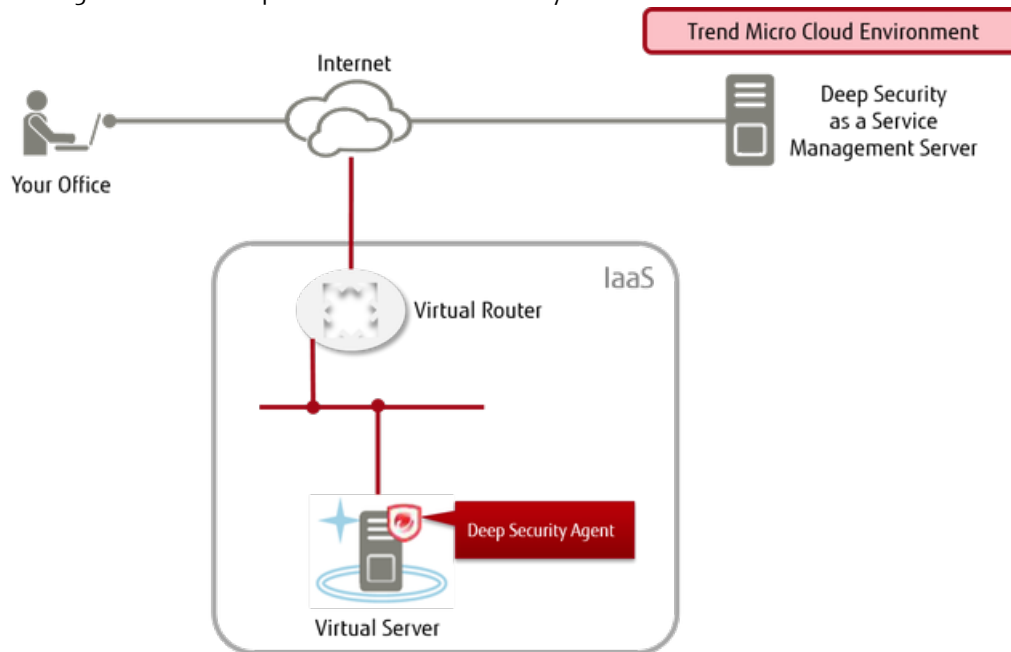
Figure 52: Overall Layout of Trend Micro Deep Security as a Service Option

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 165: 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

How to Use This Service

STEP 1	Applying Through the Application Form	Enter the required number of licenses on the application form and submit the application.
STEP 2	Activating the product	Fujitsu will issue an activation code and contact you.
STEP 3	Acquiring an Account	Acquire a Trend Micro Deep Security Manager account.
STEP 4	Downloading the Agent	Log into Deep Security Manager, enter the activation code and download the agent.
STEP 5	Installing the Agent	Install the Deep Security agent on the virtual server you want to protect.

Figure 53: 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.

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 IaaS service official website.

Part 12: Management

Topics:

- Overview of Functions
- Subscription Management
- User Management
- Key Management

IaaS provides a function to manage the privileges for using the resources.

12.1 Overview of Functions

12.1.1 Information to Know in Advance

This section explains the concepts provided by the user management functions.
With 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:
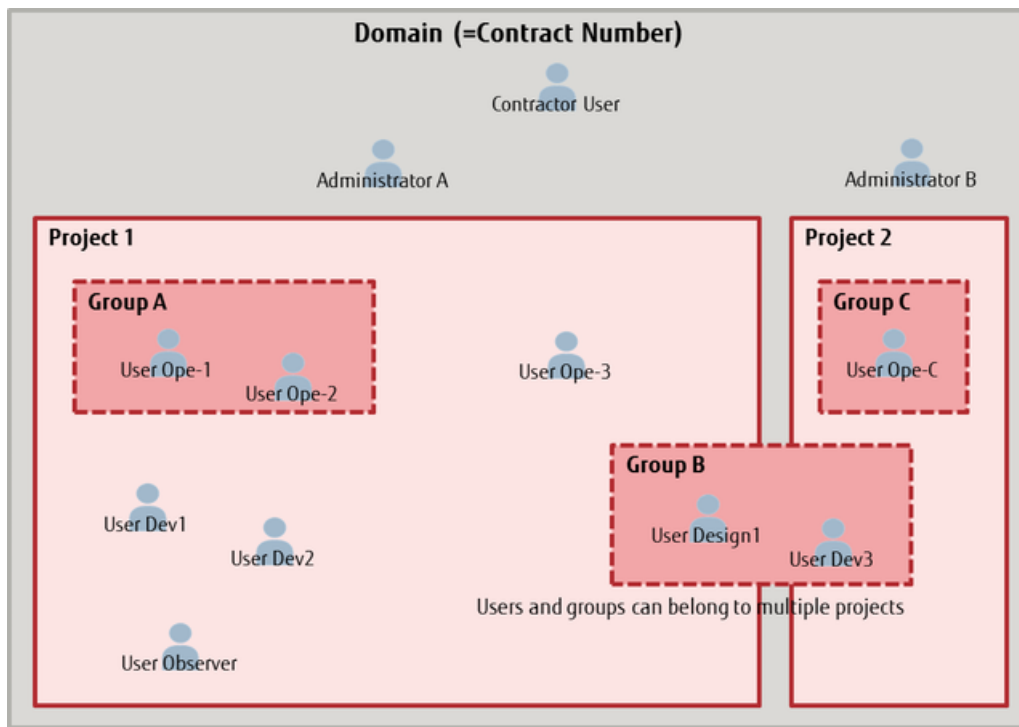
Figure 54: Relationship Concepts Provided by the User Management Functions

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
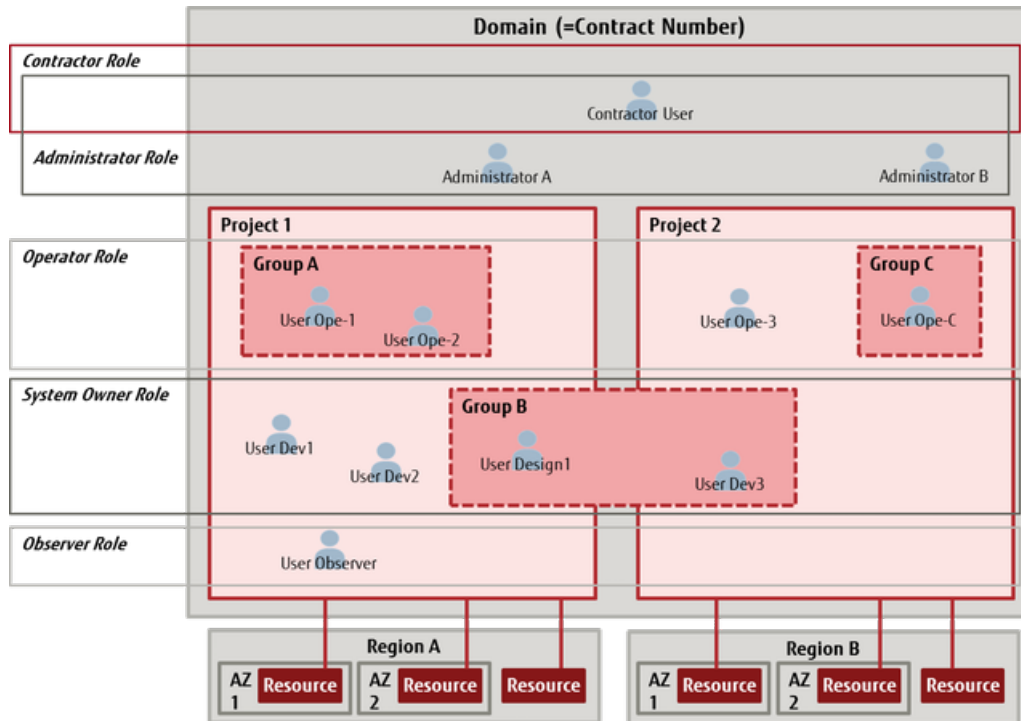
Figure 55: Domain, Group, and User Relationships

12.1.2 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.

User Operation Procedure
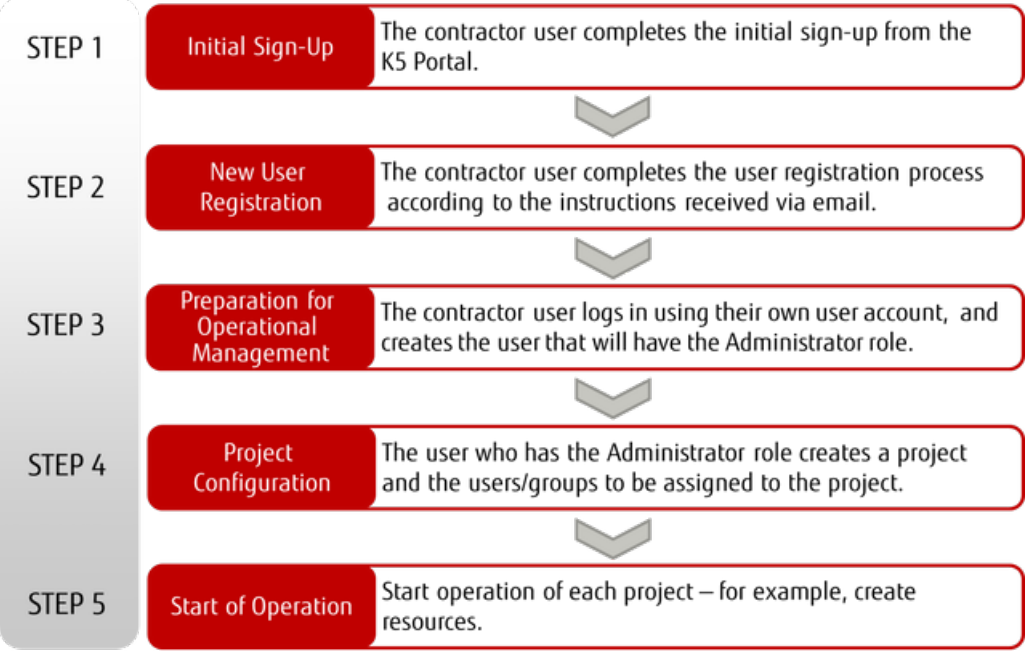
Figure 56: Procedure from Signup to Start of Operation

For details on new registration and the user management functions, refer to *K5 Portal User Guide*.

12.2 Subscription Management

12.2.1 Region Management

This function allows you to activate additional regions in addition to the regions that have been used since 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 2 (jp-east-2)" 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 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.

12.3 User Management

12.3.1 Overview of Functions

12.3.1.1 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

12.3.1.2 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

12.3.1.3 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.

> **Note**
>
> It is not possible to directly assign the Administrator role (cpf_admin) privileges to a user.
> - When assigning the Administrator role to a user
>
>   The domainmanager group is provided as a group that has the Administrator role assigned. Add the relevant user to the domainmanager group.

System Owner Role (cpf_systemowner)

This role can be created by the contractor user 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 user 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 user 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 FUJITSU Cloud Service for OSS 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.

12.3.2 Global User Management

12.3.2.1 Group Management

12.3.2.1.1 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. For example, you can configure 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

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 166: 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 167: 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

Item	Description	Required
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 💡 Specify the domain to which you belong. Tip	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.
Important

Limiting Values

Table 168: 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 (,), dot (.), 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 (,), dot (.), 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 - 246 characters • Available character type: Alphanumeric characters and the following symbols: Dot (.), at mark (@), hyphen (-), underscore (_)

Item	Limiting Values
User Password	• Length: 16 - 64 characters • Available character type: Alphanumeric characters, single-byte spaces, and the following symbols: !#$%&()*+-.=?@[]_{}~ • Complexity constraints 　・ Must not contain the user name 　・ Must include at least 1 alphabetic character 　・ Must include at least 1 numeric character • Case sensitivity: Yes
Email Address	• Length: 5 - 64 characters • Available character type: Alphanumeric characters and the following symbols: !#$%&'*+-./=?@^_`{|}~

12.3.3 Regional User Management

12.3.3.1 Project Management

12.3.3.1.1 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.

Creating a Project

Create projects within a domain. Items that you can specify are as follows.

Table 169: 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
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 170: 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. However, you cannot disable the default project.

> **Important**
> If you simply disable a project, the virtual resources belonging to that project are not returned automatically. The operational conditions of the virtual server, global IP address, virtual router, firewall, and such will persist. If you no longer require the virtual resources, return them before disabling the project.

> **Tip**
> It is not possible to delete created projects.

Limiting Values

Table 171: List of Limiting Values Related to Domains, Projects, Groups, and Users

Item	Limiting Values
Number of Projects	1,000 per domain

Item	Limiting Values
Project Name	• Length: 4 - 64 characters • Available character type: Alphanumeric characters and the following symbols: Plus sign (+), equal sign (=), comma (,), dot (.), 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 (,), dot (.), 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 - 246 characters • Available character type: Alphanumeric characters and the following symbols: Dot (.), at mark (@), hyphen (-), underscore (_)
User Password	• Length: 16 - 64 characters • Available character type: Alphanumeric characters, single-byte spaces, and the following symbols: !#$%&()*+-.=?@[]_{}~ • Complexity constraints • Must not contain the user name • Must include at least 1 alphabetic character • Must include at least 1 numeric character • Case sensitivity: Yes
Email Address	• Length: 5 - 64 characters • Available character type: Alphanumeric characters and the following symbols: !#$%&'*+-./=?@^_`{|}~

12.3.3.2 Role Management

12.3.3.2.1 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).

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.
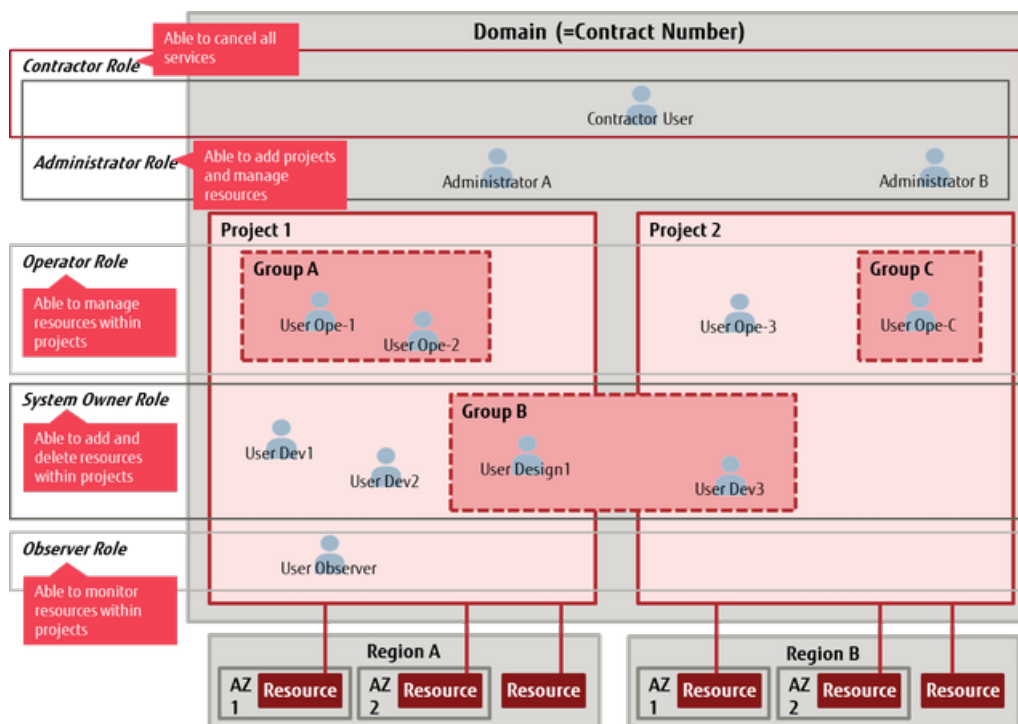
Figure 57: Role Assignment Example

12.4 Key Management

12.4.1 Key Management Function

This function allows you to centrally manage the key metadata that is required for SSL communication. Users can use key metadata that they have created and registered as well as key metadata that is registered by services such as the load distribution service.

Managing Key Metadata

Register and manage key metadata that was created in PEM format by a user.

Table 172: Registering Key Metadata (List of Items That Can Be Set)

Item	Description
Key Metadata Name	Specify the name of the key metadata
Encryption Algorithm	Specify the encryption algorithm for the key metadata 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 metadata will be deleted automatically. If this setting is omitted, no limit is set on use of the key metadata **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 **Note** When confidential information is specified, this item becomes necessary.

