FUJITSU Software
Cloud Storage Gateway V1.2.0

User's Guide

J2UL-2275-03ENZ0(02)
March 2020

Preface

Purpose of This Manual

This manual gives an overview of FUJITSU Software Cloud Storage Gateway (hereinafter referred to as "this product") and describes how to install and operate this product.

Intended Readers

This manual is intended for users who are considering the installation of this product or system administrators who install or manage this product.
In addition, this manual assumes that the reader has knowledge of the following:

- Server virtualization system (VMware vSphere, KVM or Hyper-V)
- Public cloud services (Amazon Web Services or Microsoft Azure/FUJITSU Cloud Service for Microsoft Azure)
- Network Attached Storage (NAS)
- Cloud storage

Structure of This Manual

The structure of this manual is as follows:

Chapter 1 Product Description

Describes an overview of this product.

Chapter 2 Installation

Describes how to install this product.

Chapter 3 Configuring Operating Environments

Describes how to configure the required operating environment for this product.

Chapter 4 Operation

Describes operations using this product.

Chapter 5 Changing Operating Environments

Describes how to change the operating environment for this product.

Chapter 6 Maintenance

Describes the maintenance procedure for this product.

Chapter 7 Deleting Operating Environments

Describes how to remove the operating environment for this product.

Appendix A Specifications List

Describes the specifications of this product.

Appendix B Status Information

Describes the status information of this product.

Appendix C Upgrading from an Old Product

Describes how to upgrade from an old product.

Appendix D Snapshots

Describes how to use snapshots.

Appendix E Incompatibility Information

Describes information about incompatibility with an old product.

Conventions

The abbreviations and style shown below are used in this manual.

- Abbreviations

Type	Formal Name	Abbreviation
Operating systems	VMware vSphere(R) 6.0 VMware vSphere(R) 6.5 VMware vSphere(R) 6.7 VMware vSphere(R) 7.0	VMware vSphere
	Red Hat(R) Enterprise Linux(R) 7.3 (for Intel 64) Red Hat(R) Enterprise Linux(R) 7.4 (for Intel 64) Red Hat(R) Enterprise Linux(R) 7.5 (for Intel 64) Red Hat(R) Enterprise Linux(R) 7.6 (for Intel 64) Red Hat(R) Enterprise Linux(R) 7.7 (for Intel 64) Red Hat(R) Enterprise Linux(R) 8.1 (for Intel 64)	RHEL
Software products	Windows(R) Internet Explorer(R)	Internet Explorer
	Microsoft(R) Edge	Microsoft Edge
	Google Chrome(TM)	Chrome

- Style
  - Screen and keyboard keys

Item	Description	Example
Screen name	Screen names are described in bold.	**Datastore** screen
Panel name	Panel names are described in bold.	**Logs** panel
Tab name	Tab names are described in bold.	**Mail server** tab
Field name	Field names are described in bold.	**Mail address** field
Button name	Button names are described in bold.	**OK**
Radio button name	Radio button names are described in bold.	**Shared folder** radio button
Key name of keyboard	Keyboard keys are enclosed in square brackets ([ ]).	[Enter] key

  - Manual related names

Item	Description	Example
Manual name	Enclosed in double quotes (").	Refer to "Messages" in the "Reference Guide".
Chapter/section title within the manual		

Export Controls

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademarks

- Linux is a registered trademark or trademark of Linus Torvalds in the United States and other countries.
- Red Hat and RPM are registered trademarks of Red Hat, Inc. in the U.S. and other countries.

- VMware, VMware logo, Virtual SMP, and vMotion are the registered trademarks or trademarks of VMware, Inc. in the United States and other countries.
- Microsoft, Windows, Windows Server, and other Microsoft products are registered trademarks of Microsoft Corporation in the United States and other countries.
- Active Directory, Hyper-V, Azure, Internet Explorer, and Microsoft Edge are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Amazon Elastic Cloud Compute (Amazon EC2) is a registered trademark or trademark of Amazon Web Services, Inc. in the United States and other countries.
- All other brand and product names are registered trademarks or trademarks of their respective owners.

Shipment Date and Revision History

Shipment Date	Revision	Document Part Number	
		PDF	HTML
April 2018	1	J2UL-2275-01ENZ0(00)	J2UL-2275-01ENZ2(00)
October 2018	2	J2UL-2275-02ENZ0(00)	J2UL-2275-02ENZ2(00)
January 2019	2.1	J2UL-2275-02ENZ0(01)	J2UL-2275-02ENZ2(01)
June 2019	3	J2UL-2275-03ENZ0(00)	J2UL-2275-03ENZ2(00)
October 2019	3.1	J2UL-2275-03ENZ0(01)	J2UL-2275-03ENZ2(01)
March 2020	3.2	J2UL-2275-03ENZ0(02)	J2UL-2275-03ENZ2(02)

Notice

- No part of this manual may be reproduced without permission.
- This manual is subject to change without advance notice.

Copyright

Revision History

Content of Update	Location of changes	Revision
Added support for following. - VMware vSphere(R) 7.0 - Red Hat(R) Enterprise Linux(R) 7.6 (for Intel 64) - Red Hat(R) Enterprise Linux(R) 7.7 (for Intel 64) - Red Hat(R) Enterprise Linux(R) 8.1 (for Intel 64) - Windows Server 2019	Preface, Chapter 2, Appendix A	3.2
Added notes related to "User Logon Name".	Chapter 2, Chapter 3	
Added notes related to "CSG Web GUI".	Chapter 2	
Added examples of "Communication Settings of CSG Web GUI".	Chapter 2	
Deleted unnecessary FTP descriptions.	Preface, Chapter 2, Chapter 6	3.1
Added support for Amazon Elastic Cloud Compute (Amazon EC2) and Microsoft Azure/FUJITSU Cloud Service for Microsoft Azure.	Preface, Chapter 2	3

Content of Update	Location of changes	Revision
Reduced the required amount of resources (memory size and virtual disk size for the cache area) for the virtual machine in which this product is running.	Chapter 2	
Added support for the regions that require Signature Version 4 of Amazon S3 cloud provider.	Chapter 2	

Documentation Road Map

Manual Organization

The manual organization of this product is as follows.