Item	Description
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+GgAwIBAgIQU3O6HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCBtTELMAkGA1UEBh
MCVVMxFzAVBgNVBAoTDIZIcmITaWduLCBJbmMuMR8wHQYDVQQL........
NM856xjqhJCPxYzk9buuCI1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn1qiwRk45OmCOnq
H4Iy4P4IXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELTOe5YR7CKx7fc5xRaeQdyGj/dJevm9BF/mSdncIS5vas=
-----END CERTIFICATE-----
```

Managing Certificate Information

Manage the following key metadata 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 13: Private Connection

This service provides the functions and ports for a closed connection between the IaaS environment and an environment such as a hosting environment to which the user subscribes or an on-premises environment.

13.1 Overview of Functions

13.1.1 Private Connection Function

This function provides the features and ports for a closed connection between the IaaS environment and another environment, such as the hosting environment to which the contractor user subscribes or an on-premises environment.

> ⚠️ **Important**
> ・An application must be made in advance. Please contact your Fujitsu representative regarding an application for the Private Connection function.

Provided Service Menu

・IaaS environment connection
・On-premises (Region Private Network) connection
・Cloud connection provided by other company

> 💡 **Tip**
> For further details about this service, refer to the "FUJITSU Cloud Service for OSS - Private Connection Service Descriptions."

13.1.2 Direct Port Connection Function

This function provides physical ports for a direct connection to the IaaS environment via L3, not via the Internet or the Private Connection function.

> ⚠️ **Important**
> ・An application must be made in advance. Please contact your Fujitsu representative regarding an application for the Private Connection function.

Provided Service Menu

・Direct port connection

> 💡 **Tip**
> For further details about this service, refer to the "FUJITSU Cloud Service for OSS - Private Connection Service Descriptions."

A: 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 173: 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
Number of Server Groups *	10 per project per availability zone
Number of Virtual Servers that Can Be Registered in a Server Group *	20

> **Note** The limits of values of the items in Table 173: List of Limiting Values Related to Virtual Servers (marked with *) only apply to the Eastern Japan Region 2.

Table 174: List of Limiting Values Related to the Virtual Server Remote Console Function

Item	Limiting Values
Maximum Duration of a Console Connection	30 minutes
Number of Simultaneous Console Connections to a Virtual Server	1
Maximum Number of Simultaneous Console Connections	For one contract: 5 Connections per AZ
Expiration Time of a Console Connection URL	10 minutes

Table 175: List of Limiting Values Related to Virtual Server Import

Item	Limiting Values
Maximum Number of Virtual Server Import Requests	100 per domain
Maximum Execution Period of Virtual Server Import Processing	7 days

Item	Limiting Values
Number of Virtual Server Import Processing Results Retained	1,000 💡 Tip: If this limiting value is exceeded, the oldest processing results are deleted.
File Size of a Single Virtual Server Image (Size in Raw Format)	300 GB 💡 Tip: .vmdk files that are divided and uploaded separately are automatically converted into Raw format. This limiting value is the size after Raw conversion.

Table 176: List of Limiting Values Related to Virtual Server Export

Item	Limiting Values
Maximum Number of Virtual Server Export Requests for a Single Domain	100
Maximum Number of Virtual Server Export Requests for a Single Project	50
Maximum Execution Period of Virtual Server Export Processing	7 days
Number of Virtual Server Export Processing Results Retained	1,000 💡 Tip: If this limiting value is exceeded, the oldest processing results are deleted.
File Size of a Single Virtual Server Image (Size in Raw Format)	300 GB
Maximum Simultaneous Execution Number for a Single Domain	5
Maximum Simultaneous Execution Number for a Single Project	2

• Services for SAP

Table 177: 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
Number of Storage Systems that Can Be Added	1 - 55
Number of Snapshots Taken	10

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

Limiting Values Related to Storage

Table 178: List of Limiting Values Related to Block Storage

Item	Limiting Values
Storage Size (Standard Type)	1 GB to 10 TB (specified in GB)
Storage Size (High Performance Type)	1 TB to 3 TB (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 no more than 26 for a single virtual server.
Storage Capacity (total for a project)	5 TB per project per availability zone (including capacity for snapshots)
Number of Snapshots Taken	100 per project per availability zone

Note
- 1 GB = 1,024^3 bytes
- 1 TB = 1,000 GB

Table 179: 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 180: List of Limiting Values Related to Networking

Item	Limiting Values
Number of Networks	10 per project per availability zone

Item	Limiting Values
Number of Subnets	10 per project per availability zone
Number of Host Routes that Can Be Set per Subnet	20
Number of Ports	50 per project per availability zone **Tip** The number of ports that are added due to the addition of storage is not counted. **Note** The total number of additional storage systems and additional ports must be no more than 26 for a single virtual server.
Number of Allowed Address Pairs that Can Be Set for Ports	10 per port
Number of Global IP Addresses	50 per project per availability zone
Number of Security Groups	20 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 VPN Services	1 per virtual router
Number of IPsec VPN Sites	20
Number of SSL-VPN Connections	20 sessions per connection
Number of Security Groups that Can Be Set for SSL-VPN Connection Resources	6 per connection
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 181: 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

Item	Limiting Values
Maximum Number of Policies to be Created	100 per load balancer

Table 182: 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

Table 183: 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, LBR, PTR, SRV
Record Type with Wildcard Support	A, AAAA, MX, CNAME, TXT

Table 184: List of Limiting Values for DNS Record Entries

Record Type	Item	Limitations	Required
A	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Available character type: Alphanumeric characters and dots (.) Must be a valid IPv4 address	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
	Weight	0 - 100 Available character type: Numeric characters	*1
	Health Check IP Address	Length: 1 - 32 characters Alphanumeric characters and dots (.)	*2
	Health Check Port No.	Length: 1 - 5 characters Available character type: Numeric characters	*2

Record Type	Item	Limitations	Required
	Health Check Host Name	Length: 0 - 255 characters Available character type: Single-byte characters	*3
	Health Check Path	Available character type: Single-byte characters Only omittable when failover is selected in the policy	*3
AAAA	Record Name	Length: 1 - 63 characters Alphanumeric characters, hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Alphanumeric characters and colons (:) Must be a valid IPv6 address	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
	Weight	0 - 100 Available character type: Numeric characters	*1
	Health Check IP Address	Length: 1 - 32 characters Available character type: Alphanumeric characters and dots (.)	*2
	Health Check Port No.	Length: 1 - 5 characters Available character type: Numeric characters	*2
	Health Check Host Name	Length: No more than 255 characters Available character type: Single-byte characters	*3
	Health Check Path	Available character type: Single-byte characters	*3
CNAME	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, hyphens (-), and wildcards (*)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)	Yes

Record Type	Item	Limitations	Required
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
MX	Record Name	Length: 1 - 63 characters Alphanumeric characters, dots (.), hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)	Yes
	Priority	0 - 64000 Available character type: Numeric characters	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
TXT	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, underscores (_), hyphens (-), wildcards (*), and at marks (@)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Alphanumeric characters, single-byte spaces, and single-byte symbols other than double quotation marks (")	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	
NS	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters and hyphens (-)	Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority	
	Value	Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters	

Record Type	Item	Limitations			Required
LBR	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters and hyphens (-)			Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters			
PTR	Record Name	Character type: Alphanumeric characters, dots (.), and hyphens (-)			
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority			
	Value	Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-)			Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters			
SRV	Record Name	Length: 1 - 63 characters Available character type: Alphanumeric characters, dots (.), hyphens (-), and underscores (_) Specify using the "_<Service Name>._<Protocol Name>" format (Example: _ftp._tcp)			Yes
	TTL	60 - 86,400 seconds *When there is no value entered, the TTL value of the zone is given priority			
	Value	Specify the priority, the weight, the port number, and the target in this order, separating the values with blank spaces			Yes
		Priority	0 - 64000 Available character type: Numeric characters		Yes
		Weight	0 - 65535 Available character type: Numeric characters		Yes
		Port No.	0 - 65535 Available character type: Numeric characters		Yes

Record Type	Item	Limitations		Required
		Target	Length: 1 - 255 characters Available character type: Alphanumeric characters, multi-byte domains, dots (.), and hyphens (-) Specify using the format "<Record name of A record>.<Domain name>" Tip: When the record name of the A record is "ftp-server-01" and the domain name is "example.com": Set it as "ftp-server-01.example.com"	Yes
	Memo	Length: No more than 255 characters Available character type: Double-byte characters		

*1: A required item when weighting has been selected using the policy.

*2: A required item when failover has been selected using the policy.

*3: An optional item when failover has been selected using the policy.

Limiting Values Related to Database as a Service

Table 185: List of Limiting Values Related to Database as a Service

Item	Limiting Values
Number of Virtual Database Servers	40 per project
Total Disk Size of All Virtual Database Servers	100 TB
Number of DB Snapshots that Can Be Created	50 generations per virtual database server
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
Number of Read Replicas	5

Item	Limiting Values
Specification of the virtual database server 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 Virtual Database Server	• Length: 1 - 1,024 characters
Master User Name	• Length: 1 - 63 characters • Available character type: Alphabetic characters (lowercase), numeric characters, and underscores (_) • Other limitations • You can only use an alphabetic character (lowercase) 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 186: 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
Total Value of Registered Source Email Addresses and Registered Source Domains	1,000 per project
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 Service

Table 187: List of Limiting Values Related to Content Delivery

Item	Limiting Values
Time until the Content Delivery Service Becomes Available	Within 10 minutes 💡 **Tip** This is the time from when application of delivery settings is requested from the API.
Number of Delivery Settings that Can Be Created	200 per project
Number of Secure Communication Settings per Unique Domain	3 domain names per project 💡 **Tip** When more than the maximum is necessary, submit the necessary number of domain names using an application form. We will issue the extra license keys.
Caching Behavior Control Rules that Can Be Created	100 behaviors per delivery setting
File Size that Can Be Delivered	1.8 GB (single file)
Number of Files that Can Be Maintained on the Edge Server	No upper limit

Item	Limiting Values
Maximum Size of Caching Behavior Control Rules	• Sending: 16 KB **Tip** This value is the total of the following: • User-specified length • Delivery FQDN length x Number of behaviors of origin settings • Receiving: No upper limit
Characters that Can Be Specified for FQDN Information	For assigned domains • Characters that can be specified for the prefix: 0 - 30 characters • Character type: Alphanumeric characters and hyphens (-) For unique domains • Characters that can be specified for FQDN: 1 - 255 characters • Character type: Alphanumeric characters, hyphens (-), and dots (.) **Note** • Uppercase alphabetic characters are treated as the corresponding lowercase character. • You cannot use a hyphen as the first or last character. • You cannot specify "xn--."
Cache TTL that Can Be Specified	0 - 9999 days
Number of API Execution Limits per Second (Rate Limiting)	There are execution limits per second for some APIs. **Tip** If you receive status code 429, wait a while and retry the operation.
Volume of Concurrent Access Possible	No upper limits for edge servers.
Characters that Can Be Specified for the Prefix of Access Log Storage Destination	1 - 256 characters **Tip** This includes the account name and the container name.

Limiting Values Related to the Template Service

Table 188: 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 dots (.)
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

Limiting Values Related to Management Functions

Table 189: 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 190: 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 (,), dot (.), 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 (,), dot (.), at mark (@), hyphen (-), underscore (_) • Case sensitivity: No • Uniqueness constraint: Uniqueness is required within a domain

Item	Limiting Values
Number of Users	• 100 per group • 100,000 per domain
User Name	• Length: 4 - 246 characters • Available character type: Alphanumeric characters and the following symbols: Dot (.), at mark (@), hyphen (-), underscore (_)

User Password	• Length: 16 - 64 characters
	• Available character type: Alphanumeric characters, single-byte spaces, and the following symbols:
	!#$%&()*+-.=?@[]_{}~
	• Complexity constraints
	  • 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 191: 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
Password History	Last 4 passwords Tip — When the password after changing would the same as one of the last 4 passwords, it is not possible to use that password.

Table 192: List of Limiting Values Related to Key Management Functions

Item	Limiting Values
Key Metadata Container Name	• Length: 1 - 255 characters • Available character type: Alphanumeric characters and single-byte symbols
Number of Key Metadata Containers	100
Key Metadata Records that Can Be Stored in a Key Metadata Container	10 per key metadata container
Number of Key Metadata Records	100
Key Metadata Name	• Length: 1 - 255 characters • Available character type: Alphanumeric characters and single-byte symbols
Size of Key Metadata	10,000 bytes or less

A.2 Points to Note

This section explains points to note regarding 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 (a maximum of 180 seconds)
• Loss of communication using the network, subnets, virtual routers, and network connectors

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 193: List of Software Support Service Related ID

Software	Software ID	Support Level	Support ID
Windows Server 2008 R2 SE SP1 64bit Japanese Version	W2k8R2SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Windows Server 2008 R2 EE SP1 64bit Japanese Version	W2k8R2EE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Windows Server 2012 SE 64bit Japanese Version	W2k12SE	No support	nosupport
		Support on weekdays	spt_daytime

Software	Software ID	Support Level	Support ID
		24-hour support	spt_24h
Windows Server 2012 R2 SE 64bit Japanese Version	W2k12R2SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Windows Server 2016 SE 64bit Japanese Version	W2k16SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Windows Server 2008 R2 SE SP1 64bit English Version, No support (charged by usage time) (x-core) (x is a number)	W2k8R2SE	No support	nosupport
Windows Server 2012 R2 SE 64bit English Version, No support (charged by usage time) (x-core) (x is a number)	W2k12R2SE	No support	nosupport
Windows Server 2016 SE 64bit English Version, No support (charged by usage time) (x-core) (x is a number)	W2k16SE	No support	nosupport
Windows Server 2008 R2 SE SP1 64bit Japanese Version, No support (charged by usage time) (x-core) (x is a number)	W2k8R2SE	No support	nosupport
Windows Server 2012 R2 SE 64bit Japanese Version, No support (charged by usage time) (x-core) (x is a number)	W2k12R2SE	No support	nosupport
Windows Server 2016 SE 64bit Japanese Version, No support (charged by usage time) (x-core) (x is a number)	W2k16SE	No support	nosupport
Red Hat Enterprise Linux 6.x 64bit English Version (x is a number)	RHEL	Limited Support	spt_limited
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Red Hat Enterprise Linux 7.x 64bit English Version (x is a number)	RHEL	Limited Support	spt_limited
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Red Hat Enterprise Linux 7.x 64bit English Version AUS (x is a number)	RHEL_AUS	24-hour support	spt_24h
CentOS 6.x 64bit English Version (x is a number)	CentOS	No support	nosupport

Software	Software ID	Support Level	Support ID
CentOS 7.x 64bit English Version (x is a number)	CentOS	No support	nosupport
Ubuntu Server 14.04 LTS English Version	UBUNTU	No support	nosupport
Ubuntu Server 16.04 LTS English Version	UBUNTU	No support	nosupport
Red Hat OpenShift Container Platform 3.x (Node) (x is a number)	OPNSHFT_ND	24-hour support	spt_24h
Red Hat OpenShift Container Platform 3.x (Master) (x is a number)	OPNSHFT_MS	24-hour support	spt_24h
Microsoft SQL Server 2008 SE SP4 64bit Japanese Version	MSSQL2K8SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Microsoft SQL Server 2008 R2 SE SP3 64bit Japanese Version	MSSQL2K8R2SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Microsoft SQL Server 2014 SE 64bit Japanese Version	MSSQL2K14SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Microsoft SQL Server 2014 EE 64bit Japanese Version	MSSQL2K14EE	No support	nosupport
		24-hour support	spt_24h
Microsoft SQL Server 2016 SE 64bit Japanese Version	MSSQL2K16SE	No support	nosupport
		Support on weekdays	spt_daytime
		24-hour support	spt_24h
Microsoft SQL Server 2016 SE 64bit English Version	MSSQL2K16SE	No support	nosupport
Interstage Application Server Standard-J Edition V11	INTER_S_L11	24-hour support	spt_24h
Symfoware Server Lite Edition V12	SYMFO_L_L12	24-hour support	spt_24h
Systemwalker Operation Manager Standard Edition V13	SYSWO_S_L13	24-hour support	spt_24h
Systemwalker Centric Manager Standard Edition (for Managers) V15	SYSWCM_S_L15	24-hour support	spt_24h
Systemwalker Centric Manager Standard Edition (for Agents) V15	SYSWCA_S_L15	24-hour support	spt_24h

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 (CentOS)
- Red Hat Update Infrastructure (RHUI)
- Windows activation (KMS)
- NTP server
- WSUS (Windows Server Update Services) server
- Red Hat Satellite server

Note — Common network services can only be used from IaaS environments.

The following is a list of servers that provide common network services:

DNS Server

Tip — Allow the following in the firewall and security group settings:
- Egress: TCP/Port 53, UDP/Port 53

Region	AZ	Name Server 1	Name Server 2
Eastern Japan Region 1 (jp-east-1)	jp-east-1a	133.162.193.9	133.162.193.10
	jp-east-1b	133.162.201.9	133.162.201.10
Eastern Japan Region 2 (jp-east-2)	jp-east-2a	133.162.97.9	133.162.97.10
	jp-east-2b	133.162.106.9	133.162.106.10
Western Japan Region 1 (jp-west-1)	jp-west-1a	133.162.161.9	133.162.161.10
	jp-west-1b	133.162.169.9	133.162.169.10
Western Japan Region 2 (jp-west-2)	jp-west-2a	133.162.145.9	133.162.145.10
	jp-west-2b	133.162.153.9	133.162.153.10

yum Repository Mirror Server (CentOS)

Tip — Allow the following in the firewall and security group settings:
- Egress: TCP/Port 53, UDP/Port 53, TCP/Port 80

Region	AZ	FQDN
Eastern Japan Region 1 (jp-east-1)	Common to all AZ	yum.jp-east-1.cloud.global.fujitsu.com
Eastern Japan Region 2 (jp-east-2)	Common to all AZ	yum.jp-east-2.cloud.global.fujitsu.com

Region	AZ	FQDN
Western Japan Region 1 (jp-west-1)	Common to all AZ	yum.jp-west-1.cloud.global.fujitsu.com
Western Japan Region 2 (jp-west-2)	Common to all AZ	yum.jp-west-2.cloud.global.fujitsu.com

Red Hat Update Infrastructure (RHUI)

> 💡 Tip
> Allow the following in the firewall and security group settings:
> • Egress: TCP/Port 53, UDP/Port 53, TCP/Port 443

Region	AZ	FQDN
Common to all regions	Common to all AZ	rhui.jp-west-2.cloud.global.fujitsu.com

Windows Activation (KMS)

> 💡 Tip
> Allow the following in the firewall and security group settings:
> • Egress: TCP/Port 1688, UDP/Port 53

Region	AZ	FQDN
Eastern Japan Region 1 (jp-east-1)	Common to all AZ	kms.jp-east-1.cloud.global.fujitsu.com
Eastern Japan Region 2 (jp-east-2)	Common to all AZ	kms.jp-east-2.cloud.global.fujitsu.com
Western Japan Region 1 (jp-west-1)	Common to all AZ	kms.jp-west-1.cloud.global.fujitsu.com
Western Japan Region 2 (jp-west-2)	Common to all AZ	kms.jp-west-2.cloud.global.fujitsu.com

NTP Server

> 💡 Tip
> Allow the following in the firewall and security group settings:
> • Egress: UDP/Port 123

Region	AZ	NTP Server 1	NTP Server 2
Eastern Japan Region 1 (jp-east-1)	jp-east-1a	133.162.193.106	133.162.195.141
	jp-east-1b	133.162.203.207	133.162.203.208
Eastern Japan Region 2 (jp-east-2)	jp-east-2a	133.162.97.19	133.162.97.20
	jp-east-2b	133.162.106.19	133.162.106.20
Western Japan Region 1 (jp-west-1)	jp-west-1a	133.162.161.19	133.162.161.20
	jp-west-1b	133.162.169.19	133.162.169.20
Western Japan Region 2 (jp-west-2)	jp-west-2a	133.162.145.19	133.162.145.20
	jp-west-2b	133.162.153.19	133.162.153.20

WSUS Server

> 💡 **Tip**
> Allow the following in the firewall and security group settings:
> ・Egress: TCP/Port 8530, UDP/Port 53

Region	AZ	FQDN
Eastern Japan Region 1 (jp-east-1)	Common to all AZ	wsus.jp-east-1.cloud.global.fujitsu.com
Eastern Japan Region 2 (jp-east-2)	Common to all AZ	wsus.jp-east-2.cloud.global.fujitsu.com
Western Japan Region 1 (jp-west-1)	Common to all AZ	wsus.jp-west-1.cloud.global.fujitsu.com
Western Japan Region 2 (jp-west-2)	Common to all AZ	wsus.jp-west-2.cloud.global.fujitsu.com

Red Hat Satellite Server

> 💡 **Tip**
> Allow the following in the firewall and security group settings:
> ・Egress: TCP/Port 53, UDP/Port 53, TCP/Port 80, TCP/Port 443, TCP/Port 5000, TCP/Port 5646, TCP/Port 5647, TCP/Port 8000, TCP/Port 8140, TCP/Port 8443, TCP/Port 9090

Region	AZ	FQDN
Common to all regions	Common to all AZ	rh-satellite.jp-west-2.cloud.global.fujitsu.com

A.5 Domains That Can Be Registered in a Zone

The domains that you can register in a zone are as follows.

Table 194: 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	.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 Predefined Security Policies

This section describes information about configurable security policies for listeners when you create a load balancer.
Details of the most recent predefined security policies, including available SSL protocols and SSL cipher suites are given in the table below. There are two types of pre-defined security policies in the table below, but when using security policies it is recommended to use the most recent ones.

Predefined SSL Security Policies (Most Recent)

The name of the most recent security policy is given below. Refer to the "2017-05" column in the table.

・Security Policy Name: LBServiceSecurityPolicy-2017-05

Predefined SSL Security Policies (Older)

The name of the previously released security policy is given below. Refer to the "2015-12" column in the table.

・Security Policy Name: LBServiceSecurityPolicy-2015-12

Table 195: Security Policy Names

Encryption Protocol	Cipher Suite	Cipher Suite Parameter Name (User Specified)	Predefined Security Policies	
			"2017-05"	"2015-12"
TLS 1.2 Default : true	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	○	○
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	○	○
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	○	○
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	○	○
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	○	○
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	○	○
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	○	○
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	○	○
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	○	○
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	○	○
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384	○	○
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384	○	○
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	ECDH-RSA-AES256-SHA384	○	○
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	ECDH-ECDSA-AES256-SHA384	○	○

Encryption Protocol	Cipher Suite	Cipher Suite Parameter Name (User Specified)	Predefined Security Policies	
			"2017-05"	"2015-12"
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	○	○
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	○	○
	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	○	○
	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	○	○
	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	○	○
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	○	○
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	○	○
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	○	○
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	○	○
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	○	○
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	○	○
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	○	○
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	○	○
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	○	○
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	○	○
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	○	○
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	-	○
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	ECDH-RSA-AES128-GCM-SHA256	○	○
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH-ECDSA-AES128-GCM-SHA256	○	○
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	ECDH-RSA-AES128-SHA256	○	○
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH-ECDSA-AES128-SHA256	○	○
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	○	○
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	○	○
	TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	○	○
	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	○	○
	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	○	○
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	○	○
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	-	○
TLS 1.1 Default : true	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	○	○
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	○	○
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	○	○
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	○	○
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	○	○
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	○	○
	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	○	○
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	○	○
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	○	○
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	○	○
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	○	○
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	○	○
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	-	○
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	○	○
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	○	○
	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	○	○
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	○	○

Encryption Protocol	Cipher Suite	Cipher Suite Parameter Name (User Specified)	Predefined Security Policies	
			"2017-05"	"2015-12"
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	-	○
TLS 1.0 Default : false	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	-	-
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	-	-
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	-	-
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	-	-
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	-	-
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	-	-
	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	-	-
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	-	-
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	-	-
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	-	-
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	-	-
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	-	-
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	-	-
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	-	-
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	-	-
	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	-	-
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	-	-
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	-	-
SSL 3.0 Default : false	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	-	-
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	-	-
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	-	-
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	-	-
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	-	-
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	-	-
	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	-	-
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	-	-
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	-	-
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	-	-
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	-	-
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	-	-
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	-	-
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	-	-
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	-	-
	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	-	-
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	-	-
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	-	-

A.7 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.

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 197: Network Services - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.ip.floating	G	ip	Existence of a global IP (when the resource is operated)
fcx.port	G	port	Existence of a port (when the resource is operated)

Table 198: Load Distribution Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.loadbalancing.instance.healthy	G	instance	Number of virtual servers running normally for each subnet
fcx.loadbalancing.instance.unhealthy	G	instance	Number of virtual servers that are experiencing abnormality for each subnet
fcx.loadbalancing.throughput	D	B	Performance information (differences of throughput)

Compute

Table 199: Standard Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.compute.instance	G	instance	Existence of a virtual server (when the resource is operated)
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

Monitored Item	Type	Units	Description
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
fcx.compute.instance.status_check.failed	G	count	Status check information for instance • 0: Normal • 1: Error

Table 200: Services for SAP - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.compute-w.instance	G	instance	Existence of a virtual server for SAP (when the resource is operated)

Storage

Table 201: Block Storage - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.blockstorage.volume.size	G	GB	Capacity of block storage

Table 202: 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 203: Image Archiving Service - List of Monitored Items

Monitored Item	Type	Units	Description
fcx.image.size	G	B	Size of uploaded image

Database

Table 204: 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 virtual database server to read replica virtual database server
fcx.database.swap.size *	G	B	Size of swap space used for virtual database server
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

* As this function is currently restricted, this information cannot be obtained.

A.8 Formula for Estimation

When you use the functions of 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.9 Setup of an SSL-VPN Client (Windows)

A.9.1 Setup of an OpenVPN Client (Windows)

- Obtain the following certificates that are required for building an SSL-VPN connection environment and setting up a client:
  - CA certificate of server certificate
  - Client certificate
  - Client private key
- Fujitsu has confirmed operation of this setup procedure in the following environment:
  - OS: Windows 7 Professional 64bit Japanese Version
  - OpenVPN: 2.3.X (X: 10 or later), 2.4

> **Note**
> When using OpenVPN 2.3.9 or earlier, uninstall it, and then re-install it following the procedure below.

To establish an SSL-VPN connection from a PC where Windows OS is installed, follow the setup procedure below.

Procedure

1. Acquisition of an OpenVPN client
   Download the installer for Windows from https://www.openvpn.jp/download.
2. Execution of the installer
   Click the [Next] button.
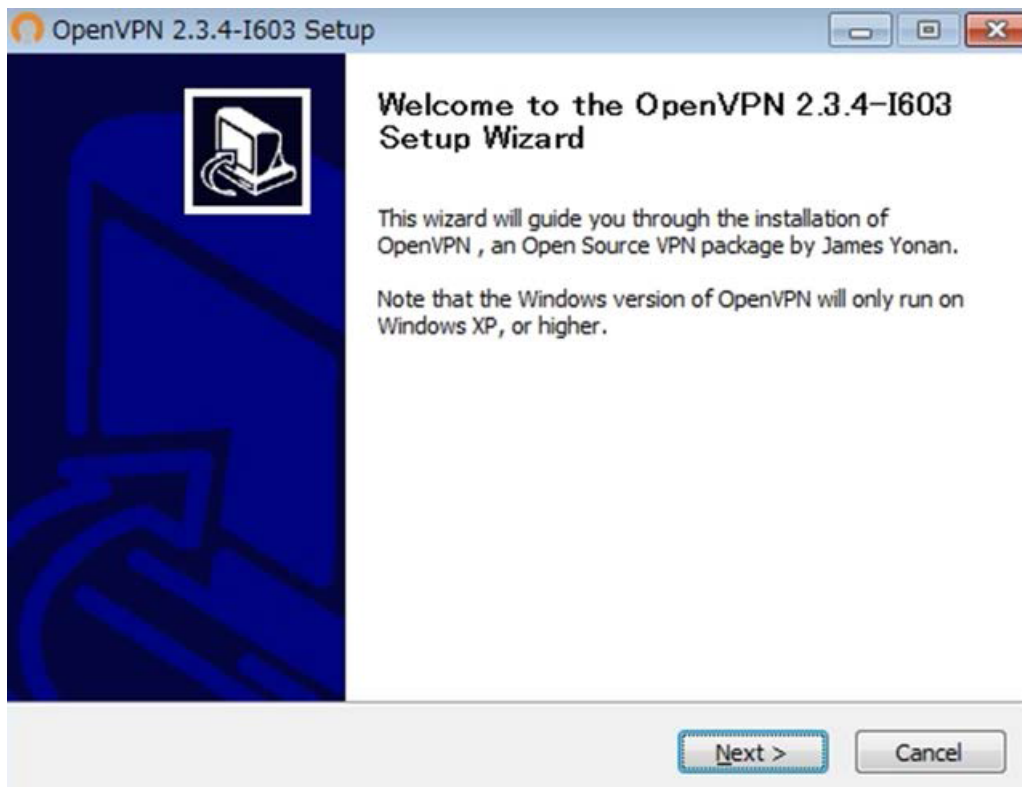
3. Agreement to the terms of the license
   Confirm the displayed terms of the license and click the [I Agree] button.
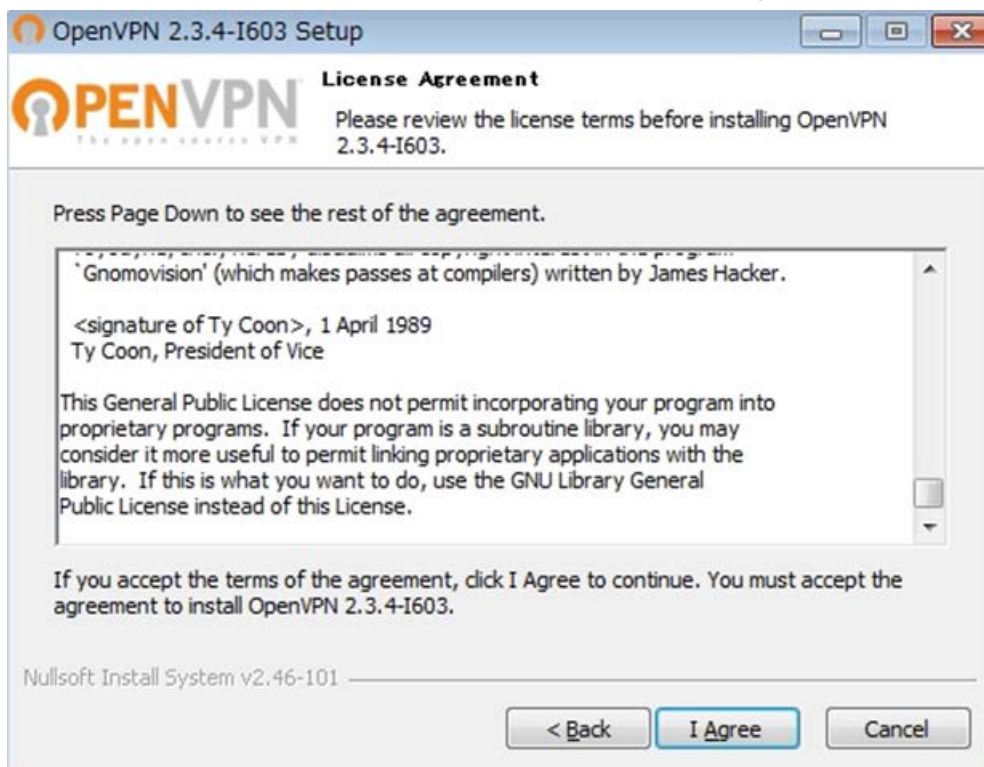
4. Confirmation of the components to be installed
   Click the [Next] button with the default options selected.
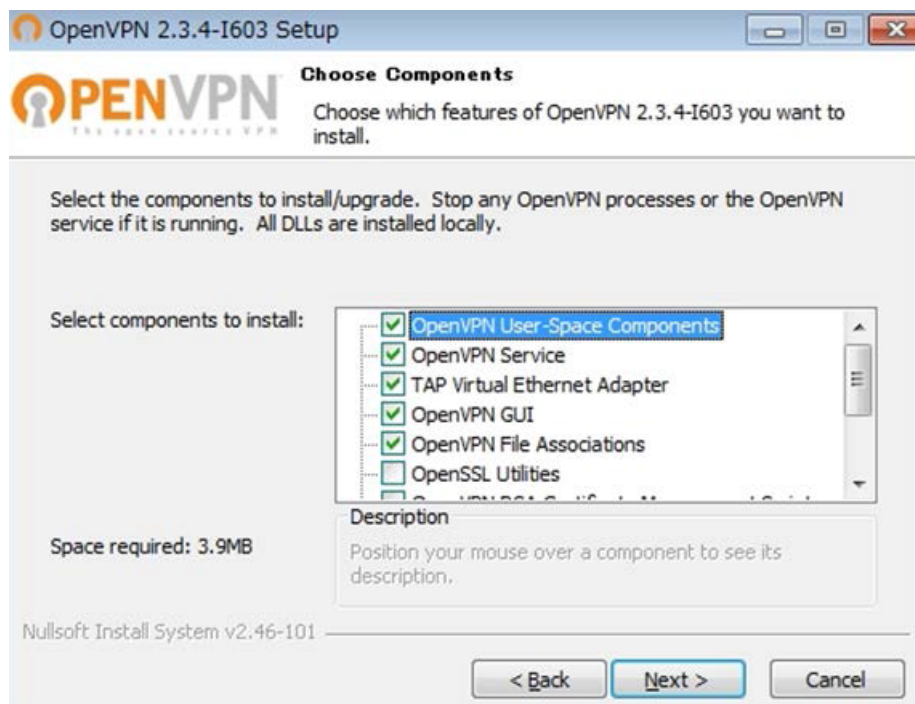
5. Checking of the installation folder
   If you want to use the default folder, click the [Install] button.
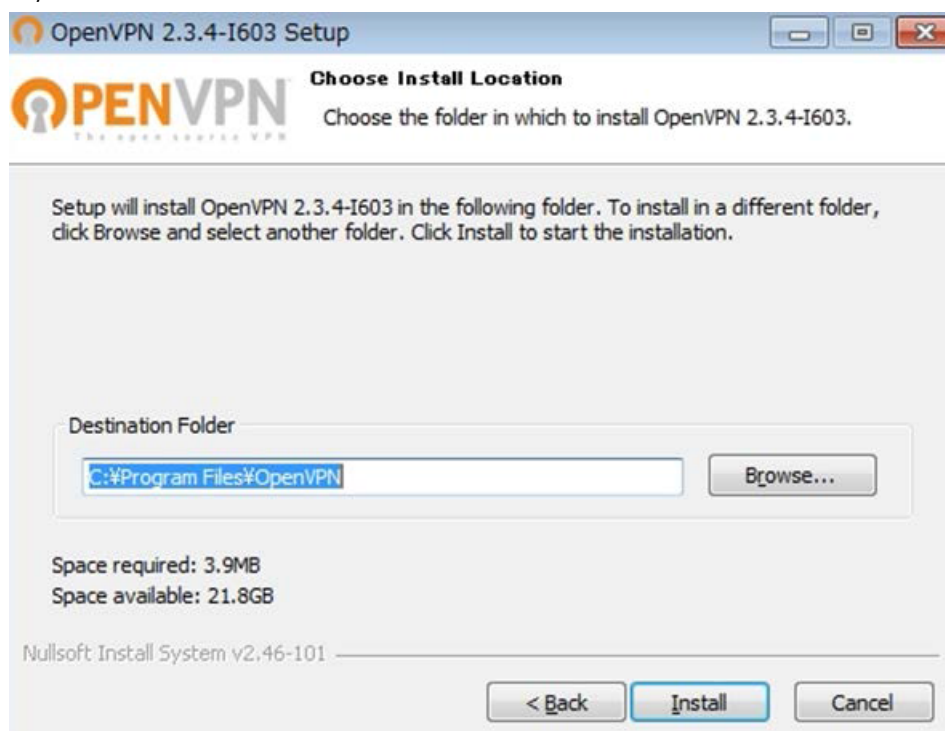
6. Acceptance of the security warning
   Click the [Install] button.
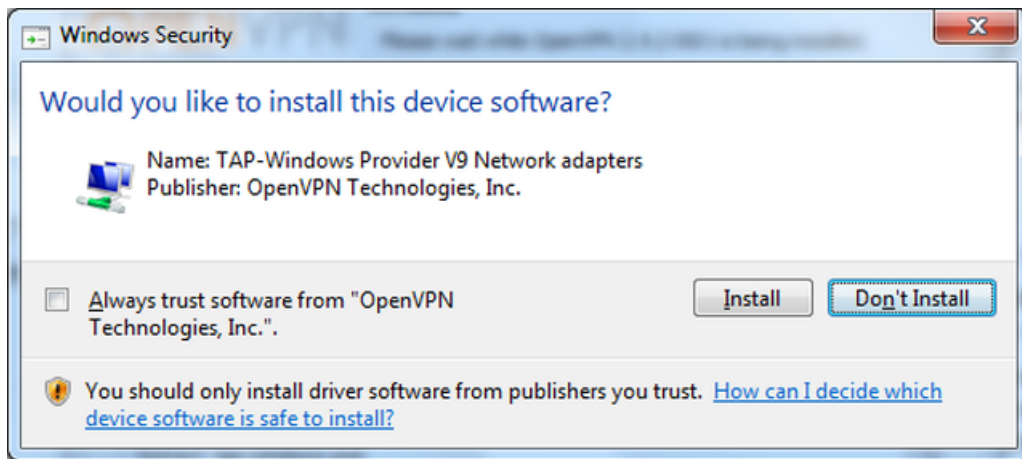
7. Confirmation of installation completion
When the completion screen appears, click the [Next] button.
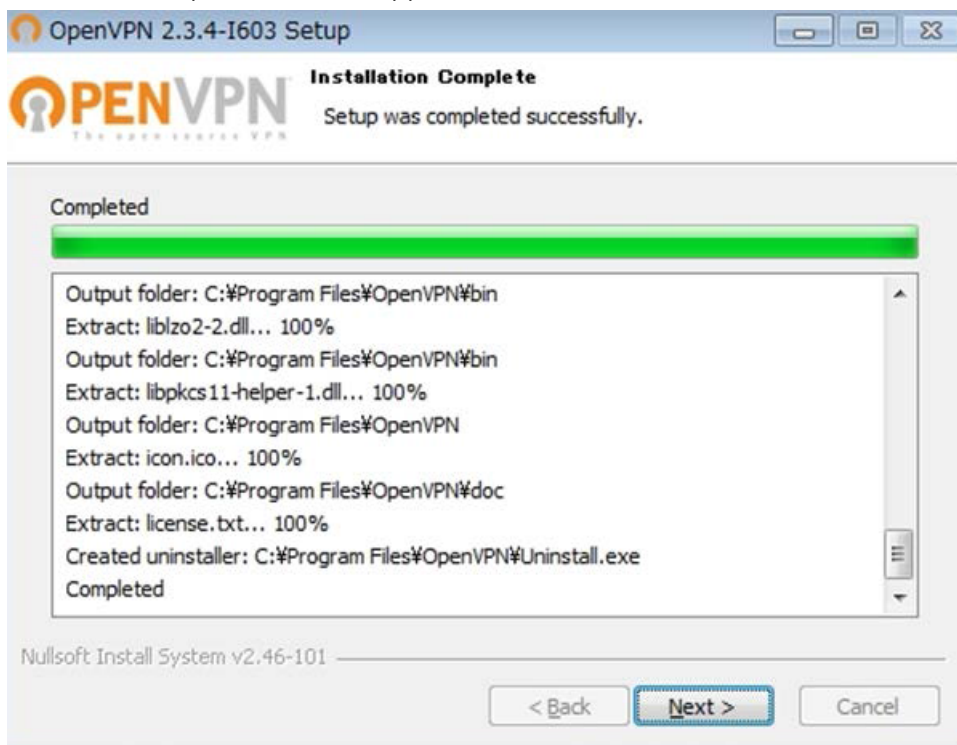
8. Completion of the installation
Click the [Finish] button to finish the installer.
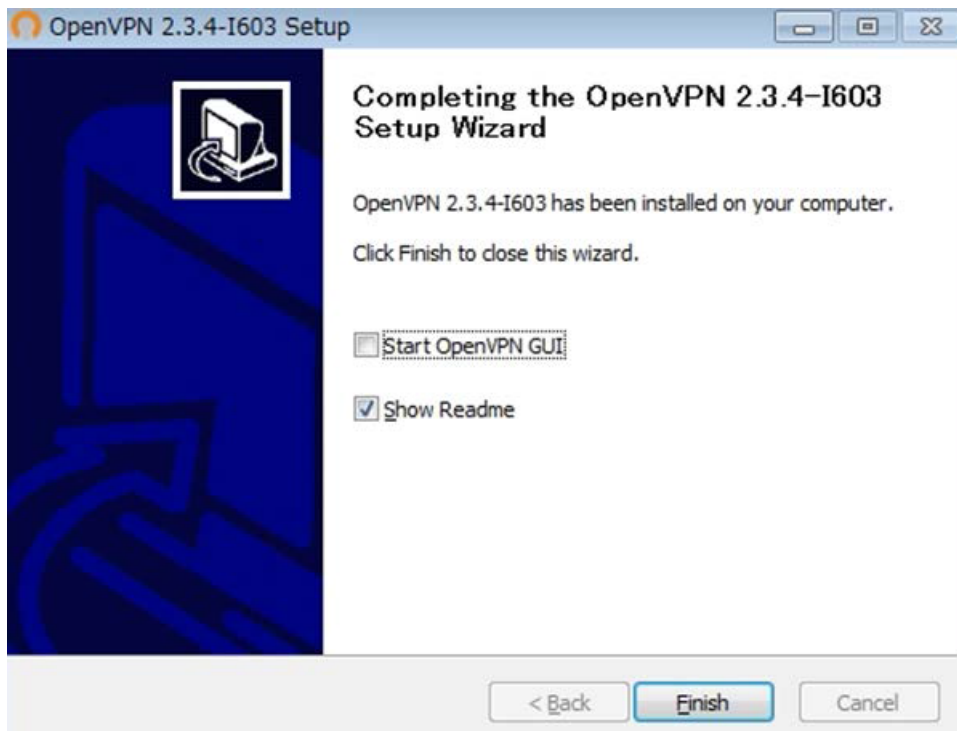
This completes the installation of OpenVPN client.

Set up the OpenVPN client.

1. Storage of certificate files and a key file