Manual Title	Description	Purpose/Use					
		Concept	Assessment	POC and Installation	Training	Tuning and Migration	As Required
User's Guide	Purpose To understand the product overview, installation procedure, and operation procedure of this product. Contents - Product overview - Install and setup procedure - Operation procedure Prerequisite manual None.	✓	✓	✓	✓	✓	
Reference Guide	Purpose To understand the detailed information about the available REST API specifications, the meanings and actions for the output messages, and the terms and their descriptions for the manuals of this product. Contents - Description of the REST API format and function - Message meaning and action plan - Terms and their description Prerequisite manual None.						✓

✓ indicates which manual to read for which purpose/use.

Contents

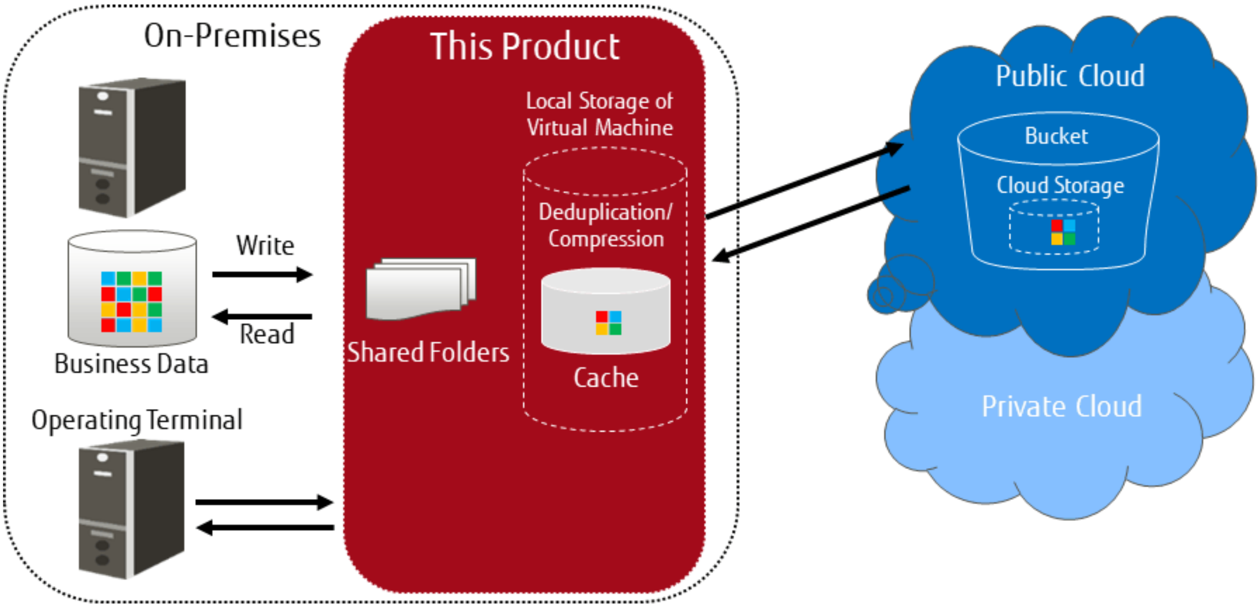
Chapter 1 Product Description

1.1 Product Overview

This product allows access to a cloud storage using the NFS/SMB protocols.

It provides a "shared folder" that can be accessed with the NFS/SMB protocols, performs a deduplication and compression on the data that is written to this shard folder, and stores the data in a local storage (cache). After that, the data is transferred to a cloud storage in the background.

Figure 1.1 Overview of System with This Product Installed



This product provides the following advantages:

- Reduce operation and maintenance costs related to the use of tapes by changing the backup location for data from tapes to a cloud storage
- Reduce the total cost compared to storing backup data on a tape and transporting the tape to a remote location, by storing data in a cloud storage for simple disaster recovery

Main Features

Continued Use of Current Backup Software

You can continue using your current backup software to back up data to a cloud storage, simply by changing the data storage destination to the shared folders that are provided by this product. There is no need to purchase additional software options or make changes to any settings in order to back up data to the cloud storage. You can back up to the cloud storage without making major changes to your current backup operations.

Even in companies in which departments use different backup software, each department can continue to use their current backup software. The backup software does not need to be changed or integrated even if the destination of the backup operation is changed to the cloud storage.

Reduced Data Transmission and Storage Costs through the Utilization of Optimal Deduplication Methods Associated with the Cloud Storage

Deduplication with a variable length division method is utilized in order to remove a larger amount of duplicate data.

Supports dynamic capacity expansion/small start with additional capacity licenses

Provides additional capacity licenses to control initial costs and to add capacity as needed.

1.2 System Configuration

The system configuration diagrams of this product are shown below.