```
C:¥Program Files¥OpenVPN¥config¥
```

In the folder above, store the files below, which are prepared in advance. (The file names are shown only as an example.)

- ca.crt: CA certificate
- client.crt: Client certificate
- client.key: Client private key

2. Creation of the client settings file

Create the client settings file using a text editor.

Include the content below in a text file. Copy the text to the text file.

```
client
dev tun
proto tcp
remote xxx.xxx.xxx.xxx 443
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
cipher AES-128-CBC
http-proxy xxx.xxx.xxx.xxx 8080 stdin basic
```

Based on the information of SSL-VPN resources, edit this text file as follows.

Location to Edit (Starting String)	Content to Edit	
proto	Format	proto [protocol (tcp/udp)] * If an HTTP proxy server is involved when using an SSL-VPN connection, specify "tcp".
	Example	proto tcp (when using tcp) proto udp (when using udp)
remote	Format	remote [Connection destination server address (Global IP address of the SSL-VPN Connection resource)] [Connection destination port (443/1194)] *When SSL-VPN Connection resources are in a redundant configuration, enter two lines that start with "remote" and specify one connection destination in each line.
	Example	remote xxx.xxx.xxx.xxx 443 (when using tcp) remote xxx.xxx.xxx.xxx 1194 (when using udp)
ca	Format	ca [Authentication certificate file name]
	Example	ca ca.crt
cert	Format	cert [Client certificate file name]
	Example	cert client.crt
key	Format	key [Client private key file name]
	Example	key client.key
http-proxy	Format	http-proxy [IP address of the HTTP proxy server] [Port number of the HTTP proxy] stdin basic stdin: When connecting to an HTTP proxy server, input of the user name and password will be requested. basic: The authentication method will be basic authentication. * If an HTTP proxy server is not involved when using an SSL-VPN connection, delete this setting.
	Example	http-proxy xxx.xxx.xxx.xxx 8080 stdin basic

> **Note** When using OpenVPN 2.4 or later, add the following line.
>
> ```
> tls-cipher DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
> SHA:DHE-RSA-CAMELLIA128-SHA:AES128-GCM-SHA256:AES128-SHA256:CAMELLIA128-
> SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-
> SHA:ECDH-ECDSA-AES128-SHA
> ```

3. Saving of the edited file

Save the edited file using the folder and file name shown below.

```
C:¥Program Files¥OpenVPN¥config¥client.ovpn
```

> **Tip**
>
> It is possible to change the "client" section of "client.ovpn" to another desired string. It is also possible to prepare multiple files, with one file for each connection destination.

A.9.2 Connection/Disconnection from an OpenVPN Client (Windows)

To connect or disconnect the SSL-VPN Connection resource on IaaS from a PC where an OpenVPN client has been set up, follow the procedure below.

Procedure

1. Starting up of an OpenVPN client
   Click [Start menu] > [OpenVPN] > [OpenVPN GUI].

   > **Note**
   >
   > If you are not logged in as the system administrator, right-click the menu and click [Run as administrator].
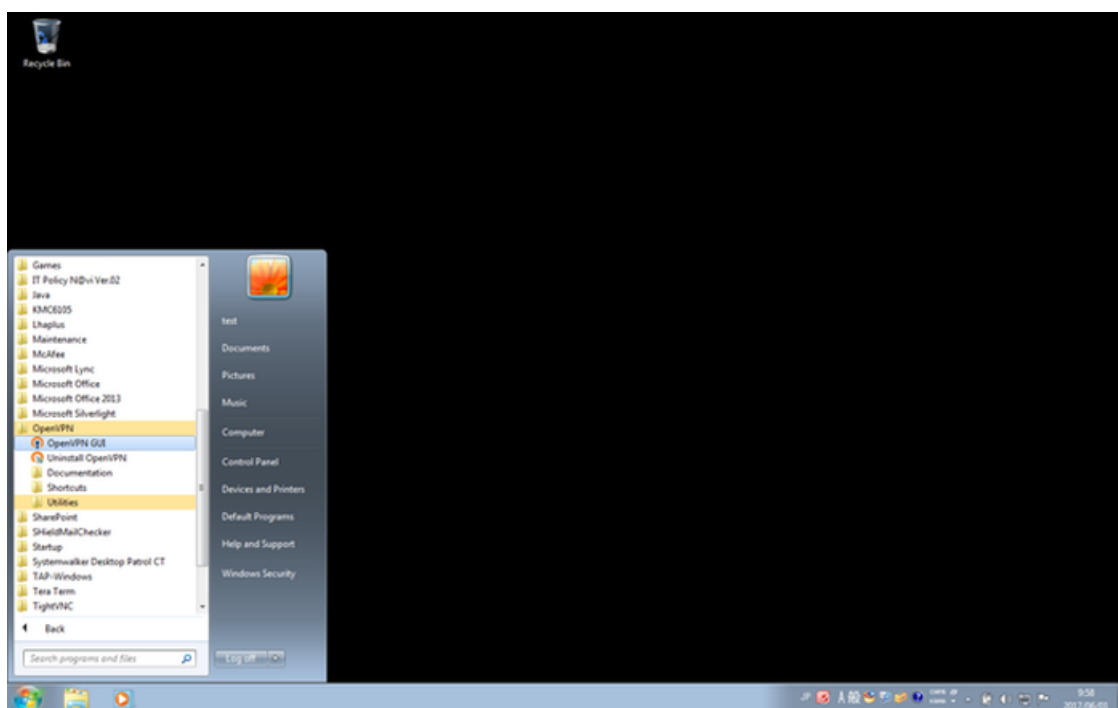
2. SSL-VPN Connection
   Right-click the OpenVPN icon in the notification area of the PC, and click the [Connect] menu.
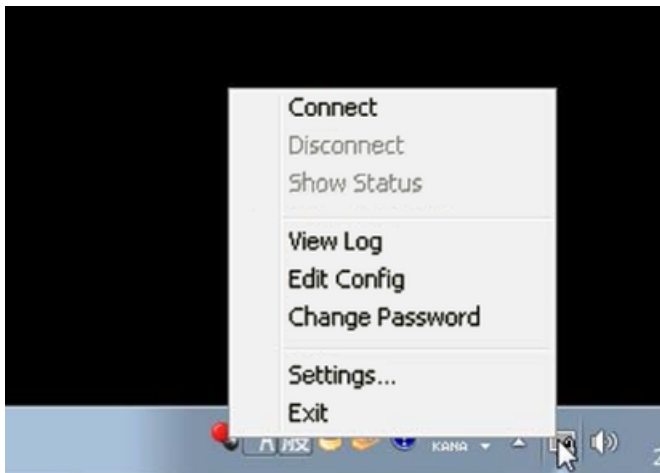
3. Authentication of HTTP proxy servers

If an HTTP proxy server is involved when using an SSL-VPN connection, input the user name and password registered on the HTTP proxy server.
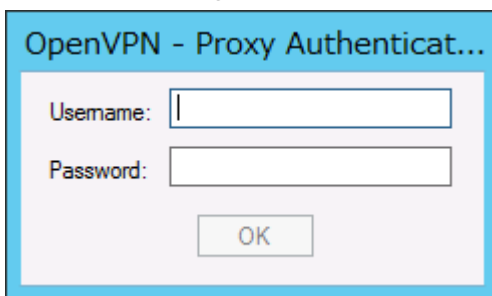
4. Authentication of a client private key

When using an encrypted client private key, enter the password for the client private key.
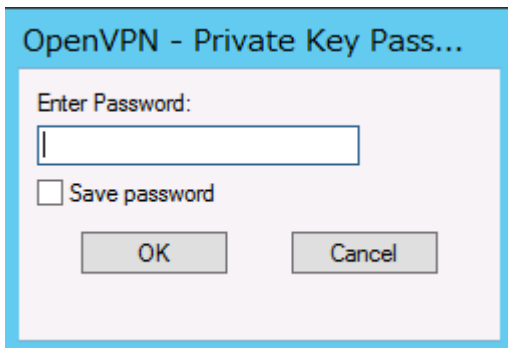
> **Regarding client private key passwords**
> Tip
> • When using a self-signed certificate
>   Use the password specified when converting the client certificate and the private key to the pkcs#12 format.
> • When using a client certificate that was downloaded from the K5 portal
>   Use the password set for the certificate on the K5 portal.

When connection to the SSL-VPN Connection resource is successfully established, the icon in the notification area turns to green.
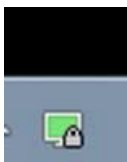
To disconnect, right-click the icon in the notification area and click [Disconnect].

A.10 Setup of an SSL-VPN Client (CentOS)

A.10.1 Setup of an OpenVPN Client (CentOS)

- Obtain the following certificates that are required for building an SSL-VPN connection environment and setting up a client:
  - CA certificate of server certificate
  - Client certificate
  - Client private key
- Fujitsu has confirmed operation of this setup procedure in the following environment:
  - OS: CentOS 6.6 64bit
  - OpenVPN: 2.3.X (X: 10 or later)

> **Note**
> When using OpenVPN 2.3.9 or earlier, uninstall it, and then re-install it following the procedure below.

> **Important**
> In case of using OpenVPN 2.3.9 or earlier, please install again according to following procedure after uninstallation.

To establish an SSL-VPN connection from a PC where CentOS is installed, follow the setup procedure below.

Procedure

1. Acquisition of an OpenVPN client
   Obtain the EPEL repository information from dl.fedoraproject.org.
   http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
2. Installation of the EPEL repository information
   Execute the following command to install the repository information:
   ```
   # rpm -ivh epel-release-6-8.noarch.rpm
   ```
3. Installation of an OpenVPN client
   Execute the following command to install the OpenVPN client:
   ```
   # yum install --enablerepo=epel openvpn
   ```

This completes the installation of OpenVPN client.

Set up the OpenVPN client.

1. Storage of certificate files and a key file
   ```
   /etc/openvpn
   ```

   In the folder above, store the files below, which are prepared in advance. (The file names are shown only as an example.)
   - ca.crt: CA certificate
   - client.crt: Client certificate
   - client.key: Client private key
2. Creation of the client settings file

   Create the client settings file using a text editor.

   Include the content below in a text file. Copy the text to the text file.
   ```
   client
   dev tun
   ```

```
proto tcp
remote xxx.xxx.xxx.xxx 443
resolv-retry infinite
nobind
persist-key
persist-tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/client.crt
key /etc/openvpn/client.key
ns-cert-type server
cipher AES-128-CBC
http-proxy xxx.xxx.xxx.xxx 8080 stdin basic
```

Based on the information of SSL-VPN resources, edit this text file as follows.

Location to Edit (Starting String)	Content to Edit	
proto	Format	proto [protocol (tcp/udp)] * If an HTTP proxy server is involved when using an SSL-VPN connection, specify "tcp".
	Example	proto tcp (when using tcp) proto udp (when using udp)
remote	Format	remote [Connection destination server address (Global IP address of the SSL-VPN Connection resource)] [Connection destination port (443/1194)] *When SSL-VPN Connection resources are in a redundant configuration, enter two lines that start with "remote" and specify one connection destination in each line.
	Example	remote xxx.xxx.xxx.xxx 443 (when using tcp) remote xxx.xxx.xxx.xxx 1194 (when using udp)
ca	Format	ca [Authentication certificate file name]
	Example	ca ca.crt
cert	Format	cert [Client certificate file name]
	Example	cert client.crt
key	Format	key [Client private key file name]
	Example	key client.key
http-proxy	Format	http-proxy [IP address of the HTTP proxy server] [Port number of the HTTP proxy] stdin basic stdin: When connecting to an HTTP proxy server, input of the user name and password will be requested. basic: The authentication method will be basic authentication. * If an HTTP proxy server is not involved when using an SSL-VPN connection, delete this setting.
	Example	http-proxy xxx.xxx.xxx.xxx 8080 stdin basic

3. Saving of the edited file
   Save the edited file using the folder and file name shown below.

```
/etc/openvpn/client.ovpn
```

> 💡 **Tip** It is possible to change the "client" section of "client.ovpn" to another desired string. It is also possible to prepare multiple files, with one file for each connection destination.

A.10.2 Connection/Disconnection from an OpenVPN Client (CentOS)

To connect or disconnect the SSL-VPN Connection resource on IaaS from a PC where an OpenVPN client has been set up, follow the procedure below.

Procedure

1. Starting up of an OpenVPN client

   Execute the following command to start the OpenVPN client:

   ```
   # /usr/sbin/openvpn /etc/openvpn/client.ovpn
   ```

2. Authentication of HTTP proxy servers

   If an HTTP proxy server is involved when using an SSL-VPN connection, input the user name and password registered on the HTTP proxy server.

   ```
   Enter HTTP Proxy Username: <User name for the HTTP proxy server>
   Enter HTTP Proxy Password: <Password for the HTTP proxy server>
   ```

3. Authentication of a client private key

   When using an encrypted client private key, enter the password for the client private key.

   ```
   Enter Private Key Password: <Password for the client private key>
   ```

   > 💡 **Tip** Regarding client private key passwords
   > - When using a self-signed certificate
   >
   >   Use the password specified when converting the client certificate and the private key to the pkcs#12 format.
   > - When using a client certificate that was downloaded from the K5 portal
   >
   >   Use the password set for the certificate on the K5 portal.

4. Checking of SSL-VPN connection status

   ```
   [root@centos66 openvpn]# /usr/sbin/openvpn /etc/openvpn/client.ovpn &
   [1] 31279
   [root@centos66 openvpn]# Sat Nov 22 17:00:50 2014 OpenVPN 2.3.2 x86_64-redhat-linux-gnu
   [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [eurephia] [MH] [IPv6] built on Sep 12 2013
   Sat Nov 22 17:00:50 2014 UDPv4 link local: [undef]
   Sat Nov 22 17:00:50 2014 UDPv4 link remote: [AF_INET]172.21.2.40:1194
   Sat Nov 22 17:00:50 2014 [server] Peer Connection Initiated with
   [AF_INET]172.21.2.40:1194
   Sat Nov 22 17:00:53 2014 TUN/TAP device tun0 opened
   Sat Nov 22 17:00:53 2014 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
   Sat Nov 22 17:00:53 2014 /sbin/ip link set dev tun0 up mtu 1500
   Sat Nov 22 17:00:53 2014 /sbin/ip addr add dev tun0 local xxx.xxx.xxx.xxx peer
   yyy.yyy.yyy.yyy
   Sat Nov 22 17:00:53 2014 Initialization Sequence Completed
   ```

   Content to check:

   - 2nd line: Process number in which connection is executed. Used for disconnecting the SSL-VPN connection.
   - 10th line: Confirm that "peer yyy.yyy.yyy.yyy", which indicates that the peer address is allocated, is displayed.
   - 11th line: Confirm that "Completed", which notifies that startup has been completed, is output.

To disconnect, input the following command to end the OpenVPN client process:

```
# pgrep openvpn
# kill [Process number]
```

or

```
# killall openvpn
```

A.11 Connecting to a Virtual Server OS through an SSL-VPN Connection

This section describes the procedure for building a network environment that allows you to log in to a virtual server through an SSL-VPN connection.

To create an environment for an SSL-VPN connection, prepare the following items for server and client use, respectively. The file names below should be read as the names of the files that you created.

- For server use
  - Certification Authority certificate (ca.crt)
  - Server certificate (server.crt)
  - Server private key (server.key)
  - DH private key (dh2048.pem)
- For client use
  - Certificate Authority certificate file (ca.crt, shared for server use)
  - Client certificate (client_001.crt)
  - Client private key (client_001.key)

> **Note**
> Prepare an unencrypted server private key.

Follow the steps below to build an SSL-VPN connection environment and log in to the OS of the virtual server. If necessary, adjust the value for each resource according to the system you use.
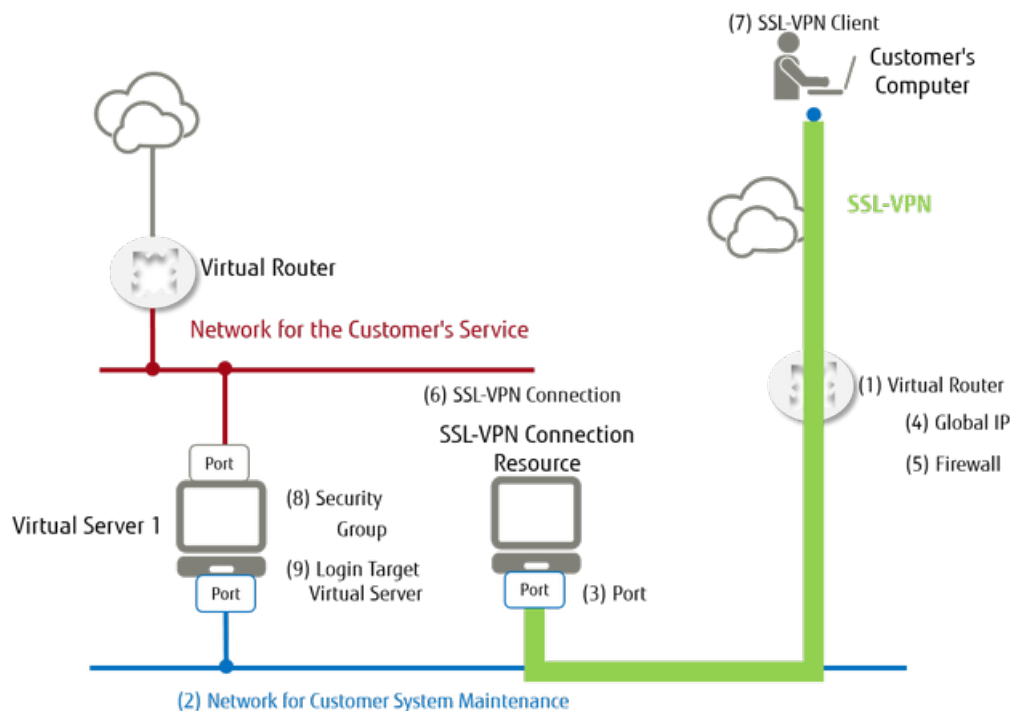
Figure 58: Building an SSL-VPN environment

Procedure

1. Obtaining a global IP address

   Obtain a global IP address from an external network that is in the same availability zone as the virtual server that you want to connect.

<div align="center">Table 205: Example Settings</div>

Item	Value
External Network ID	ID of 'inf_az1_ext-net01'
Availability Zone Name	jp-west-2a

2. Creating a virtual network for SSL-VPN

<div align="center">Table 206: Example Settings</div>

Item	Value
Availability Zone Name	jp-west-2a
Virtual Network Name	SSL-VPN_Network

3. Creating a subnet for SSL-VPN

   Create a subnet in the virtual network for SSL-VPN that you created.

<div align="center">Table 207: Example Settings</div>

Item	Value
Subnet Name	SSL-VPN_Subnet
Virtual Network ID	ID of 'SSL-VPN_Network'
IP Version	IPv4
Network Address Range	172.18.1.0/24 Note — Use a prefix length of 16 - 29 bits.
Gateway Address	172.18.1.1 Note — Make sure that you specify the IP address of the port of the virtual router for SSL-VPN. Do not delete this after it has been specified.
DHCP	true
Availability Zone Name	jp-west-2a

Item	Value
DNS Server	133.162.145.9 133.162.145.10
Host Root	CIDR : 192.168.1.0/24 Destination IP Address : 172.18.1.1

4. Creating a virtual router for SSL-VPN

Table 208: Example Settings

Item	Value
Virtual Router Name	SSL-VPN_Router
Availability Zone Name	jp-west-2a

5. Setting up a gateway for the virtual router for SSL-VPN
   Change the following information of the SSL-VPN virtual router that you created.

Table 209: Example Settings

Item	Value
External Network ID	ID of 'inf_az1_ext-net01'

6. Connecting the virtual router for SSL-VPN to the subnet

   Update the setting information of the virtual router for SSL-VPN, and then connect to the subnet for SSL-VPN. For details, refer to "Changing the information of a virtual router (attaching to a subnet)" in the "API User Guide".

Table 210: Example Settings

Item	Value
Virtual Router ID	ID of 'SSL-VPN_Router'
Subnet ID	ID of 'SSL-VPN_Subnet'

7. Creating firewall rules for SSL-VPN

   Create rules to allow certain traffic and to block other, based on the conditions under which traffic can pass through to the OS.

Table 211: Example Settings for Allowing Traffic

Item	Value
Name of Firewall Rule	SSL-VPN_FW_rule01_tcp22
Protocol	tcp
Source IP Address	192.168.1.0/24
Source Port Number	1:65535
Destination IP Address	0.0.0.0/0

Item	Value
Destination Port Number	22 💡 Tip Specify '3389' for Windows RDP connection
Actions	allow
Availability Zone Name	jp-west-2a

Table 212: Example Settings for Blocking Traffic

Item	Value
Name of Firewall Rule	SSL-VPN_FW_rule_all_deny
Actions	deny
Availability Zone Name	jp-west-2a

8. Creating a firewall policy for SSL-VPN
   Compile the firewall rules that you created into a firewall policy.

Table 213: Example Settings

Item	Value
Firewall Policy Name	SSL-VPN_Firewall_Policy
List of Firewall Rules	Specify the following IDs that represent firewall rule lists that you created: • ID of 'SSL-VPN_FW_rule01_tcp22' • ID of 'SSL-VPN_FW_rule_all_deny'
Availability Zone Name	jp-west-2a

9. Creating a firewall for SSL-VPN
   Create a firewall by associating the created firewall policy with the virtual router for SSL-VPN.

Table 214: Example Settings

Item	Value
Firewall Name	SSL-VPN_Firewall
Firewall Policy ID	ID of 'SSL-VPN_Firewall_Policy'
Virtual Router ID	ID of 'SSL-VPN_Router'
Availability Zone Name	jp-west-2a

10. Registering a Certificate Authority certificate for SSL VPN
    Use the key management service to register the Certificate Authority certificate.

Table 215: Example Settings

Item	Value
Key Metadata Name	ca

Item	Value
Confidential Information (payload)	-----BEGIN CERTIFICATE-----\n (character string where the line break codes in the payload of ca.crt are replaced with '\n') \n-----END CERTIFICATE-----
Content Type for Confidential Information	text/plain
Retention Period	2025-12-31T23:59:59

11. Registering a server certificate for SSL VPN
    Use the key management service to register the server certificate.

Table 216: Example Settings

Item	Value
Key Metadata Name	server_certificate
Confidential Information (payload)	-----BEGIN CERTIFICATE-----\n (character string where the line break codes in the payload of server.crt are replaced with '\n') \n-----END CERTIFICATE-----
Content Type for Confidential Information	text/plain
Retention Period	2025-12-31T23:59:59

12. Registering the server's private key for SSL-VPN
    Use the key management service to register the server's private key.

Table 217: Example Settings

Item	Value
Key Metadata Name	server_key
Confidential Information (payload)	-----BEGIN PRIVATE KEY-----\n (character string where the line break codes in the payload of server.key are replaced with '\n') \n-----END PRIVATE KEY-----
Content Type for Confidential Information	text/plain
Retention Period	2025-12-31T23:59:59

13. Registering a DH private key for SSL-VPN
    Use the key management service to register a DH private key.

Table 218: Example Settings

Item	Value
Key Metadata Name	dh
Confidential Information (payload)	-----BEGIN DH PARAMETERS-----\n (character string where the line break codes in the payload of dh2048.pem are replaced with '\n') \n-----END DH PARAMETERS-----
Content Type for Confidential Information	text/plain
Retention Period	2025-12-31T23:59:59

14. Creating a key metadata container for SSL-VPN

Create a key metadata container for the four certificates and private keys that you created in the above procedures.

<p style="text-align:center"><u>Table 219: Example Settings</u></p>

Item	Value
Key Metadata Container Name	SSL-VPN_VPNCredential
Key Metadata Type	generic
Key Metadata List	Specify as a list of objects with the following elements: • 'name': Specify all of the following key metadata as the name 　• For a Certification Authority certificate: ca 　• For a server certificate: server_certificate 　• For a server private key: server_key 　• For a DH private key: dh • 'secret_ref': Specify the value of 'secret_ref,' generated when the key metadata was created

Example Settings of a Key Metadata List