Figure 1.2 Single network system configuration diagram

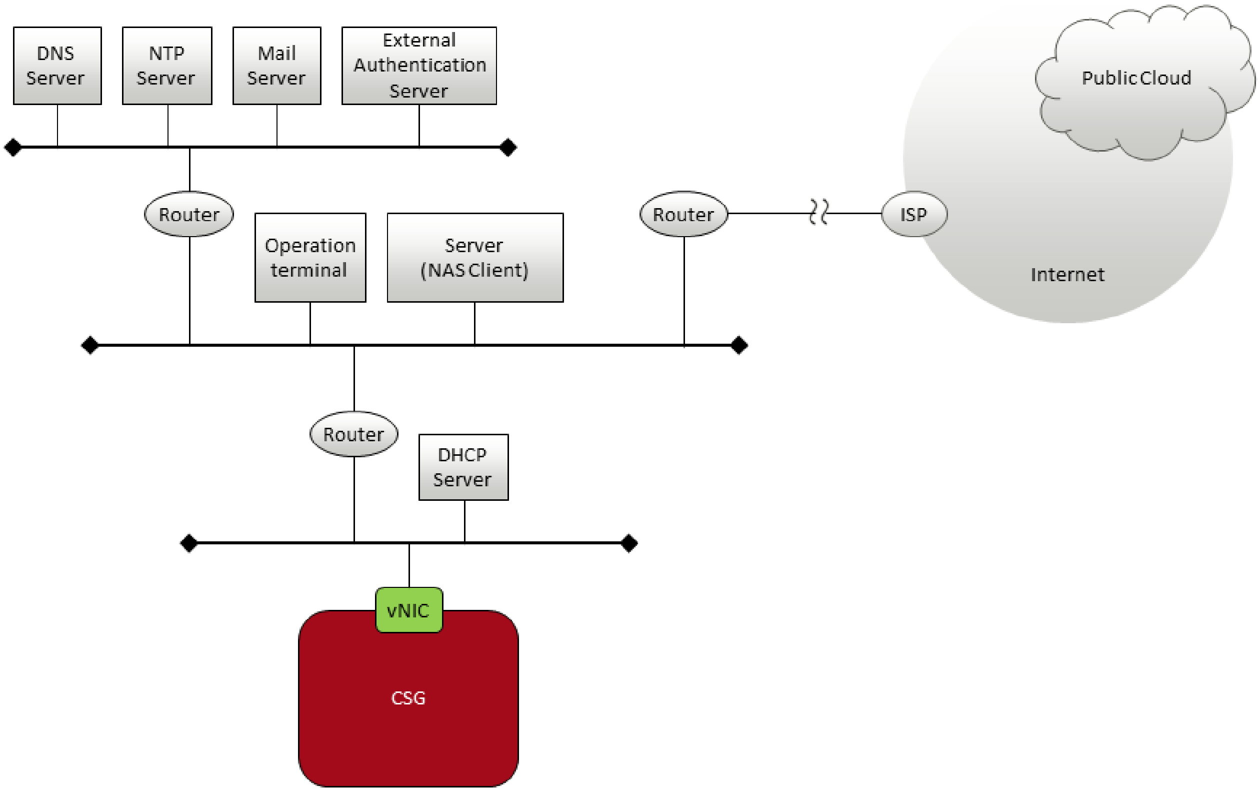
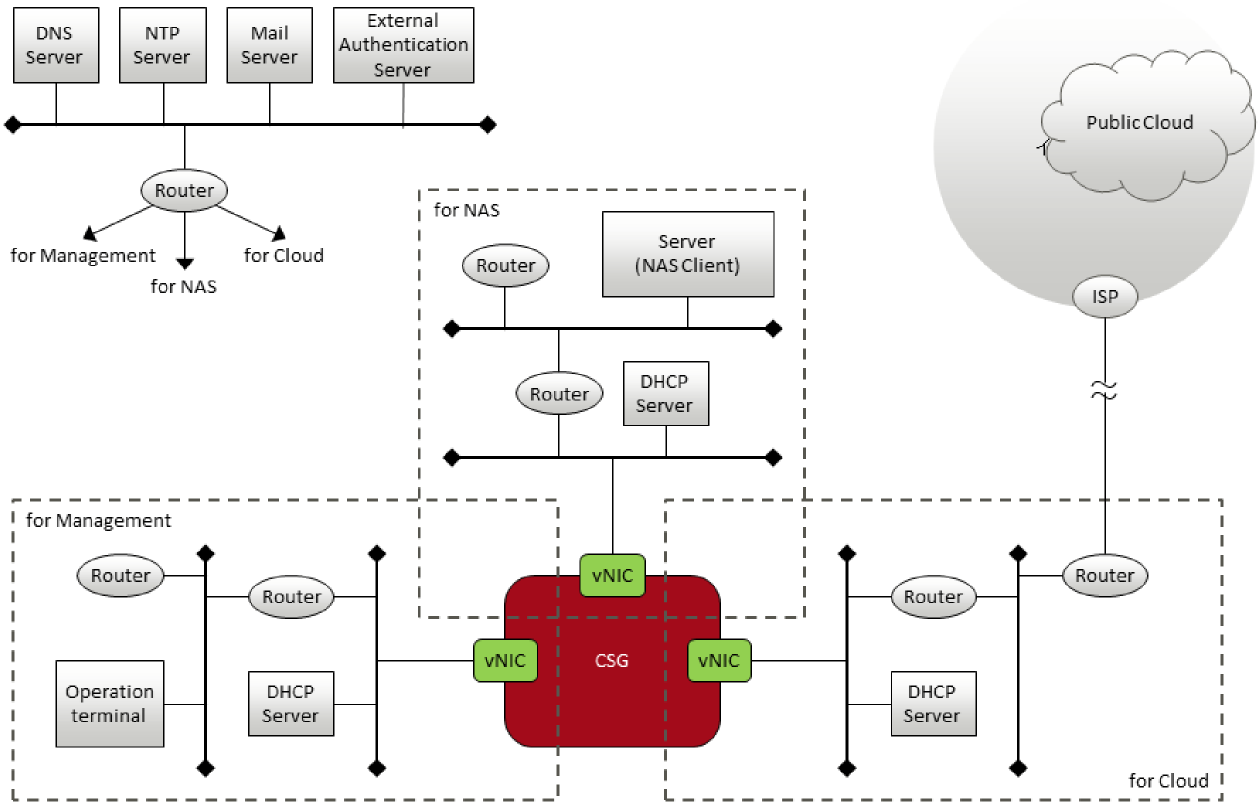


Figure 1.3 Multi-network System configuration diagram



The components that are required to use this product to store data in a cloud storage are shown below.