```
{
  "name": "SSL-VPN_VPNCredential",
  "type": "generic",
  "secret_refs": [
    {
      "name": "ca",
      "secret_ref": "https://keymanagement. jp-west-2. cloud. global. fujitsu. com/v1/
{Project ID}/secrets/{ID of Certificate Authority certificate key metadata}"
    },
    {
      "name": "server_certificate",
      "secret_ref": "https://keymanagement. jp-west-2. cloud. global. fujitsu. com/v1/
{Project ID}/secrets/{ID of server certificate key metadata}"
    },
    {
      "name": "server_key",
      "secret_ref": "https://keymanagement. jp-west-2. cloud. global. fujitsu. com/v1/
{Project ID}/secrets/{ID of server private key metadata}"
    },
    {
      "name": "dh",
      "secret_ref": "https://keymanagement. jp-west-2. cloud. global. fujitsu. com/v1/
{Project ID}/secrets/{ID of DH private key metadata}"
    }
  ]
}
```

15. Setting up a VPN service for SSL-VPN

Set up a VPN service that connects to the SSL-VPN subnet via the SSL-VPN virtual router.

<p style="text-align:center"><u>Table 220: Example Settings</u></p>

Item	Value
Name of VPN Service	SSL-VPN_Service

Item	Value
Subnet ID	ID of 'SSL-VPN_Subnet'
Virtual Router ID	ID of 'SSL-VPN_Router'
admin_state_up	true
Availability Zone Name	jp-west-2a

16. Setting up an SSL-VPN connection

Set up an SSL-VPN connection by associating the created VPN service for SSL-VPN with the key metadata container for SSL-VPN.

Table 221: Example Settings

Item	Value
Name of SSL-VPN Connection	SSL-VPN_Connection
Client Address Pool	192.168.1.0/24
Key Metadata Container ID	ID of 'SSL-VPN_VPNCredential'
VPN Service ID	ID of 'SSL-VPN_Service'
Protocol	tcp
Global IP	ID of 'Global IP Address'
Availability Zone Name	jp-west-2a

> **Tip**
>
> IP addresses in the client address pool are consumed based on the following formula.
>
> Amount of consumed IP addresses = The number of VPN clients x 4 + 8 (8 are consumed by the VPN server)
>
> Specify a subnet prefix value in the range of 16 - 29.
>
> However, when the prefix value is 29, the above formula will not be applied, and only one client can be connected.

17. Setup of the client environment for the SSL-VPN connection

To set up the client for the SSL-VPN connection, refer to the relevant section in the appendix.

- Setup of an OpenVPN Client (Windows)
- Setup of an OpenVPN Client (CentOS)

After setting up the client environment, check whether you can successfully connect through SSL-VPN.

18. Connecting the virtual server to the virtual network for SSL-VPN

After setting up an environment where SSL-VPN connection is available, connect or create a virtual server in 'SSL-VPN virtual network.'

> **Note**
>
> When you connect an existing virtual server to 'SSL-VPN virtual network,' you need to add a port. Log in to the virtual server from the existing network, and then adjust the network adapter settings of the OS according to the IP address of the added port.

19. Logging in to the OS

Log in to the OS of the virtual server via the SSL-VPN connection, using SSH or remote desktop protocol.

> 💡 **Tip**
> If you are unable to connect, check the settings of 'Firewall rules for SSL-VPN' to verify whether communication for OS login is allowed.

Related concepts

SSL-VPN Connection
The SSL-VPN connection function allows you to make secure connections to a virtual environment built on the system, and to log in to the virtual server to perform management operations.

A.12 Setup of SQL Server

A.12.1 Microsoft SQL Server Usage Guide

This section describes the procedure to make Microsoft SQL Server available after creating a virtual server from an image equipped with Microsoft SQL Server.

Use an image equipped with Microsoft SQL Server to create a virtual server.

Complete setup of Microsoft SQL Server using the procedure below.

> 💡 **Tip**
> The screenshots used in the following procedure are of Microsoft SQL Server 2014.

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.
> - If the Program Compatibility Assistant window is displayed, click the [Run program] button.

2. Installation of Microsoft SQL Server is performed automatically as shown below.
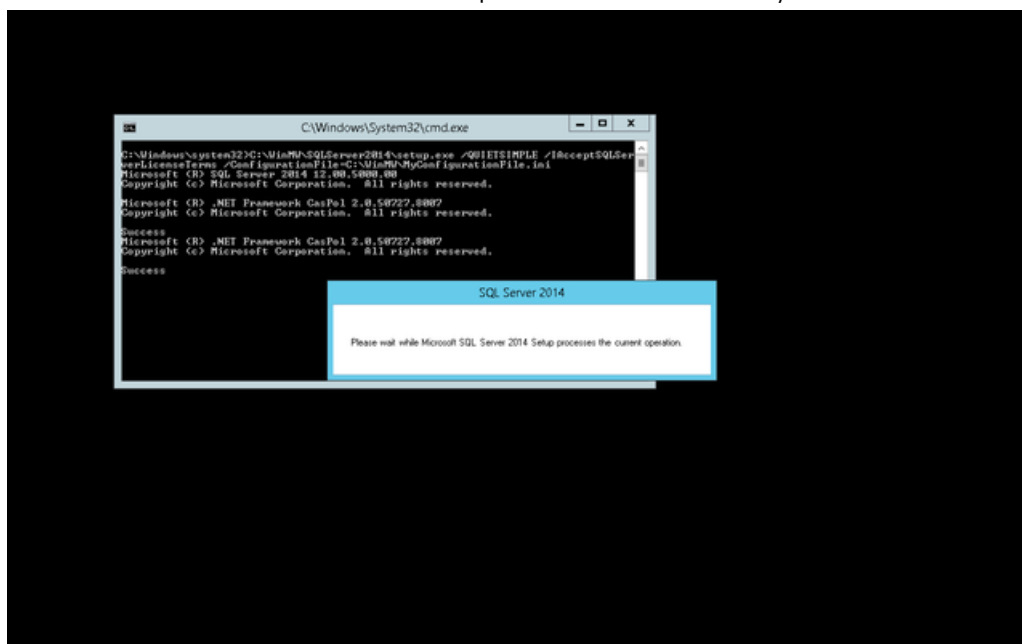
3. When installation is completed, the password file for the Microsoft SQL Server administration account is created on the desktop.

> The Microsoft SQL Server administration account name is "SQLServerAdmin".
>
> Tip
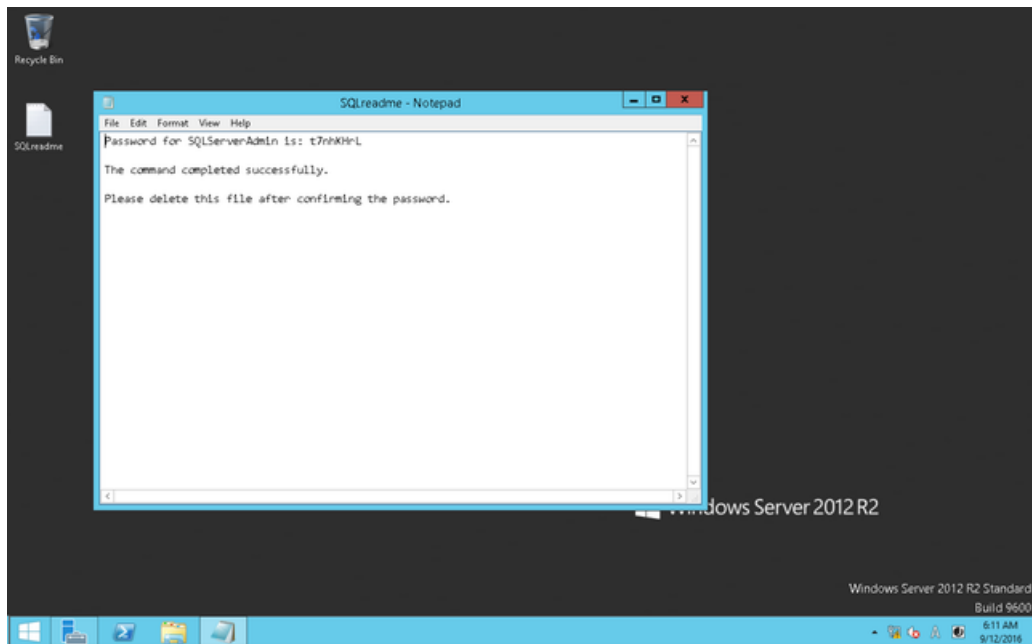
4. To use the "SQLServerAdmin" account to connect to Integration Services, change the account type to [Administrator].
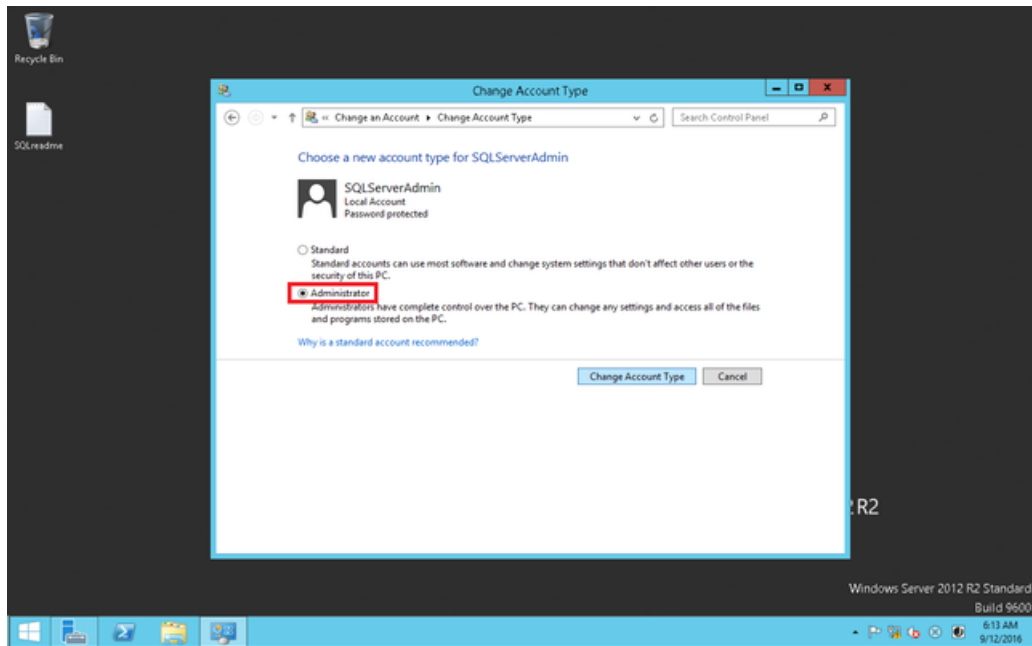
Tip

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.

a. From the Start menu, click [Control Panel] > [System and Security] > [System] > [Remote settings].
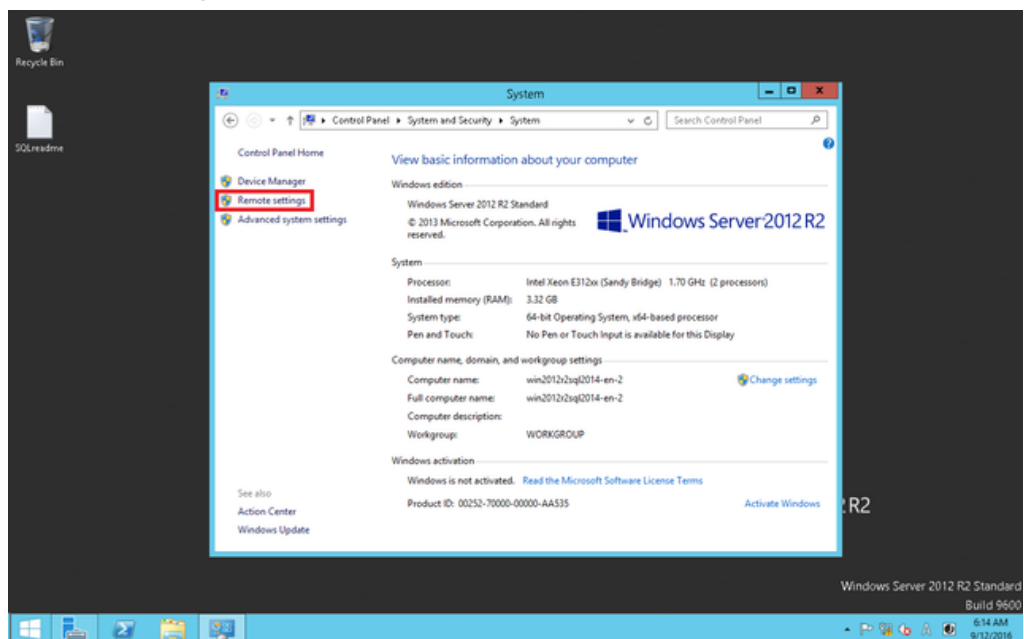
b. In the [Remote Desktop] dialog box, click the [Select Users] button.

---
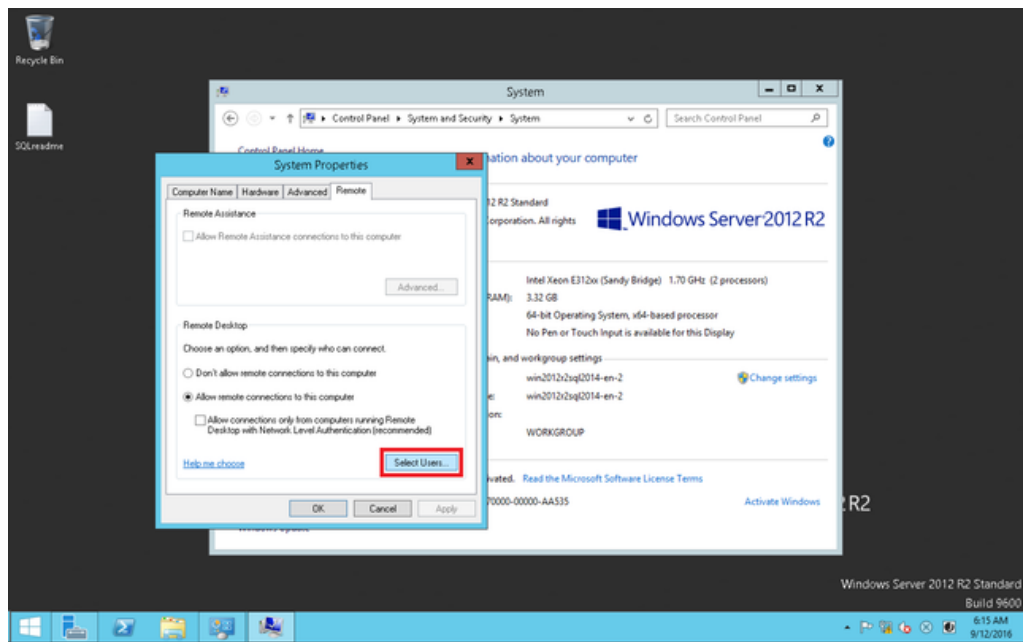
c. In the [Remote Desktop Users] dialog box, click the [Add] button.
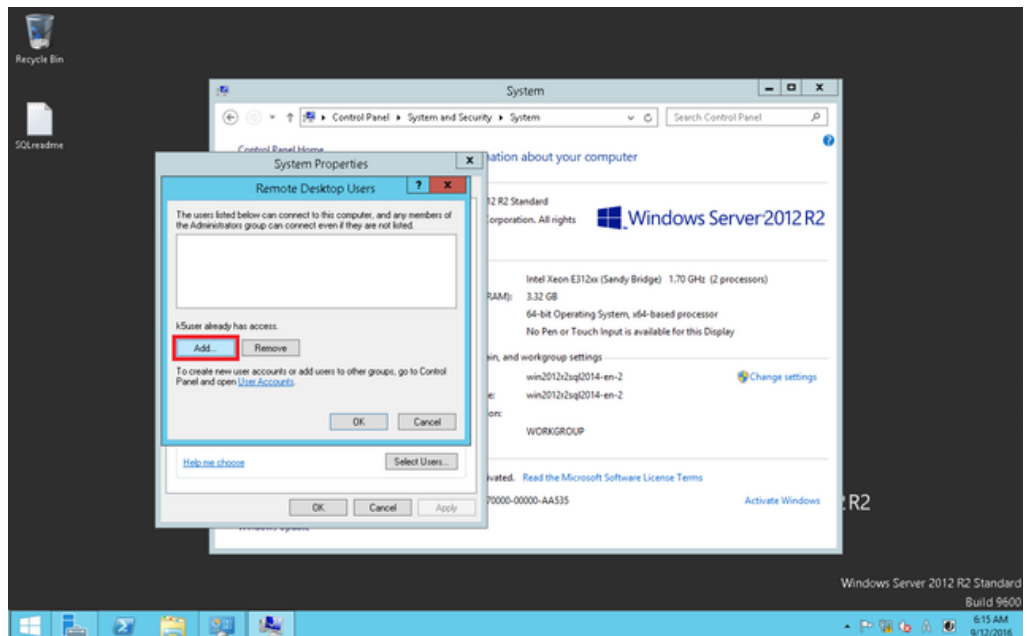
d. In the [Select Users] dialog box, enter "SQLServerAdmin" in the [Enter the object names to select] field and click the [Check Names] button.
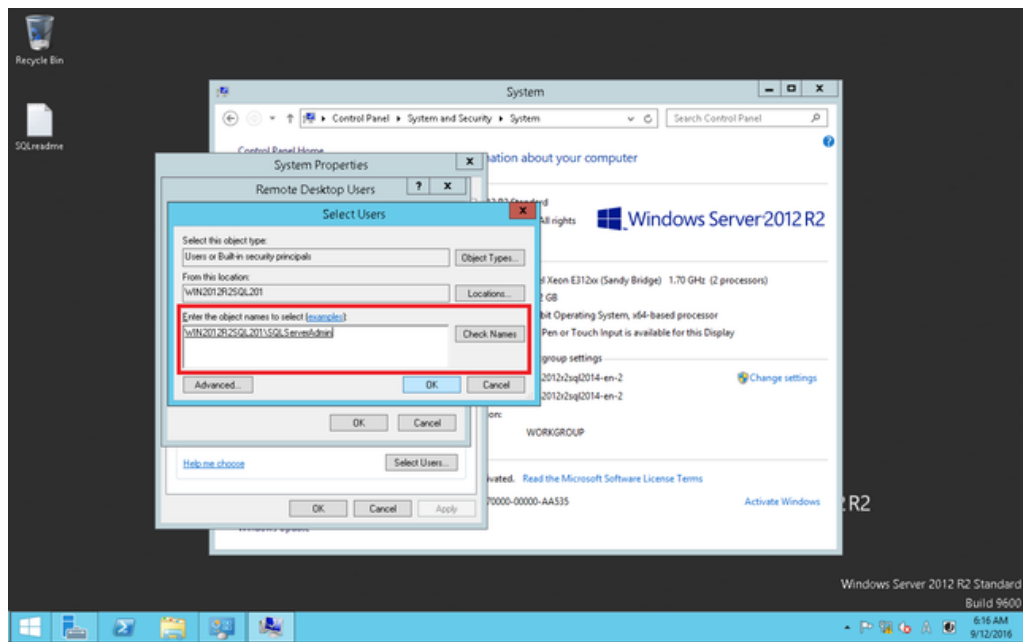
e. Click the [OK] button.

f. In the [Remote Desktop Users] dialog box, confirm that "SQLServerAdmin" has been added.
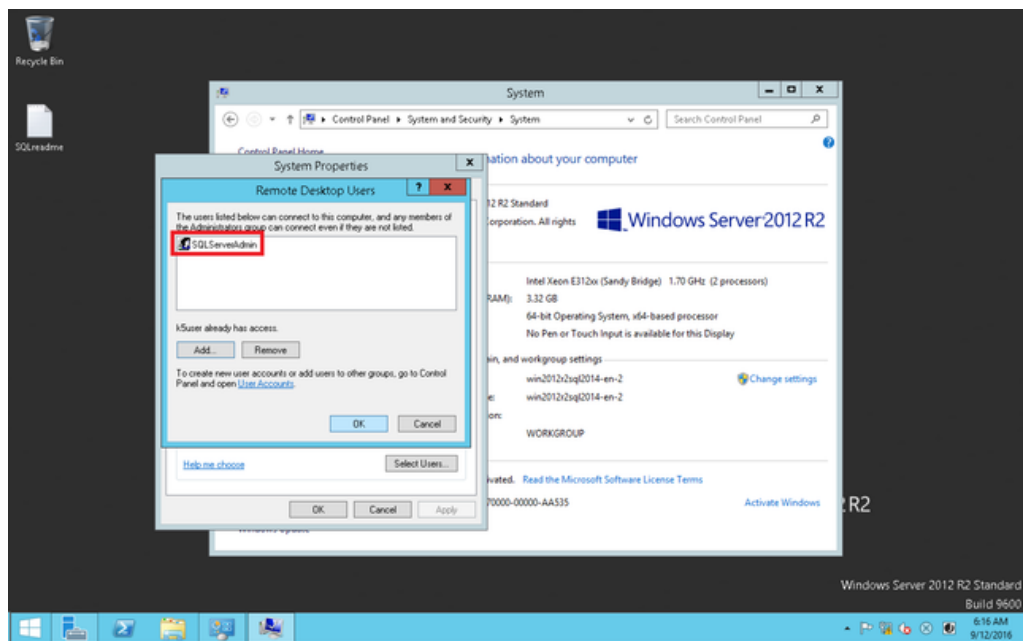
5. Restart the virtual server.

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.
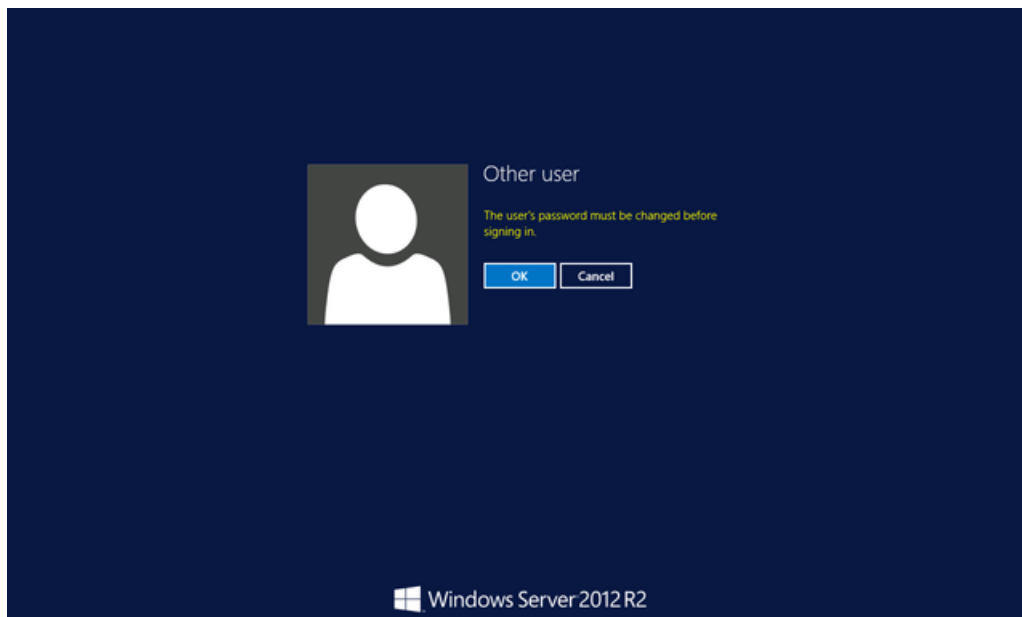
7. Select [Apps] > [SQL Server Management Studio].

>   Tip
>
> a. When you select SQL Server Management Studio, right-click it and then click [Run as administrator].
> b. In [User Account Control], enter the password for k5user.

8. Confirm that a connection can be established with the "SQLServerAdmin" account.
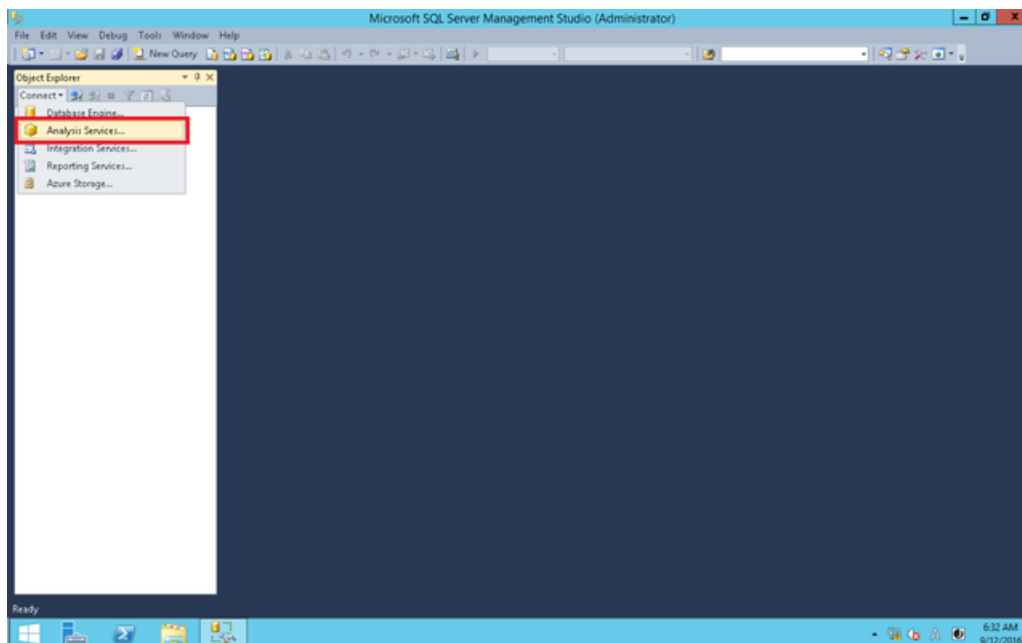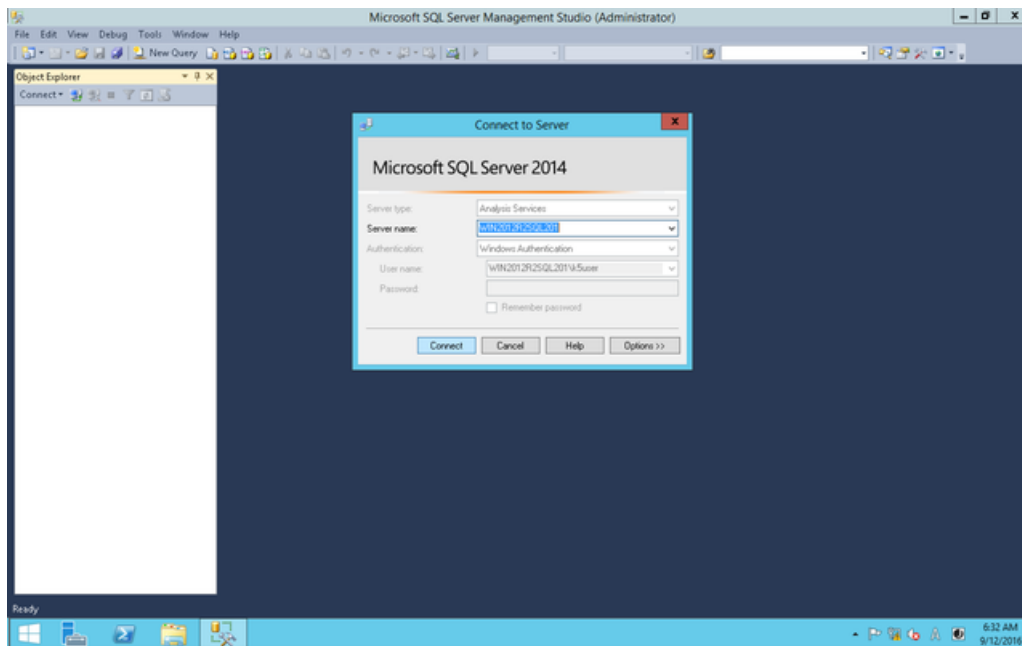
This completes the setup procedure.

Table 222: List of Execution Accounts for SQL Server 2008 Related Services

Service	Account Name
SQL Server Agent	NT AUTHORITY\NETWORK SERVICE
SQL Server Database Engine	NT AUTHORITY\NETWORK SERVICE
SQL Server Analysis Services	NT AUTHORITY\NETWORK SERVICE
SQL Server Reporting Services	NT AUTHORITY\NETWORK SERVICE
SQL Server Integration Services	NT AUTHORITY\NETWORK SERVICE

Table 223: List of Execution Accounts for SQL Server 2014 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
SQL Server Distributed Replay Controller	NT Service\SQL Server Distributed Replay Controller

A.13 Protocols and Cipher Suites Supported by API Endpoint

The API endpoints that are provided by IaaS support the following combinations of protocols and Cipher Suites.

Table 224: List of Available Cipher Suites

SSL Protocol	SSL Cipher Suites
TLS1.1	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1.2	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

A.14 Using a Downloaded Key Pair (*.pem) with PuTTY.exe

This section describes how to download a key pair created with IaaS and use it with the SSH client software 'PuTTY.'

To convert *.pem files downloaded from IaaS to *.ppk files, follow the steps below.

Procedure

1. Starting the PuTTY Key Generator
   Start PuTTY by double-clicking 'puttygen.exe' in the folder in which it is installed.
2. Load the *.pem file
   Click [Load] and select the *.pem file downloaded from IaaS.

   > **Tip**
   > In the dialog box, change the file type to [All Files(*.*)] and select the *.pem file.
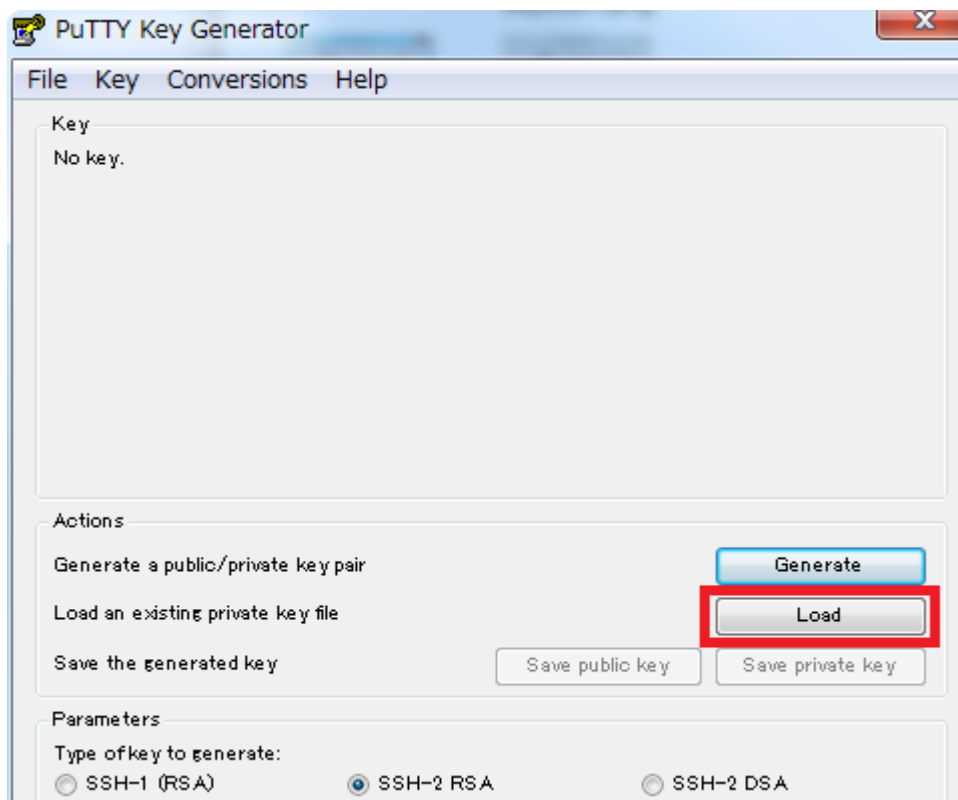
The following message will be displayed. Click [OK] to proceed.
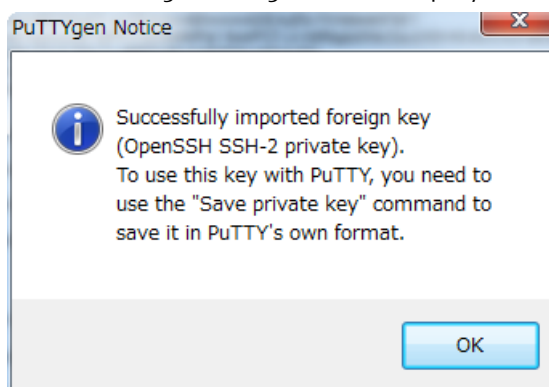
3. Saving the *.ppk file

Click [Save private key] and save the file as a *.ppk file in a folder of your choice.
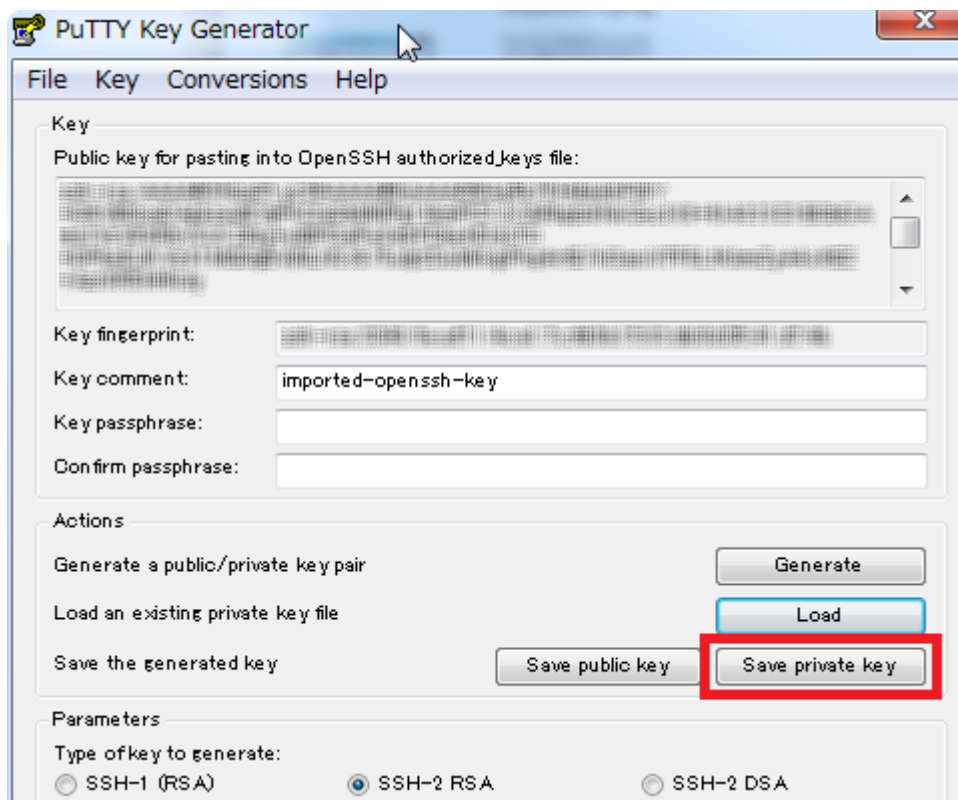
Specify the saved *.ppk file on the SSH authentication setting screen to use it.
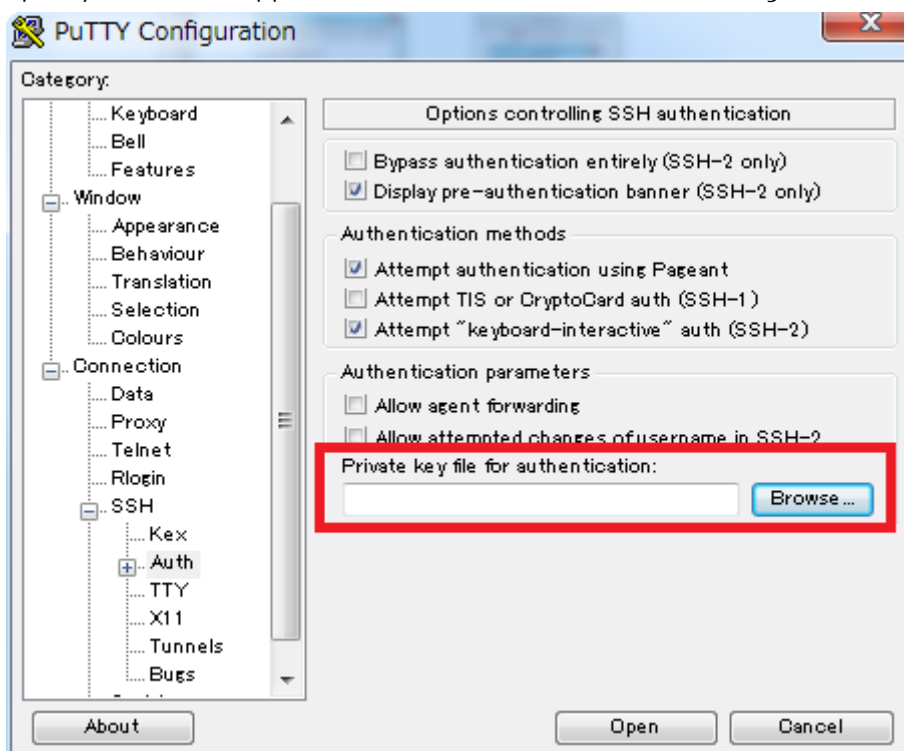
A.15 Procedure for Connecting to the WSUS (Windows Server Update Services) Server

This section describes how to connect to WSUS (Windows Server Update Services) provided by IaaS.

- The targets for connection are Windows virtual servers that are available in IaaS. This section describes the procedure for Windows 2012.
- Check that the following conditions apply to the server on which you want to configure WSUS.
  - In the security group's egress rules, permission is granted to use 8530/tcp and 53/udp.
  - In the Windows Firewall rules for incoming and outgoing connections, permission is granted to use 8530/tcp and 53/udp.

The following section describes how to connect to a WSUS server.

Procedure

1. Logging in to the Windows virtual server

   Log in to your Windows virtual server. To log in to the server, use the default user name 'k5user' or log in as a user who belongs to the administrator group.

2. Starting the command prompt

   a. Right-click the [Windows] button, and then click [Command Prompt (Admin)].
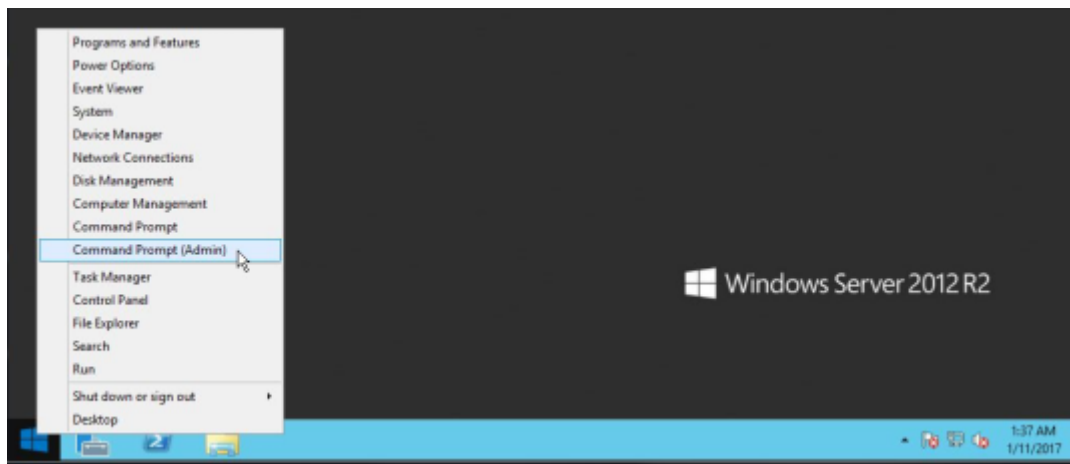
   b. When the User Account Control dialog box appears, click [Yes].

3. Starting the Local Group Policy Editor

   At the command prompt, run the following command. Alternatively, click Run, and enter 'gpedit.msc' to execute it.

   `C:¥Users¥Administrator>gpedit.msc`
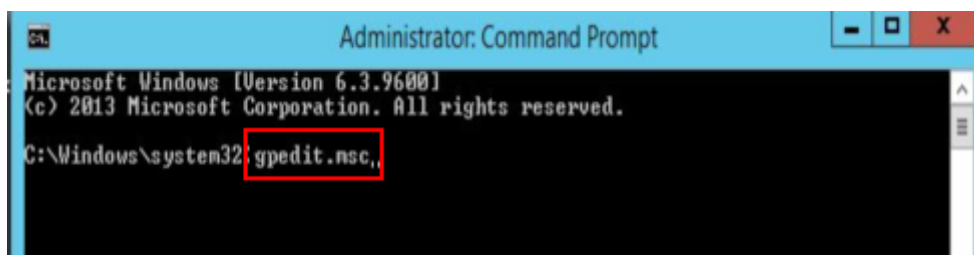
4. Configuring settings for Windows Update
   a. In the left-hand tree of the Local Group Policy Editor, click [Local Computer Policy] > [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Update].
   b. Double-click [Configure Automatic Updates]. In the screen to configure automatic updates, select [Enabled], and then click [OK].
   c. Double-click [Specify intranet Microsoft update service location].
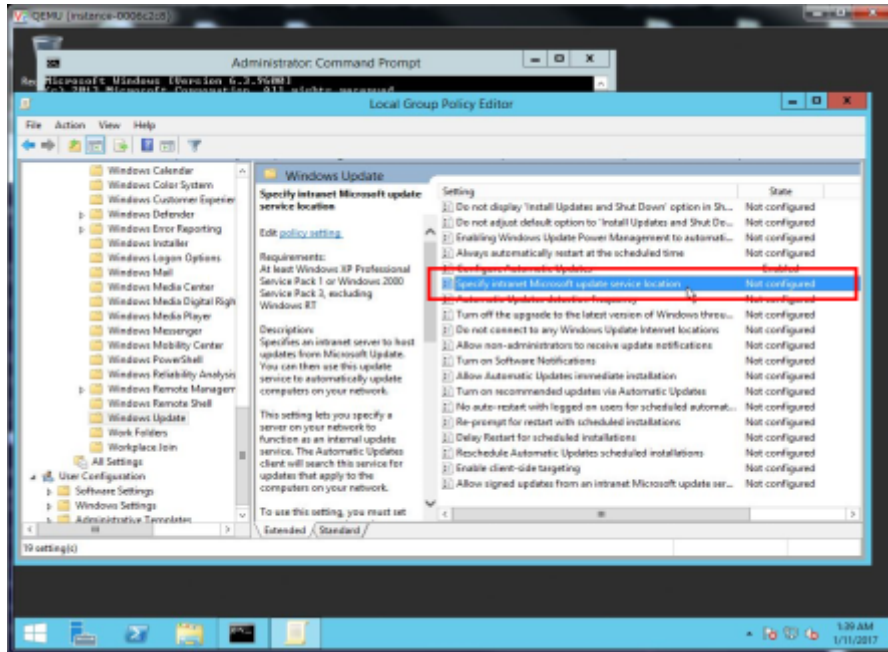
   d. In the screen to specify the intranet Microsoft update service location, select [Enabled], and then, under [Options], enter the information below for [Set the intranet update service for detecting updates] and [Set the intranet statistics server].

   `http`://<<FQDN of the WSUS service>>:`8530`

   After entering the above URL, click [OK].

   For the FQDN of the WSUS service, refer to Common Network Services.
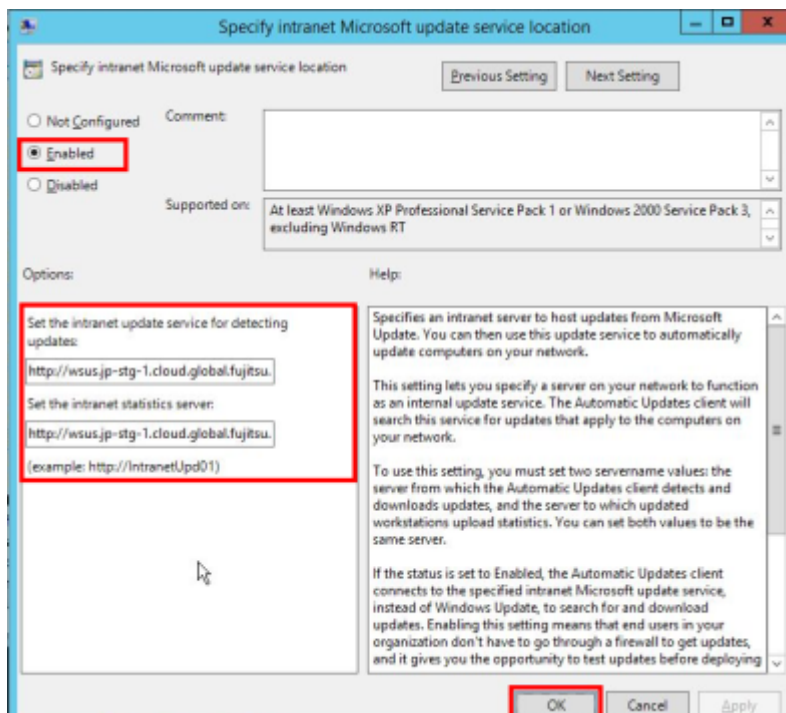
e. Double-click [No auto-restart with logged on users for scheduled automatic updates installations], select "Enabled", and then click the [OK] button.

5. Updating the group policy
   a. In the command prompt, run the following command:

   ```
   C:¥Windows¥system32>gpupdate /force
   ```
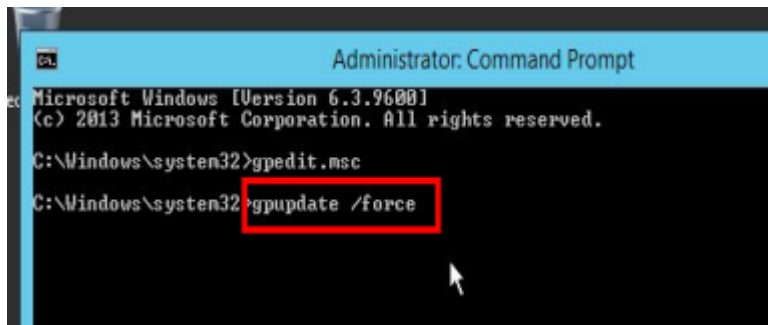

   b. Make sure that the message 'User Policy update has completed successfully' is displayed.

6. Checking the status of Windows Update
   a. Right-click the [Windows] button, and then click [Control Panel].
   b. In Control Panel, click [System and Security].
   c. In the System and Security screen, click [Windows Update].
   d. In the left-hand tree of the Windows Update screen, click [Check for updates].
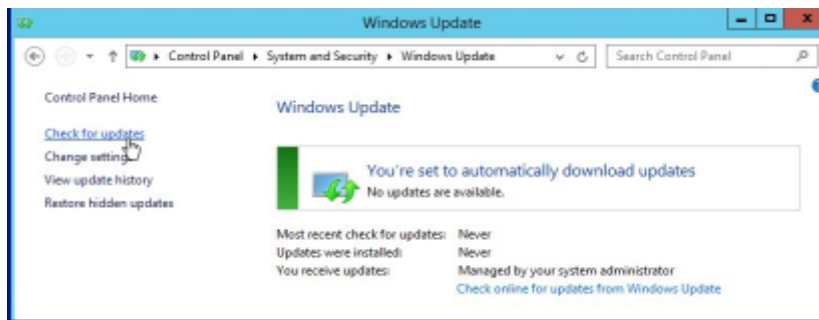
   e. Make sure that no program update notifications or updates are displayed.
      Also make sure that no errors are displayed.
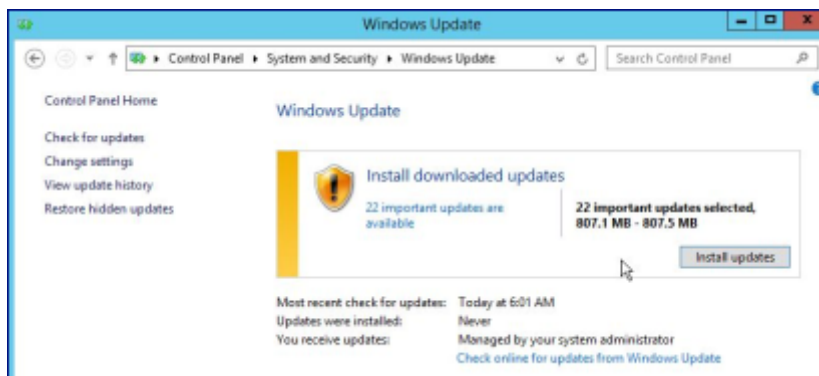
A.16 Supported Cipher Suites for SSL-VPN Connection

The supported cipher suites for SSL-VPN V2 Service are shown below.

Table 225: Supported Cipher Suites for SSL-VPN Connection

SSL Protocol (*1)	SSL Cipher Suite (*2)
TLS 1.1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SSL Protocol (*1)	SSL Cipher Suite (*2)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

Note (*1): TLS 1.2 is selected by an SSL protocol.

Note (*2): An SSL cipher suite is chosen with priority.

A.17 Registering Server Certificates Used by Load Balancers

This section explains the procedure for registering server certificates with the key management function when performing HTTPS communication or SSL communication using a load balancer. Creating a key metadata container registers server certificates.

The following preparations are necessary to register a server certificate for a load balancer. The file names below should be read as the names of the files that you created.

- Server certificate
- Server private key

Procedure

1. Register server certificates

   Register server certificates using the key management service. For details about the registration method, refer to "Create key metadata" in the "API Reference - Management Administration".

Table 226: Example Settings for Server Certificate Registration

Item	Example Settings
Key Metadata Name	lb_server_certificate
Retention Period	2025-12-31T23:59:59

Item	Example Settings
Confidential Information	-----BEGIN CERTIFICATE-----\n (character string where the line break codes in the payload of server.crt are replaced with '\n') \n -----END CERTIFICATE-----
Content Type for Confidential Information	text/plain

> **Tip**
>
> When including certificates other than server certificates, create a new file containing the information given below, and use it as a new server.crt file.
>
> - When including an intermediate CA certificate
>
> ```
> -----BEGIN CERTIFICATE-----
>   Server certificate confidential information
> -----END CERTIFICATE-----
> -----BEGIN CERTIFICATE-----
>   Intermediate CA certificate confidential information