Figure 1.4 Component Layout

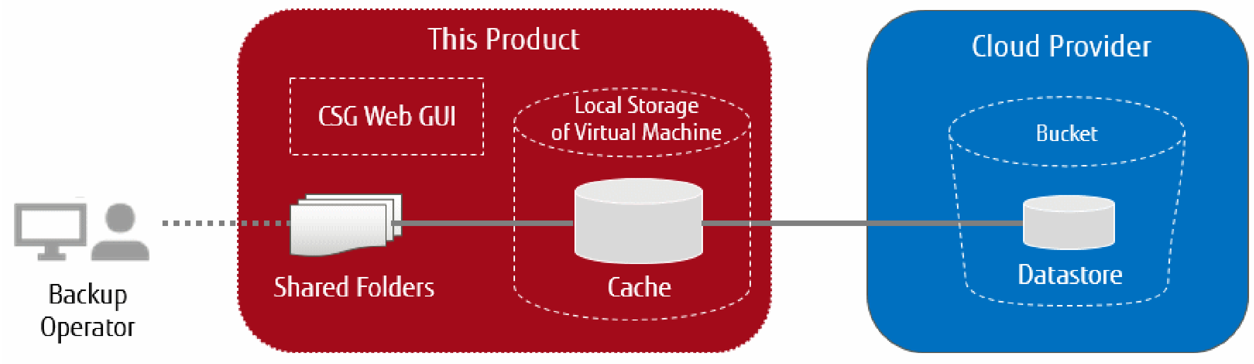


Table 1.1 List of Required Components

Component Name	Description
CSG Web GUI	GUI for setting and monitoring this product. Refer to "1.4.2 User Interface" for details.
Shared folders	NAS interfaces that are the gateways for cloud storage.
Cache	An area where data that has been written to a shared folder is stored temporarily before the data is transferred to a cloud storage. Cache is located on the local disk of the virtual machine. In addition to actual data, meta data (management data regarding deduplication and compression, and management data such as for cloud storage information of the data storage destination) is also stored. Actual data is written to cache after it is deduplicated and compressed. If there is room in the cache area, data that has been transferred to the cloud storage is kept in the cache in order to improve the response speed when data is read from shared folders.
Cloud provider	Refers to the cloud storage (such as FUJITSU Cloud Service for OSS, Object Storage and Amazon S3) that is provided by cloud providers, and online storage environments for private clouds using OpenStack.
Bucket	Logical storage area that is created in a cloud storage.
Datastore	A cloud storage area where the data that is written to the shared folder is eventually stored. A datastore is created in a bucket in the cloud storage. In the same way as cache, actual data that has been deduplicated and compressed and meta data are stored in a datastore.

1.3 Operating Environment

Refer to "A.1 Virtual Appliance Specifications", "A.2 Functional Specifications", and "A.3 Support List" for details about the operating environment for this product.

1.4 Provided Functions

This section describes the functions that are provided by this product.

1.4.1 Data Transfer

NAS Interface

In general, you must use the private API provided by the cloud provider to access the cloud provider. This product provides a familiar NAS interface (NFS/SMB). Users do not need to be aware of the API for accessing a cloud provider. This product performs conversions and transfers automatically, and therefore you can store data in a cloud provider without making major changes to the existing backup operations.

With standard backup software, by just changing the output destination of the backup data to the shared folder provided by this product, the backup operations to the cloud provider can be implemented.

Deduplication and Compression

This product performs deduplication and compresses data, stores the data in cache, and then transfers the deduplicated/compressed data to the cloud provider. Therefore, it provides the following advantages:

- Reduce the amount of data stored in cache
- Reduce the time to transfer data to the cloud provider
- Reduce the cost for storing data in the cloud provider

Deduplication and compression are performed on this product's virtual machine, and therefore there is no load on the backup server. Note that although deduplication is performed without any conditions, you can select whether to enable or disable compression in the **Settings** screen.

Cache

This product uses the local disk for the virtual machine as "cache". The effects of using cache are as follows:

- When transferring data to the cloud provider

  "Writing Completed" is returned to the backup software when data is written to cache, allowing a high-speed response to the backup software.

- When restoring data

  Data is restored from cache instead of restoring from the cloud provider, allowing the restoration time to be reduced.

Both actual data and meta data are stored in cache. This product handles actual data and meta data as described below, according to the cache usage rate.

Table 1.2 Operation of Cache

Cache Usage Rate	Handling of Actual Data	Handling of Meta Data
Less than 80 %	Stored in cache.	Stored in cache.
80 % or more	Stored in cache. After that, the data is deleted starting from the data with the oldest access date until the usage rate of the cache becomes less than 80%.	Stored in cache. Not subject to deletion.

The user can define the size of the cache when this product is installed.

Encryption

This product can encrypt data before storing it in a datastore. Doing so improves security for the data. Refer to "3.2 Registering a Datastore and Cache" for details about how to set data encryption.

Traffic control

This product can adjust the amount of data transferred based on the upper limit set for the transfer rate. This can reduce the amount of network bandwidth used.

Note

This function monitors the amount of data transferred to and from the Cloud and adjusts data transfer amount by temporarily stopping the transfer when the upper limit has been exceeded. Therefore, the upper limit may be exceeded temporarily. In particular, depending on the amount of data sent from the Cloud, the data amount may greatly exceed the upper limit.

Multi-network configuration

This product supports network configurations that connect to up to three subnets from a traffic partitioning and security point of view for management, NAS, and cloud networks.

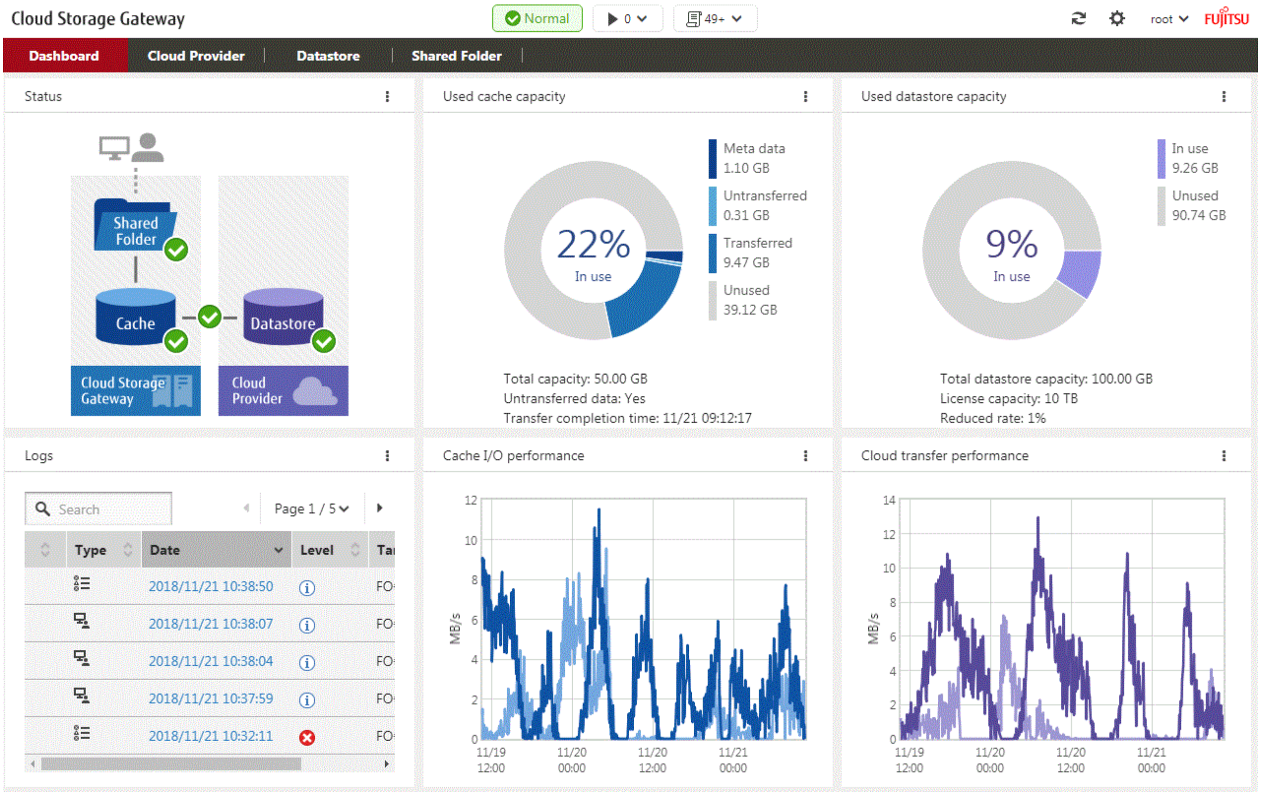
1.4.2 User Interface

This product provides both a GUI and a REST API as user interfaces.

CSG Web GUI

This product provides a Web interface (called "CSG Web GUI" in the manuals for this product).

Figure 1.5 CSG Web GUI Dashboard



You can use CSG Web GUI to view the status of each component, logs, cache usage, cache I/O performance, datastore usage, and cloud transfer performance. You can also create/change/delete cloud providers, datastores, and shared folders.
Refer to "4.3 Status Checking" for details about how to use CSG Web GUI to check status, "4.4 Capacity Checking" for details about how to use CSG Web GUI to check capacity, and "4.5 Performance Checking" for details about how to use CSG Web GUI to check performance.

CSG REST API

This product provides a REST API (called "CSG REST API" in the manuals for this product).
Refer to the "Reference Guide" for details about "CSG REST API".
CSG Web GUI and CSG REST API are supported as follows:

Table 1.3 CSG Web GUI and CSG REST API support

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
2.5.5 Starting CSG Web GUI Initial user creation	Initial User Creation
2.5.6 Registering a License	License
2.5.8 Monitoring Settings	Mail Server
	Mail Notification
2.6.1 Settings When Using CSG Web GUI and CSG REST API with the Local Authentication User	Local Authentication User
2.7 Setting NAS Access Users	NAS Access Group

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
	NAS Access User
2.7.2 Settings When Accessing the NAS with the External Authentication User	NAS Authentication Server
3.1 Registering a Cloud Provider	Cloud Provider
3.2 Registering a Datastore and Cache	Datastore
3.3 Registering a Shared Folder	Shared Folder
4.5 Performance Checking	Performance
5.1 Changing Shared Folder Settings	Shared Folder
5.2 Changing Datastore Settings	Datastore
5.3 Changing Cloud Provider Settings	Cloud Provider
6.1 Checking Logs	Operation Log
	Event Log
6.2 Checking Performance Data	Performance
6.3 Troubleshooting	Troubleshooting Data Download
6.4 Restoring the Environment	Meta Data Recovery
	Shared Folder List (on Recovery)
7.1 Deleting Defined Information	Shared Folder
	Datastore
	Cloud Provider

1.4.3 Logs

This product displays the following logs on the CSG Web GUI dashboard:

- Operation logs
- Event logs

Refer to "6.1 Checking Logs" for details about how to check logs.

1.4.4 E-mail Notification

This product can send notification by e-mail when a "Warning" or "Error" event log is output.
An e-mail server and destination e-mail addresses must be set in order to send e-mail notifications. Refer to "2.5.8 Monitoring Settings" for details about how to configure these settings.

1.5 Licenses

This product provides a trial license and a regular license.
These licenses determine the amount of data (after deduplication and compression) that can be stored in the cloud provider.
In addition, licenses can be dynamically extended to increase based on the quantity of data required.
Refer to "2.5.6 Registering a License" for details about how to configure settings for licenses.

Chapter 2 Installation

This chapter describes how to install this product.

The CSG REST APIs that corresponds to the operation described in this chapter are as follows:

Table 2.1 Support for Chapter 2 CSG Web GUI and CSG REST API

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
2.5.5 Starting CSG Web GUI Initial user creation	Initial User Creation
2.5.6 Registering a License	License
2.5.8 Monitoring Settings	Mail Server
	Mail Notification
2.6.1 Settings When Using CSG Web GUI and CSG REST API with the Local Authentication User	Local Authentication User
2.7 Setting NAS Access Users	NAS Access Group
	NAS Access User
2.7.2 Settings When Accessing the NAS with the External Authentication User	NAS Authentication Server

2.1 Before Installation

This section describes the areas and items that must be designed before this product is installed.

2.1.1 Datastore Capacity

This product offers capacity licenses according to the amount of data to be stored in the cloud provider.

For the datastore capacity, a range up to the maximum capacity defined by the metered license can be specified.