> -----END CERTIFICATE-----
> ```
>
> - When including an intermediate CA certificate and a cross root certificate
>
> ```
> -----BEGIN CERTIFICATE-----
>   Server certificate confidential information
> -----END CERTIFICATE-----
> -----BEGIN CERTIFICATE-----
>   Intermediate CA certificate confidential information
> -----END CERTIFICATE-----
> -----BEGIN CERTIFICATE-----
>   Cross root certificate confidential information
> -----END CERTIFICATE-----
> ```

2. Register the server private key

   Using the key management service, register the server private key. For details about the registration method, refer to "Create key metadata" in the "API Reference - Management Administration".

Table 227: Example Settings for Server Private Key Registration

Item	Example Settings
Key Metadata Name	lb_server_private_key
Retention Period	2025-12-31T23:59:59
Confidential Information	-----BEGIN RSA PRIVATE KEY-----\n (character string where the line break codes in the payload of server.key are replaced with '\n') \n -----END RSA PRIVATE KEY-----
Content Type for Confidential Information	text/plain

3. Create a key metadata container

   Create a key metadata container to contain both the server certificate and the private key created in steps 1 and 2. For details about the creation method for the key metadata container, refer to "Create key metadata container" in the "API Reference - Management Administration".

Table 228: Example Settings for Key Metadata Containers

Item	Example Settings
Key Metadata Container Name	ELBCredential
Key Metadata Type	certificate 📲 **Note** Only specify "certificate" for the key metadata type.

Key Metadata List	"secret_refs": [
	{
	"name": "certificate",
	"secret_ref": "https://keymanagement.jp-west-2.cloud.global.fujitsu.com/v1/{Project ID}/secrets/{ID of server certificate key metadata}"
	},
	{
	"name": "private_key",
	"secret_ref": "https://keymanagement.jp-west-2.cloud.global.fujitsu.com/v1/{Project ID}/secrets/{ID of server private key metadata}"
	}
	]
	
	💡 **Tip** It is unnecessary to set "intermediates".

A.18 Character Strings Specifiable for Names

The types of characters and the lengths of character strings that can be used in each service are as shown below.

Virtual Servers

Table 229: Character Strings Related to Virtual Servers

Item	Usable Character Types	Length
Virtual Server Name	ASCII character range	255 bytes or less
Snapshot Name	ASCII character range	255 bytes or less
Key Pair Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-, _) ・Alphabetical characters are case sensitive ・You cannot use blank spaces	255 bytes or less

Storage

Table 230: Character Strings Related to Object Storage

Item	Length
Object Name	1024 bytes or less
Object Metadata Name	128 bytes or less
Object Metadata	2048 bytes or less
Container Name	256 bytes or less
Container Metadata Name	128 bytes or less
Container Metadata	2048 bytes or less

Network

Table 231: Character Stings Related to Networks

Item	Usable Character Types	Length
Network Name	ASCII character range	255 bytes or less
Subnet Name	ASCII character range	255 bytes or less
Security Group Name	ASCII character range	255 bytes or less
Security Group Description	ASCII character range	1024 bytes or less
Port Name	ASCII character range	255 bytes or less
Network Connector Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-, _) ・Alphabetical characters are case sensitive	255 bytes or less
Connector Endpoint Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-, _) ・Alphabetical characters are case sensitive	255 bytes or less
Virtual Router Name	ASCII character range	255 bytes or less
Name of VPN Service	ASCII character range	255 bytes or less
Name of SSL-VPN Connection	ASCII character range	255 bytes or less

Table 232: Character Strings Related to the Firewall Service

Item	Usable Character Types	Length
Firewall Name	ASCII character range	255 bytes or less
Firewall Description	ASCII character range	1024 bytes or less

Item	Usable Character Types	Length
Name of Firewall Rule	ASCII character range	255 bytes or less
Firewall Rule Description	ASCII character range	1024 bytes or less
Firewall Policy Name	ASCII character range	255 bytes or less
Firewall Policy Description	ASCII character range	1024 bytes or less

Table 233: Character Strings Related to the Load Balancer Service

Item	Usable Character Types	Length
Load Balancer Name	Alphabetical characters (uppercase and lowercase), numbers, and hyphens (-)	1 - 30 characters
Session Persistence Policy Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (!"#$%&'()*+,-./:;<=>?@[\]^_'{|}~) ・Alphabetical characters are case sensitive	255 bytes or less
Redirect Policy Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (!"#$%&'()*+,-./:;<=>?@[\]^_'{|}~) ・Alphabetical characters are case sensitive	255 bytes or less

Database

Table 234: Character Strings Related to the Database Service

Item	Usable Character Types	Length
Specification of the virtual database server name	Alphabetical characters (uppercase and lowercase), numbers, and hyphens (-) ・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	1 - 255 characters
Master User Name	Alphabetical characters (lowercase), numbers, and symbols (-, _) ・You can only use an alphabetic character (lowercase) or symbol (_) as the first character	1 - 63 characters
Master User Password	Alphabetical characters (uppercase and lowercase), numbers, and symbols other than single quotes (')	1 - 1024 characters

Item	Usable Character Types	Length
Database Snapshot Name	Alphabetical characters (uppercase and lowercase), numbers, and hyphens (-) • 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	1 - 255 characters
Read Replica Name	Alphabetical characters (uppercase and lowercase), numbers, and hyphens (-) • 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	1 - 255 characters

Template

Table 235: Character Strings Related to the Template Service

Item	Usable Character Types	Length
Stack Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-_.)	1 - 255 characters

Management Functions

Table 236: Character Strings Related to User Management

Item	Usable Character Types	Length
Project Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-_ +=,.@) • Alphabetical characters are not case sensitive	4 - 64 characters
Project Description	There are no restrictions	255 or less characters
Group Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-_ +=,.@) • Alphabetical characters are not case sensitive	4 - 64 characters
User Name	Alphabetical characters (uppercase and lowercase), numbers, and symbols (-_.@)	4 - 246 characters

Item	Usable Character Types	Length
User Password	Alphabetical characters (uppercase and lowercase), numbers, and symbols (!#$%&()*+-.=?@[]_{}~) ・Alphabetical characters are case sensitive ・Must not contain the user name ・Must include at least 1 alphabetic character ・Must include at least 1 numeric character	16 - 64 characters

Table 237: Character Strings Related to Key Management

Item	Usable Character Types	Length
Key Metadata Container Name	Alphabetical characters (uppercase and lowercase), numbers, and single-byte symbols	1 - 255 characters
Key Metadata Name	Alphabetical characters (uppercase and lowercase), numbers, and single-byte symbols	1 - 255 characters

A.19 Red Hat Update Infrastructure 3.0 Usage Procedure

A.19.1 Red Hat Update Infrastructure 3.0 Usage Procedure

This section explains the procedure for installing the client package that is required in order to use the Red Hat Update Infrastructure.

Check the following:

・OS

This procedure is for the Red Hat Enterprise Linux OS.

・Communication Permissions

Configure security groups and firewalls so the following outbound communications are permitted:

　・DNS communication

　　Port: 53/UDP

　・RHUI service

　　Port 443/TCP

・DNS Server Settings

On the server that the Red Hat Update Infrastructure will be used, set the IaaS DNS server in /etc/resolv.conf. For the DNS server of the IaaS, refer to DNS Server.

When using the repository of Red Hat Update Infrastructure 3.0, perform the following procedure.

Procedure

1. Confirm the version of the client package
   ```
   # yum list installed | grep client-rhel
   ```

   Example for RHEL7:

   When it is client-rhel7-3.0-1.noarch.rpm, the version is 3.0.

2. Delete the old client package

   When replacing the old client package with a new one, execute the following commands to delete the old client package.

   ```
   # yum remove <The_client_packet_confirmed_in_1.>
   # yum clean all
   ```

3. Obtain the client package

   Obtain the client package corresponding to your OS from "RHUI Configuration File" on the K5 portal.

   https://doc.cloud.global.fujitsu.com/en/iaas/index_en.html

   After obtaining the client package, store it in any desired location on the virtual server on which it will be installed.

4. Install the client package

   Execute the following command to install the client package.

   ```
   # yum localinstall -y <The_client_package_obtained_in_3.> --nogpgcheck
   ```

   > **Note**
   > - After installing the client package, all of the usable repositories will have been enabled.
   >   Edit the /etc/yum.repos.d/rh-cloud.repo file, and disable any unnecessary repositories.
   > - As repositories for which rhui-custom-protected_rhel~ is set are required when updating client packages, do not disable them.

5. Fix the update version (Only when using AUS)

   Execute the following command to fix the update version.

   ```
   # echo 7.x > /etc/yum/vars/releasever
   ```

   * Note: Specify the version to update to for "x".

6. Confirm operation

   Execute the following command to display the information of the repository.

   ```
   # yum repolist
   ```

   In the displayed results, check the following:
   - That a value other than 0 is displayed for repolist in the execution results
   - That the following error message is not displayed
     "Could not retrieve mirrorlist"

   If necessary, execute yum update or yum install.

A.19.2 Repositories Usable with Red Hat Update Infrastructure 3.0

Red Hat Enterprise Linux 6

Usable Repositories	Target of OS Support	Version of the Client Package	
		3.0	3.1
Red Hat Enterprise Linux 6 Server from RHUI (RPMs)	Yes	Yes	Yes
Red Hat Enterprise Linux 6 Server from RHUI (Debug RPMs)	No	Yes	Yes

Usable Repositories	Target of OS Support	Version of the Client Package	
		3.0	3.1
Red Hat Enterprise Linux 6 Server - Optional from RHUI (RPMs)	No	Yes	Yes
Red Hat Enterprise Linux 6 Server - RH Common from RHUI (RPMs)	No	Yes	Yes
Red Hat Enterprise Linux 6 Server - Extras from RHUI (RPMs)	No		Yes
Red Hat Enterprise Linux 6 Server - Supplementary from RHUI (RPMs)	No		Yes
Red Hat Software Collections for RHEL Server from RHUI (RPMs)	No		Yes

Red Hat Enterprise Linux 7

Usable Repositories	Target of OS Support	Version of the Client Package	
		3.0	3.1
Red Hat Enterprise Linux 7 Server from RHUI (RPMs)	Yes	Yes	Yes
Red Hat Enterprise Linux 7 Server from RHUI (Debug RPMs)	No	Yes	Yes
Red Hat Enterprise Linux 7 Server - RH Common from RHUI (RPMs)	No	Yes	Yes
Red Hat Enterprise Linux 7 Server - Extras from RHUI (RPMs)	No		Yes
Red Hat Enterprise Linux 7 Server - Optional from RHUI (RPMs)	No		Yes
Red Hat Enterprise Linux 7 Server - Supplementary from RHUI (RPMs)	No		Yes
Red Hat Software Collections RPMs for Red Hat Enterprise Linux 7 Server from RHUI	No		Yes
dotNET on RHEL RPMs for Red Hat Enterprise Linux 7 Server from RHUI	No		Yes

Red Hat Enterprise Linux 7 Advanced Mission Critical Update Support (AUS)

Usable Repositories	Target of OS Support	Version of the Client Package	
		3.0	3.1
Red Hat Enterprise Linux 7 Server - AUS (RPMs) from RHUI	Yes	Yes	Yes

Usable Repositories	Target of OS Support	Version of the Client Package	
		3.0	3.1
Red Hat Enterprise Linux 7 Server - AUS (Debug RPMs) from RHUI	No	Yes	Yes
Red Hat Enterprise Linux 7 Server - RH Common from RHUI (RPMs)	No	Yes	Yes
Red Hat Enterprise Linux 7 Server - Extras from RHUI (RPMs)	No		Yes
Red Hat Enterprise Linux 7 Server - AUS - Optional (RPMs) from RHUI	No		Yes
Red Hat Enterprise Linux 7 Server - Supplementary from RHUI (RPMs)	No		Yes
Red Hat Software Collections RPMs for Red Hat Enterprise Linux 7 Server from RHUI	No		Yes
dotNET on RHEL RPMs for Red Hat Enterprise Linux 7 Server from RHUI	No		Yes

A.20 Automatic Failover Notification Messages

A.20.1 Standard Services

When automatic failover occurs or is completed, a notification email is sent to the overall administrator of the project the target resource belongs to. This section explains the details of these notification messages.

Target Regions

Notification messages are available in the regions below.

*Notification messages should become available in other regions during 2018.

・Eastern Japan Region 1
・Western Japan Region 1
・Western Japan Region 2

Timing of Notification

Notification is given at the following timings:

・When automatic failover occurs
・When automatic failover completes

Target Resources

The following resources are the targets of notification messages:

・Virtual servers
・Virtual routers
・Network connectors

Notification Messages and Message Items

The following notification messages are sent.