The usage-based licenses for this product include basic licenses and additional capacity licenses, as follows:

Table 2.2 License types

	Basic licenses			Additional capacity licenses	
Capacity	10TB	30TB	60TB	+ 1TB	+ 10TB

You can extend the capacity of the datastore by applying an additional capacity license to the basic license. However, the maximum data capacity is 60TB. Additional capacity licenses that exceed 60TB cannot be applied.

Note

This product needs 10GB of datastore capacity for system use, therefore the actual capacity available is 10GB less than the datastore capacity.

2.1.2 Cache Capacity

For the cache capacity, you can set a value from "10% of the datastore capacity (20 GB minimum)" to the "size of a virtual disk connected to the virtual machine in which this product is running - 1 MB."
It is recommended that you set the cache capacity to 50 % of the datastore capacity. If a short restore time is required, set the value with the same capacity as the datastore capacity.

Point

The cache area is secured in a virtual disk that is connected to the virtual machine in which this product is running.
Therefore, you must prepare a virtual disk that is greater than or equal to the "cache capacity to be set + 1MB".

You can also assign multiple virtual disks to the cache area.

2.1.3 Network Configuration

With this product, the network is configured to communicate with various communication targets.

Single network configuration

Communicates with all communication targets on a single network.
If the communication target is on a different subnet, a default gateway setting is required.

Multi-network configuration

Communicates with various communication targets from multiple networks.
Set the route settings (gateway settings) of each network to communicate with communication targets on different subnets. However, only one network can be configured as the default gateway.

If the following types of servers are in different subnets, only the network where the default gateway is set can be used to communicate with these servers.

- DNS Server, NTP Server, mail server (SMTP Server), external authentication server (Active directory server)

Multi-network configurations can be used to communicate with operation terminals, business servers, backup servers, and cloud providers on any network.

Point

Each network is automatically assigned a network ID and differentiated.
A network ID is an auto-generated integer value that cannot be change.

Note

Regardless of the network configuration, if an abnormality occurs in communication with the DNS server, data cannot be transferred to the Cloud due to a name resolution failure of the cloud provider URI.

2.1.4 Information for Accessing the Cloud Provider

Check the information of this product in advance to connect to the cloud provider.
Refer to "3.1.2 Information Required for Registering a Cloud Provider" and "3.2.2 Information Required for Registering a Datastore/Cache" for details.

FUJITSU Cloud Service for OSS Object Storage

- URI (Cloud provider access point)
- Account
- Password
- Domain ID
- Project ID
- Container name (Referred to as "Bucket name" in this manual)

- Network name or network ID (in a system with multiple networks)

Amazon S3

- URI (Cloud provider access point)
- Access key ID
- Secret access key
- Bucket name
- Network name or network ID (in a system with multiple networks)

Microsoft Azure Blob Storage / FUJITSU Cloud Service for Microsoft Azure Blob Storage

- URI (Cloud provider access point)
- Account
- Access key
- Container name (Referred to as "Bucket name" in this manual)
- Network name or network ID (in a system with multiple networks)

NIFCLOUD Object Storage / FUJITSU Cloud Service for VMware NC Object Storage

- URI (Cloud provider access point)
- Access key ID
- Secret access key
- Bucket name
- Network name or network ID (in a system with multiple networks)

OpenStack Swift

- URI (Cloud provider access point)
- Account
- Password
- Domain ID
- Project ID
- Container name (Referred to as "Bucket name" in this manual)
- Network name or network ID (in a system with multiple networks)

2.2 Deploying Virtual Appliances

This product is provided as a virtual appliance. Deploy the virtual appliance in the server virtualization software to install this product.

Note

The way a public cloud service is operated may change. For the latest information on how to operate each public cloud service, refer to the documentation of each service.

2.2.1 Deploying to VMware vSphere Environment

Use the OVA file included in the DVD to deploy the virtual appliance.

There are three deployment methods in a VMware vSphere environment. The methods that can be used differ depending on the version of VMware vSphere.

Table 2.3 How to deploy by version

VMware vSphere version	vSphere Client	vSphere Host Client	vSphere Web Client
6.0	OK	OK	OK
6.5, 6.7, 7.0	NG	OK	OK

Using the vSphere Client

1. Start the vSphere Client, and click **Deploy OVF Template...** in the **File** menu.
2. In the **Source** screen, select the OVA file that is on the DVD and then click **Next**.
3. In the **Storage** screen, specify a save location on the virtual machine and then click **Next**.
4. In the **Disk Format** screen, select **Thin Provision** and then click **Next**.
5. If the **Network Mapping** screen is displayed, select the network that is being used by this product and click **Next**.
6. Click **Finish** to complete the deployment of the OVF template.
7. View the progress for the deployment in **Recent Tasks** while waiting for deployment to be completed.
8. Refer to "A.1 Virtual Appliance Specifications" and change the number of virtual CPUs and the memory size as necessary.
9. Add a virtual disk for the cache area that you estimated in "2.1.2 Cache Capacity". By considering the I/O performance, set the disk provision to **Thick Provision Eager Zeroed**.
   Because the format is **Thick Provision Eager Zeroed**, it will take some time to create the virtual disk depending on the capacity.
10. For multi-network configurations, add a virtual network adapter (Ethernet adapter). Select **VMXNET 3** as the adapter type.
11. Start the virtual appliance.

When using the vSphere Host client

1. Start the vSphere Host Client, then right-click **Host** in the inventory and select **Create/Register VM**.
2. On the **Select creation type** screen, select **Deploy a virtual machine from an OVF or OVA file** and then click **Next**.
3. On the **Select OVF and VMDK files** screen, after entering the name of the virtual machine and selecting the OVA file included in the DVD media, click **Next**.
4. In the **Select storage** screen, specify a location to save the virtual machine and then click **Next**.
5. On the **Deployment options** screen, select a network and disk format to be used by the product and then click **Next**. Specify **thin** as the disk format.
6. On the **Ready to complete** screen, click **Finish** to complete the deployment of the OVF template.
7. Check the progress of the deployment for this product in **Recent Tasks** and wait for the completion of the deployment.
8. Refer to "A.1 Virtual Appliance Specifications to change the number of virtual CPUs and memory size if necessary.
9. After stopping the virtual appliance, add a virtual disk that is estimated in "2.1.2 Cache Capacity" of the *User's Guide* for the cache area. By taking the I/O performance into consideration, specify **Thick provisioning (Eager Zeroed)** for disk provisioning.
   Because the format is **Thick provisioning (Eager Zeroed),** creation of the virtual disk may take time depending on capacity.
10. For multi-network configurations, add a virtual network adapter (Ethernet adapter). Select **VMXNET 3** as the adapter type.
11. Start the virtual appliance.

Note

- If you use the vSphere Host client, version 1.8.0 or later must be used.
  Older versions do not support 1GB or larger OVA files.

- When deployed with the vSphere Host client, the virtual machine automatically starts after deployment, so you must stop the virtual machine in Step 9.

When using the vSphere Web client

1. Start the vSphere Web client and select **Deploy OVF template** from **Actions**.
2. On the **Select template** screen, select the OVA file that is included in the DVD and then click **Next**.
3. On the **Select name and location** screen, select the name and location of the virtual machine for deployment and then click **Next**.
4. On the **Select a resources** screen, select the execution location of the virtual appliance and then click **Next**.
5. On the **Review details** screen, click **Next**.
6. On the **Select network** screen, select the network to be used by this product and then click **Next**.
7. On the **Select storage** screen, select the virtual disk format and the virtual machine location and then click **Next**. Specify "thin provisioning" for the virtual disk format.
8. On the **Ready to complete** screen, click **Complete** to complete the deployment of the OVF template.
9. Check the progress of the deployment of this product in **Recent Tasks** and wait for the deployment to be completed.
10. Refer to "A.1 Virtual Appliance Specifications to change the number of virtual CPUs and memory size if necessary.
11. Add a virtual disk for the cache area that is estimated in "2.1.2 Cache Capacity". By taking the I/O performance into consideration, specify **Thick provisioning (Eager Zeroed)** for disk provisioning.
    Because the format is **Thick provisioning (Eager Zeroed),** creation of the virtual disk may take time depending on capacity.
12. For multi-network configurations, add a virtual network adapter (Ethernet adapter). Select **VMXNET 3** as the adapter type.
13. Start the virtual appliance.

Point

You can also use the above procedure to deploy this product in a VMware vSphere High Availability (vSphere HA) environment.

In a vSphere HA environment, if a failure occurs on the VM host in which this product is running, a failover occurs automatically and this product is rebooted on a different VM host in the vSphere HA cluster. As a result of this reboot, NAS access from the business server or the backup server might fail. Further, it takes approximately 10 minutes before the product can be run, and NAS access is not possible during this time.
To determine if backup operation can continue when such NAS access errors occur, refer to the manual for the backup software that you are using.

2.2.2 Deploying to KVM Environment

Use the tar.gz file on the DVD to deploy the virtual appliance. The procedure is described below.

1. Transfer the tar.gz file to a directory of your choice on the KVM host, and then extract it there.

```
# tar xzvf CSG_v120_kvm.tar.gz
CSG_v120_kvm/
CSG_v120_kvm/CSG_v120_kvm.qcow2
CSG_v120_kvm/CSG_v120_kvm.xml
```

2. Copy the files from the extracted directory to their respective locations.

```
# cp CSG_v120_kvm.qcow2 /var/lib/libvirt/images
# cp CSG_v120_kvm.xml /etc/libvirt/qemu
```

   When changing the name of a virtual machine, edit the copy destination xml file with a text editor. Change the <name> tag below to a name that differs from other virtual machines. After the deployment, the Virtual Machine Manager will display the tag as the virtual machine name.

Lines to change:

```
<name>CSG_v120_kvm</name>
```

For multiple instances of this product on a single KVM host, copy the file using a new name. The examples below show file copies with their names changed to CSG_v120_kvm2.qcow2 and CSG_v120_kvm2.xml respectively.

```
# cp CSG_v120_kvm.qcow2 /var/lib/libvirt/images/CSG_v120_kvm2.qcow2
# cp CSG_v120_kvm.xml /etc/libvirt/qemu/CSG_v120_kvm2.xml
```

Next, change the following two lines of the copy destination xml file with a text editor. Change the <name> tag to a name that differs from other virtual machines. Specify the path to the copied qcow2 file for the file property of the <source> tag.

Lines to change:

```
<name>CSG_v120_kvm</name>
<source file='/var/lib/libvirt/images/CSG_v120_kvm.qcow2'/>
```

Example:

```
<name>CSG_v120_kvm2</name>
<source file='/var/lib/libvirt/images/CSG_v120_kvm2.qcow2'/>
```

3. Specify the xml file, and register the VA image for this product.

   ```
   # virsh define /etc/libvirt/qemu/CSG_v120_kvm.xml
   ```

   If the file name is changed in Step 2, specify that name.

   ```
   # virsh define /etc/libvirt/qemu/CSG_v120_kvm2.xml
   ```

4. Click **Virtual Machine Manager** to open the Virtual Machine Manager.
5. On the Virtual Machine Manager, select the VA image for this product and then click **Open**.
6. In the virtual machine screen, select **Detail** in the **View** menu.
7. In the virtual machine details screen, select **NIC**, select the virtual network or host device to connect to, and then click **Apply**.
8. For multi-network configurations, click **Add hardware** and then select **Network** in the **Add new virtual hardware** dialog box. Select the virtual network or host device to connect with this product, specify **virtio** as the device model, and then click **Finish**.
9. Refer to "A.1 Virtual Appliance Specifications" and change the number of virtual CPUs and the memory size as necessary.
10. Add a virtual disk for the cache area that you estimated in "2.1.2 Cache Capacity". In the virtual machine details screen, click **Add Hardware** and then click **Storage** in the **Add New Virtual Hardware** dialog box.
11. Select **Select or create custom storage** to add a storage volume. In the **Add a Storage Volume** dialog, set **Format** to **raw** and then change **Max Capacity** to the value that you estimated for the cache area.
12. Return to **Add New Virtual Hardware** dialog box and set **Bus type** to **VirtIO**.
13. Click **Finish**.