```
[FUJITSU Cloud Service K5] Auto-Failover has started

Dear Sir/Madam,

Thank you for using the FUJITSU Cloud Service K5.

Due to a host error, the virtual server migration has been started.
[details]
Domain ID:0a12345bc6d78e9012f34a56bc7890de
Domain Name:domainname1
Region:jp-east1
Availability Zone:AZ1
Tenant ID:01a2b34c5de678901fab2345678c9012
Tenant Name:tenamtname1
router_id:jp0a01-pgy001-00
router_name:routername1
recovery  completion  time:2018/04/01 12:34:56

Please do not reply to this message as this address is not monitored.
==================================================
    FUJITSU LIMITED
    FUJITSU Cloud Service K5
==================================================
```

Figure 59: Notification Message (Example)

The content of the sections enclosed in the dashed lines changes depending on the timing of notification and the target resource.

The items described in email are as follows.

Table 238: Message Items of Automatic Failover Notification Messages

Category	Item Name		Description
	When Automatic Failover Occurs	When Automatic Failover Completes	
Title	[FUJITSU Cloud Service K5] Auto-Failover has started	[FUJITSU Cloud Service K5] Auto-Failover has completed	Title of the notification message
Common items	Domain ID		Domain ID
	Domain Name		Domain name
	Region		Region
	Availability Zone		Availability zone
	Tenant ID		Project ID
	Tenant Name		Project name
When the target resource is a virtual server	Server ID		Virtual server ID
	Server Name		Virtual server name
When the target resource is a virtual router	Virtual Router ID		Virtual router ID
	Virtual Router Name		Virtual router name
When the target resource is a network connector	Network Connector ID		Network connector ID
	Network Connector Name		Network connector name

Category	Item Name		Description
	When Automatic Failover Occurs	When Automatic Failover Completes	
Time	Failure Detection Time	Recovery Completion Time	Time when automatic failover occurred or competed

A.20.2 Services for SAP

When automatic failover is completed, a notification email is sent to the overall administrator of the project the target resource belongs to. This section explains the details of these notification messages.

Target Regions

Notification messages are available in the regions below.

- Eastern Japan Region 1
- Western Japan Region 2

Timing of Notification

Notification is given at the following timings:

- When automatic failover completes

Target Resources

The following resources are the targets of notification messages:

- Virtual servers

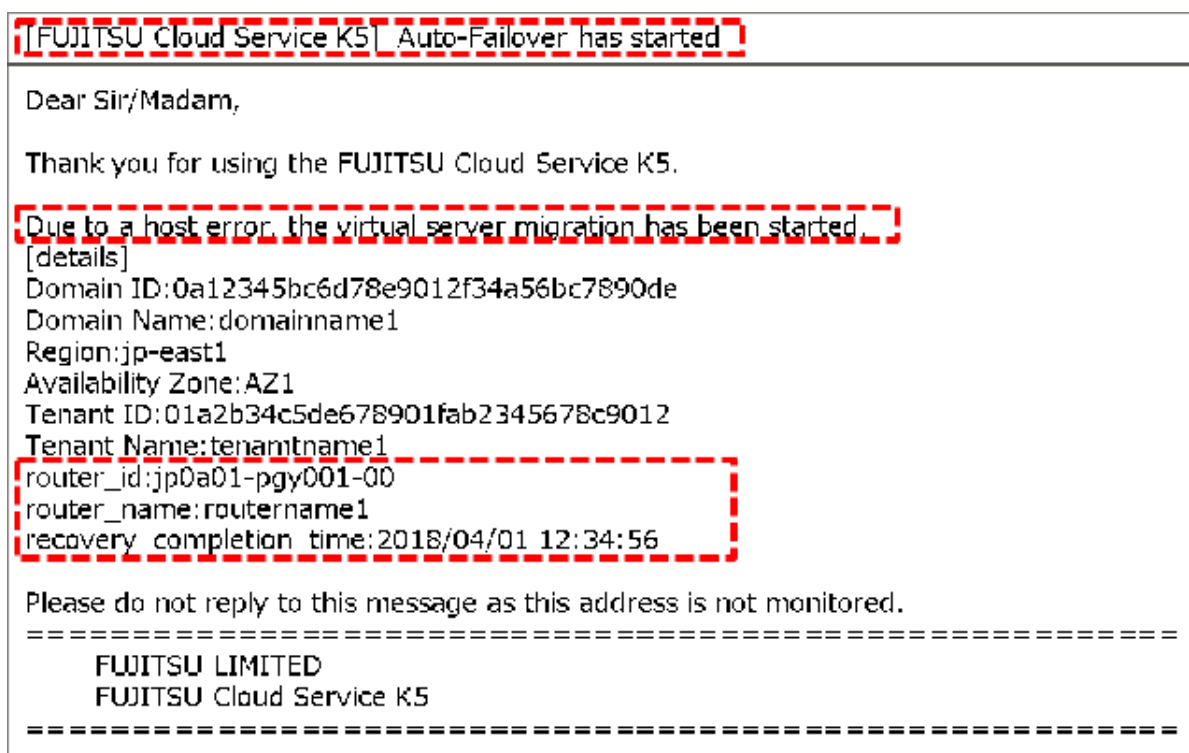### Notification Messages and Message Items

The following notification messages are sent.

Figure 60: Notification Message (Example)

The content of the sections enclosed in the dashed lines changes depending on the type of the target resource.
The items described in email are as follows.

Table 239: Message Items of Automatic Failover Notification Messages

Category	Item Name	Description
Title	[FUJITSU Cloud Service K5] [compute-w] Failover completed on your virtual server	Title of the notification message
Body	Region ID	Region ID
	Availability Zone	Availability zone
	Domain Name	Domain name (domain ID)
	Project Name	Project name (project ID)
	Virtual Server Name	Virtual server name

A.21 How to Use Reverse DNS Lookup

This section explains how to use reverse DNS lookup with IaaS. Registering a PTR record with the DNS of IaaS makes it possible to perform FQDN name resolution (reverse DNS lookup) from IP addresses.

Target IP Addresses

IP addresses that fulfill the following two conditions can be registered in PTR records:

・ IP addresses for which A or AAAA (DNS lookup) records have been registered in IaaS.

- Floating IP addresses that have been assigned from any of the following regions:
  - Eastern Japan Region 1
  - Western Japan Region 1
  - Western Japan Region 2

Operations Regarding Reverse DNS Lookup Records

The following operations can be performed for PTR records
- Registration of PTR records
- Deletion of PTR records
- Update of PTR records

For detailed specifications and advisory notes regarding PTR records, refer to "Create/delete record" in the "API Reference - Network".

> 💡 **Tip**
> It is not possible to register multiple PTR records for a single IP address. When you want to change the value of a PTR record, delete the existing PTR record and then the A or AAAA record. After that, register the modified A or AAAA record, and then register the modified PTR record.

Example: When updating the value of a PTR record from FQDN1 to FQDN2
1. Delete the PTR record of FQDN1
2. Delete the A or AAAA record corresponding to the PTR record of FQDN1
3. Register the A or AAAA record with the record name FQDN2
4. Register the PTR record of FQDN2

When You Want to Register a Floating IP of another Region or another Project

It is possible to register the PTR record of a floating IP of another region or another project. In such cases, specify the information of the assignment source of the floating IP in the following parameter of the API.
- x-fcx-region: Specify the name of the region from which the floating IP was assigned
- x-fcx-region-token: Specify the regional token of the project from which the floating IP was assigned

> 💡 **Tip**
> In X-AUTH-TOKEN, regardless of the assignment source of the floating IP, specify the regional token of the project to which the PTR record is being registered.
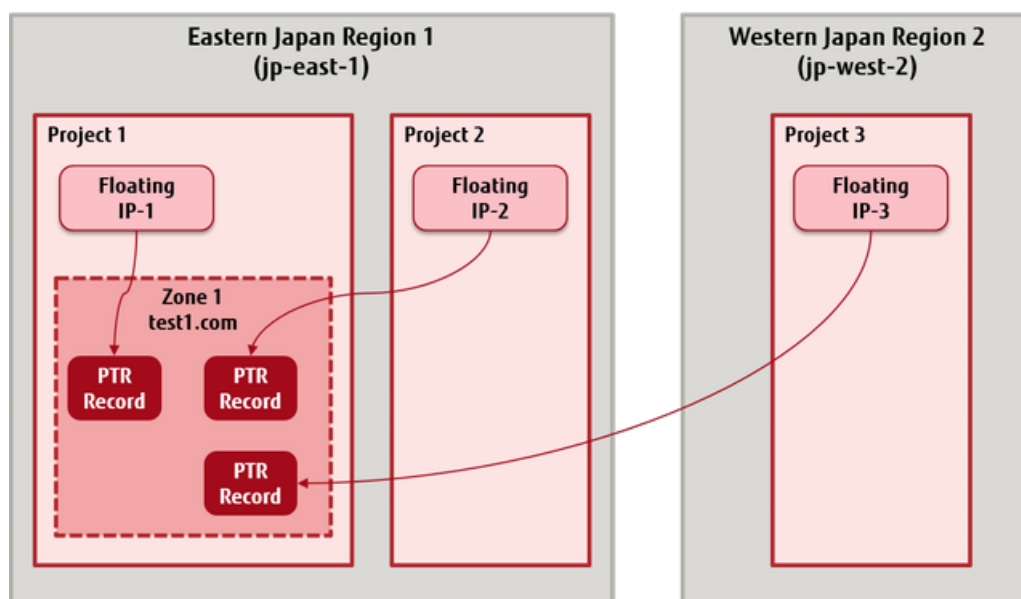
Figure 61: When Registering PTR Records of Project 2 and Project 3 in Zone 1

In the figure above, the specifications for x-fcx-region and x-fcx-region-token are as follows.

Record to Register	x-fcx-region	x-fcx-region-token	X-AUTH-TOKEN
PTR record of floating IP-1	jp-east-1	Regional token of project 1	Regional token of project 1
PTR record of floating IP-2	jp-east-1	Regional token of project 2	
PTR record of floating IP-3	jp-west-2	Regional token of project 3	
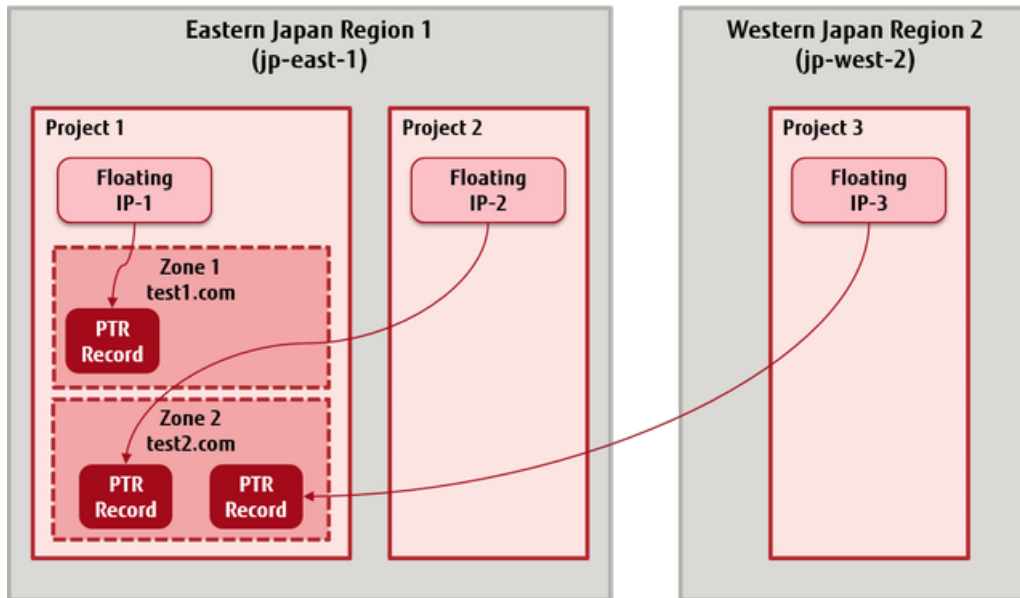
Figure 62: When Registering PTR Records of Project 2 and Project 3 in Zone 2

In the figure above, the specifications for x-fcx-region and x-fcx-region-token are as follows.

Record to Register	x-fcx-region	x-fcx-region-token	X-AUTH-TOKEN
PTR record of floating IP-1	jp-east-1	Regional token of project 1	Regional token of project 1
PTR record of floating IP-2	jp-east-1	Regional token of project 2	
PTR record of floating IP-3	jp-west-2	Regional token of project 3	
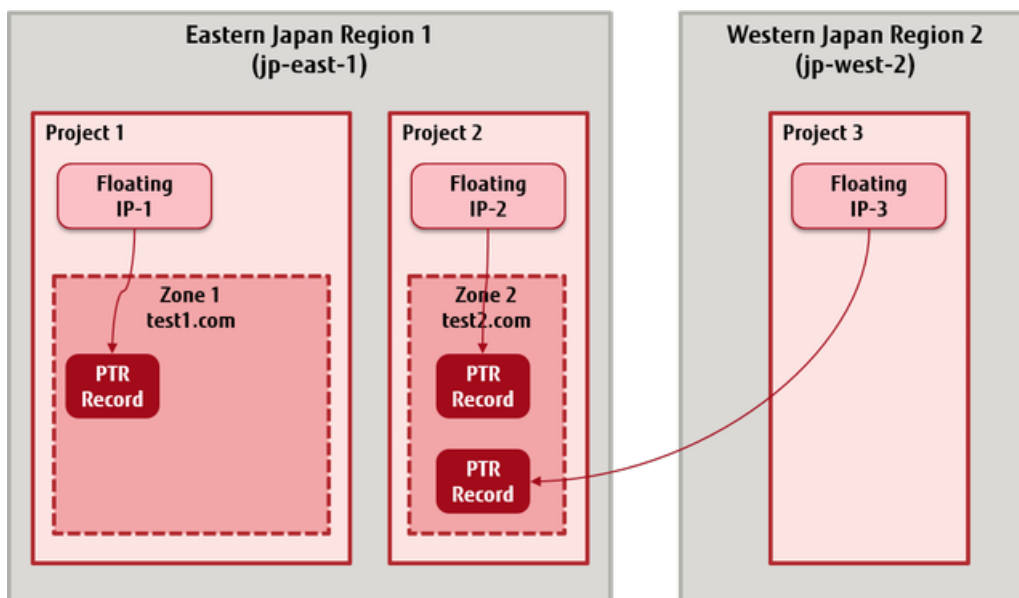
Figure 63: When Registering PTR Records of Project 2 and Project 3 in Zone 2 of Project 2

In the figure above, the specifications for x-fcx-region and x-fcx-region-token are as follows.

Record to Register	x-fcx-region	x-fcx-region-token	X-AUTH-TOKEN
PTR record of floating IP-1	jp-east-1	Regional token of project 1	Regional token of project 1
PTR record of floating IP-2	jp-east-1	Regional token of project 2	Regional token of project 2
PTR record of floating IP-3	jp-west-2	Regional token of project 3	

> **Note** The following operations are not possible when registering zones:
> • Registering multiple zones with the same name
> • Registration of zones in regions other that Eastern Japan Region 1
>
>
>
> Figure 64: Registering Zones
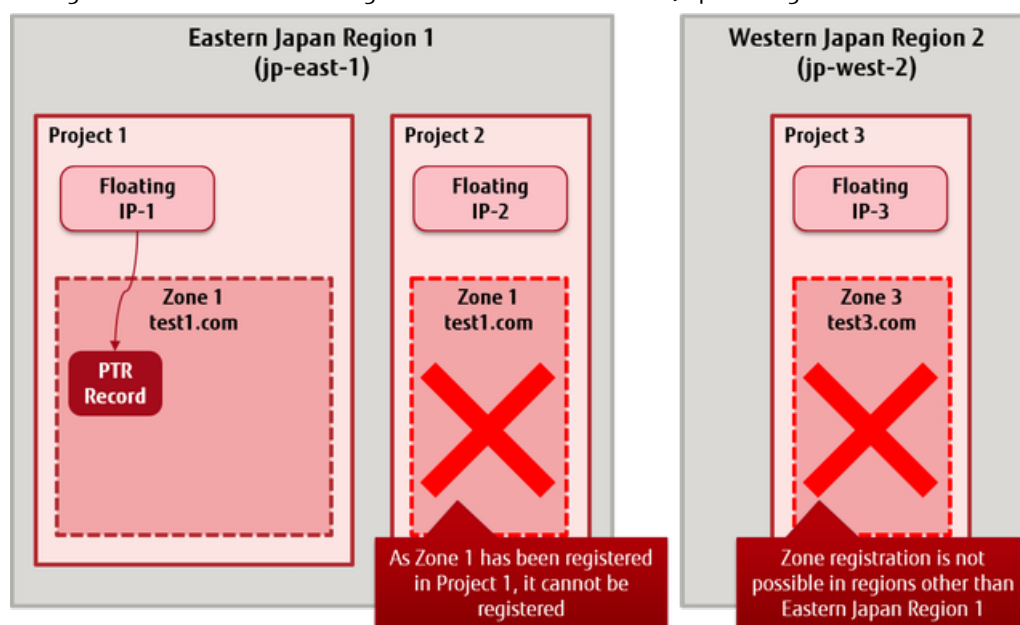
Revision History Prior to Edition 3.0

Edition	Date of Update	Location	Overview
1.2	Jan. 18, 2016	Procedure to Run Sysprep on Windows OS	Description added
		Logging In to a Virtual Server IPsec VPN Function	Points to note added
1.3	Feb. 29, 2016	Sharing Virtual Server Images NAS Software Image SSL-VPN Connection Creating a Virtual Database Server	Function added
		Preset Roles and Privileges Software Support Service	Description modified
1.4	Apr. 1, 2016	Compute overall	Functional category changed
		Dedicated Virtual Server Software Provision Service Virtual Server for SAP Dedicated Virtual Server for SAP	Function added
		New User Registration User Management	Function transferred due to establishment of K5 Portal
1.5	Apr. 7, 2016	Region Region Management User Management	Function added due to addition of new region
		Port Management Limiting Values	Description modified
1.6	May 19, 2016	Application Deployment Message Queue	Description of unprovided functions deleted
		Checking Console Log Dedicated Virtual Server Dedicated Virtual Server for SAP Port Management Firewall Service Setup of an OpenVPN Client (Windows) Limiting Values	Description modified
		Available Commands and SQL Statements	Article added

Edition	Date of Update	Location	Overview
1.7	Aug. 4, 2016	OS Provision Service OS Patch/Update Settings Japanese Language Settings for RHEL 7.x / CentOS 7.x / RHOCP 3.x Software Support Service System Storage List of Software Support Service IDs	OS image added
1.8	Aug. 19, 2016	Content Delivery Service Limiting Values	Function added
1.9	Sep. 16, 2016	Software Provision Service Microsoft SQL Server Usage Guide	Software image added
1.10	Nov. 10, 2016	Creating/Deleting a Virtual Server Dedicated Virtual Server What is Virtual Server Export? Load Distribution Condition Settings Predefined Security Policies Creating a Virtual Database Server	Function added
		NAS Software Image Limiting Values	Description modified
1.11	Nov. 28, 2016	Protocols and Cipher Suites Supported by API Endpoint	Function added
2.0	Jan. 10, 2017	Region OS Provision Service Software Provision Service Software Support Service Virtual Server for SAP Common Network Services	New region added
2.1	Jan. 23, 2017	Virtual Server Remote Console Function	Function added
		Provisioning Script Function Logging In to a Virtual Server OS Provision Service OS Patch/Update Settings Software Support Service System Storage List of Software Support Service IDs Common Network Services Procedure for Connecting to SUSE Public Cloud Infrastructure (Patch Distribution Server)	Software image added

Edition	Date of Update	Location	Overview
2.2	Feb. 13, 2017	Creating/Deleting a Virtual Server Dedicated Virtual Server Creating a Virtual Database Server	Function added
2.3	Feb. 28, 2017	Region OS Provision Service Software Provision Service Software Support Service Virtual Server for SAP Common Network Services	New region added
		OS Provision Service OS Patch/Update Settings Software Support Service System Storage List of Software Support Service IDs Common Network Services	OS image added
		NAS Software Image How to Use NAS Software Image	Description on NAS software image updated
		Common Network Services Procedure for Connecting to the WSUS (Windows Server Update Services) Server	Procedure for connecting to WSUS Server added
		Operations on a Virtual Server Virtual Server Remote Console Function Port Management Authentication Settings for Sender Policy Framework Private Connection Function Limiting Values	Description modified
2.4	Mar. 16, 2017	OS Provision Service What is Virtual Server Import? List of Software Support Service IDs	Supported OS (Cent OS 7.2) added
		Auto-Scaling Settings Limiting Values	Description modified

Edition	Date of Update	Location	Overview
2.5	Apr. 3, 2017	What is Virtual Server Import? What is Virtual Server Export?	Modified explanatory article of VM Import and Export (Added agentless support of VM Import and support of RHEL OS)
		System Storage Additional Storage Snapshot Function	Storage added
		Creating/Deleting a Virtual Server Security Group Functions Global IP Address Service Limiting Values	Description modified
2.6	Apr. 12, 2017	Region OS Provision Service Software Provision Service Software Support Service Virtual Server for SAP Common Network Services	Spain region added
		OS Provision Service OS Patch/Update Settings Software Support Service System Storage List of Software Support Service IDs Common Network Services	Windows OS image (Japanese) added
2.7	June 1, 2017	Content Delivery Service Delivery Settings Function Access Control	Function added
		SSL-VPN Connection Record Management Functions Report Functions Limiting Values	Description modified
2.7.1	June 9, 2017	--	Corrected descriptions
2.8	June 16, 2017	Creating/Deleting a Virtual Server	Virtual server types added
		OS Provision Service	

Edition	Date of Update	Location	Overview
		Software Provision Service	
		NAS Software Image	
		Creating a Virtual Database Server	
		Security Group Functions	Description modified
		Database Operations	
2.9	June 30, 2017	OS Provision Service	Supported OS (Cent OS 7.3) added
		Load Distribution Condition Settings Predefined Security Policies	Function added (Load balancer cipher suite)
		SSL-VPN Connection Connection/Disconnection from an OpenVPN Client (Windows) Connection/Disconnection from an OpenVPN Client (CentOS) Supported Cipher Suites for SSL-VPN Connection	Description modified
		What is Virtual Server Import? What is Virtual Server Export?	Supported OS added
2.10	Jul. 18, 2017	Region OS Provision Service Software Provision Service Software Support Service Virtual Server for SAP Common Network Services	New region added
		OS Provision Service Common Network Services	Supported OS (SUSE) added
2.10.1	Aug. 1, 2017	Creating/Deleting a Virtual Server for SAP Dedicated Virtual Server for SAP	Virtual server types added
		OS Provision Service Software Provision Service	Specifications of OS images changed
		SSL-VPN Connection Connecting to a Virtual Server OS through an SSL-VPN Connection	Description modified
		Points to Note	Description modified
		What is Virtual Server Import?	Corrected descriptions

Edition	Date of Update	Location	Overview
2.11	Aug. 18, 2017	Region Virtual Server for SAP Common Network Services	New region added
		Load Distribution Condition Settings Predefined Security Policies	Description modified
		Common Network Services	Information of RHUI added
		Setup of an OpenVPN Client (Windows) Setup of an OpenVPN Client (CentOS)	Description modified
2.12	Sep. 1, 2017	Load Balancer Service	Description modified
		First Login to the Virtual Server	Description modified
		Limiting Values	Description modified
2.13	Sep. 28, 2017	OS Provision Service System Storage List of Software Support Service IDs	OS image added
		Project Management	Function added
		Scaling Up and Scaling Down of a Virtual Server	Description modified
		Creating/Deleting a Container Container Management Access Policy Settings (ACL) Registering/Deleting an Object	Description modified
		Database User	Description modified
		Operations on a Virtual Server	Description added
		Creating a Virtual Database Server	Description added
		Limiting Values	Corrected descriptions
2.14	Oct. 19, 2017	SSL-VPN Connection	Description added
		Service Overview	Description modified
		Virtual Router Function	Description modified
		Creating a Virtual Database Server	Description modified

Edition	Date of Update	Location	Overview
		Setup of an OpenVPN Client (Windows) Setup of an OpenVPN Client (CentOS)	Description modified
2.15	Oct. 27, 2017	Preface Logging In to a Virtual Server OS Provision Service Software Support Service Procedure to Run Sysprep on Windows OS System Storage List of Software Support Service IDs	OS image added
2.16	Nov. 2, 2017	List of Software Support Service IDs	Support Level of SUSE changed
		List of Software Support Service IDs	Support Level of RHEL added
		Preface	Description modified
2.17	November 21, 2017	Load Distribution Condition Settings Registering Server Certificates Used by Load Balancers	Added the procedure for registering server certificates for load balancers
		System Storage Template	Description of Template Builder deleted
		Delivery Settings Function Limiting Values	Function added
		SSL-VPN Connection Connecting to a Virtual Server OS through an SSL-VPN Connection	Description modified
		Load Distribution Condition Settings Connecting to a Virtual Server OS through an SSL-VPN Connection	Added advisory notes regarding use of private keys
		Setup of an OpenVPN Client (Windows) Connection/Disconnection from an OpenVPN Client (Windows) Setup of an OpenVPN Client (CentOS) Connection/Disconnection from an OpenVPN Client (CentOS)	Added settings for authentication of HTTP proxy servers
		Common Network Services	Corrected descriptions

Edition	Date of Update	Location	Overview
2.18	December 4, 2017	Software Provision Service Software Support Service List of Software Support Service IDs Microsoft SQL Server Usage Guide	SQL Server image added
		Connecting to a Virtual Server OS through an SSL-VPN Connection	Description modified
		Email Delivery Service Sending Settings Monitoring the Status of Delivery	Description modified
		Snapshot Function	Description modified
		Common Network Services	Description added
2.19	December 15, 2017	Database as a Service Creating a Virtual Database Server DB Parameter Groups Available Commands and SQL Statements	Database engines added
		Load Distribution Condition Settings Predefined Security Policies	Description modified
2.20	December 22, 2017	Load Distribution Condition Settings Predefined Security Policies	Description modified
		Region OS Provision Service Software Provision Service Software Support Service	Description modified
		Limiting Values	Description modified
		Connecting to a Virtual Server OS through an SSL-VPN Connection	Description added
		Database Operations Database User Database Recovery	Modified descriptions due to unification of terms

Edition	Date of Update	Location	Overview
		Preface OS Provision Service Procedure to Run Sysprep on Windows OS What is Virtual Server Import? Migrating an Image of Windows Server OS What is Virtual Server Export? Transferring Image Files System Storage Procedure for Connecting to the WSUS (Windows Server Update Services) Server	Added abbreviations
2.21	January 26, 2018	What is Virtual Server Import? Migrating an Image of Windows Server OS Virtual Server Image Import Function What is Virtual Server Export? Transferring Image Files	Supported OS added
		Record Management Functions Limiting Values	Added SRV to the supported records
		SSL-VPN Connection Relationships with the Firewall Service and Security Group Function	Description modified
		SSL-VPN Connection Connecting to a Virtual Server OS through an SSL-VPN Connection	Description added
		Auto-Scaling Settings	Description added
		Adding/Deleting a Target for Load Distribution	Description modified
		Common Network Services	Port permission settings added
		How to Use NAS Software Image	Description modified
		Database Recovery	Description added
2.22	February 22, 2018	IPsec VPN Function SSL-VPN Connection Limiting Values	Description modified
		Database Recovery	Description added
		Limiting Values	Description modified

Edition	Date of Update	Location	Overview
		Character Strings Specifiable for Names	Description added
		Managing Virtual Server Images	Description modified
		IPsec VPN Function	Corrected descriptions
		Common Network Services	Corrected descriptions
2.23	March 22, 2018	OS Provision Service Software Support Service List of Software Support Service IDs	Added metered charging for Windows
		Multi-Availability Zone Distribution	Description added
		Red Hat Update Infrastructure 3.0 Usage Procedure	Description added
		Managing Virtual Server Images	Description added
		SSL-VPN Connection	Description added
		Record Management Functions Limiting Values	Description modified
		Adding/Deleting a Target for Load Distribution	Description added
		Limiting Values	Description modified
		Connecting to a Virtual Server OS through an SSL-VPN Connection	Description modified
		Key Management Function	Description modified
2.24	April 9, 2018	Preface Provisioning Script Function Logging In to a Virtual Server Virtual Server Remote Console Function OS Provision Service OS Patch/Update Settings Japanese Language Settings for RHEL 7.x / CentOS 7.x / RHOCP 3.x System Storage List of Software Support Service IDs Common Network Services	OS image added

Edition	Date of Update	Location	Overview
		Creating/Deleting a Virtual Server Virtual Server for SAP Standard Services	Function added
		Content Delivery Service Delivery URL Secure Delivery Delivery Settings Function Example Usage Scenarios and Caching Behavior Control Rules Limiting Values	Function added
		Subnet Management	Description added
		SSL-VPN Connection	Description modified
2.25	April 19, 2018	Preface List of Software Support Service IDs	OS image added
		Software Provision Service Software Support Service List of Software Support Service IDs	SQL Server image added
		Virtual Server for SAP Services for SAP	Function added
		Setup of an OpenVPN Client (Windows) Setup of an OpenVPN Client (CentOS)	Description added
		Server Group Function	Description modified
		Virtual Router Function	Description modified
		Limiting Values Character Strings Specifiable for Names	Description modified
		Database Operations	Corrected an error
2.26	June 1, 2018	Record Management Functions How to Use Reverse DNS Lookup	Description added
		Common Network Services	Description modified
		Creating/Deleting a Virtual Server	Description added
		Provisioning Script Function	Description added

Edition	Date of Update	Location	Overview
		Key Pair Management Function	Description added
		OS Provision Service	Description added
		Auto-Scaling Settings	Description added
		Additional Storage	Description added
		Network Management	Description added
		Subnet Management SSL-VPN Connection	Description added
		Load Balancer Service	Description added
		Building a Stack	Description added
		Preset Roles and Privileges	Description added
		Project Management	Description added
		Character Strings Specifiable for Names	Description added
		Record Management Functions Failover Function Weighted Round Robin Function	Description modified
		Limiting Values	Description modified

FUJITSU Cloud Service for OSS IaaS

Features Handbook

Version 3.8