2.2.3 Deploying to Hyper-V environment

Deploy the virtual appliances using the zip file (CSG_v120_Hyper-V.zip) of the virtual machine image for Hyper-V included on the DVD. The procedure is as follows.

1. Transfer the zip file of the virtual machine image to the Hyper-V environment and extract it to a folder of your choice.
2. Start Hyper-V Manager.
   Start from **Server Manager** > **Tools** > **Hyper-V Manager**.
3. Click **Import Virtual Machine...** to start the Virtual machine import wizard.

4. Search for the folder.
   Specify the folder where the virtual machine images are extracted in Step 1.
   Specify the folder that contains the following three folders.

```
Snapshots
Virtual Hard Disks
Virtual Machines
```

5. Select the virtual machine.
   Select the displayed virtual machine.

6. Select the import type.
   Select **Copy the virtual machine (create a new unique ID).**

7. Select the folder that stores the virtual machine files.
   Select a folder of your choice.

8. Select a folder to store the virtual hard disk.
   Select a folder of your choice.
   You cannot select a folder that contains a file with the name CSG_v110_hyperv-disk1.vhdx.

9. Complete the import wizard.
   Check the content and click **Finish.**
   After the import is completed, the virtual machines imported into Hyper-V manager are displayed.

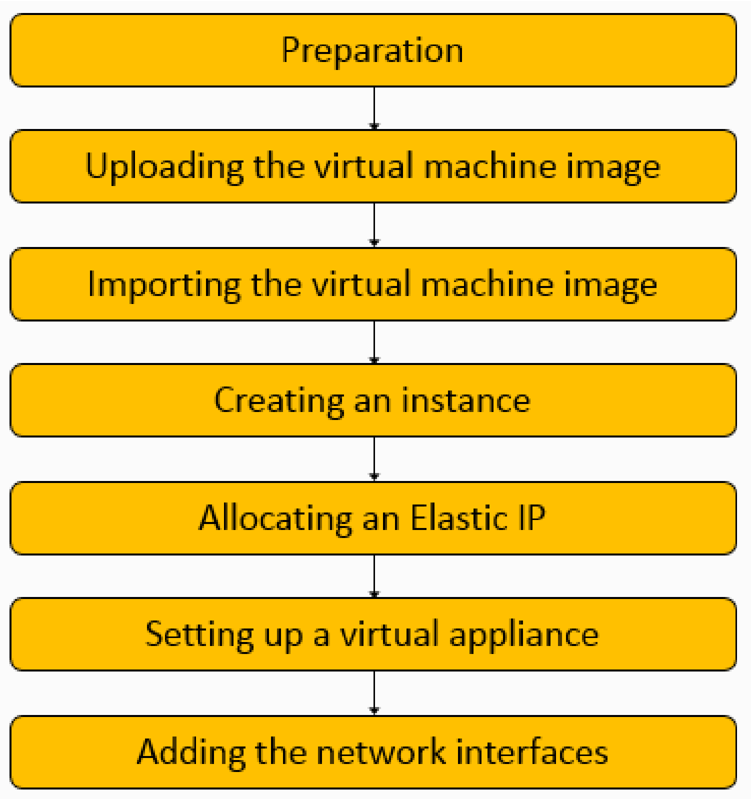
10. Refer to "A.1 Virtual Appliance Specifications" to change the number of virtual processors and memory size as required.
    Select the virtual machine on the Hyper-V manager and then click **Settings...** .
    Select the **Processor** and **Memory** from the **Hardware** and then edit.

11. Add a hard drive for the cache area estimated in "2.1.2 Cache Capacity".
    Select the virtual machine on the Hyper-V manager and then click **Settings...** .
    Select **SCSI Controller** from **Hardware** and add a hard drive.
    The recommended disk format is **VHDX**. Specify **Fixed size** for the disk type.

12. Add a network adapter to the virtual machine.
    Select the virtual machine on the Hyper-V manager and then click **Settings...** .
    Click **Add Hardware** to add a network adapter.
    For a multi-network configuration, add multiple network adapters.

2.2.4 Installing to Amazon EC2

The procedure for installing a virtual machine in an Amazon EC2 environment for this product is described below.
Perform the following operations from the AWS Management Console.



Preparation
Uploading the virtual machine image
Importing the virtual machine image
Creating an instance
Allocating an Elastic IP
Setting up a virtual appliance
Adding the network interfaces

Point

Be sure to grant AmazonEC2FullAccess, AmazonS3FullAccess, and IAMFullAccess access permissions to the AWS account users who perform operations. To grant access permissions, use the IAM service on the AWS Management Console.

1. Preparation
   Set up the following items according to your environment.

   - Network (VPC)

   - Subnet

   - Security group

   ### See

   Refer to "A.6 Used Port Number" for details on the security group settings.

2. Uploading the virtual machine image
   Use the S3 service from the AWS Management Console to create a bucket to store image on Amazon S3 and upload virtual machine image for Amazon EC2.

   - Create a bucket.
     Click **Create bucket** to create a bucket.

   - Upload virtual machine image.
     Go to the list of buckets and click a bucket you have created.
     Click **Upload** and specify a CSG_v120_ec2-disk1.vmdk file included in the virtual machine image for Amazon EC2 (CSG_v120_ec2.zip).

Note

The uploading process may fail in some web browsers. If that happens, try using a different web browser or the AWS Command Line Interface (AWS CLI). Refer to the documents related to Amazon Web Services for details on AWS CLI.

3. Importing the virtual machine image
   Use the AWS command line interface (AWS CLI) to import the virtual machine image stored in Amazon S3.
   Refer to the documents related to Amazon Web Services for details on AWS CLI.
   Refer to "VM Import/Export User Guide" for Amazon Web Services for details on the importing procedure.
   When the importing process is completed, you can check the imported image in the **AMI** section of the EC2 Dashboard. Selecting the image and clicking **Edit** to set a name in the **Description** section is recommended to easily find the image for future operations.

Point

- The operating system type for the virtual machine image to be imported is Linux/Unix (64-bit).
- The image is in the vmdk format.
- When importing an image, you must specify a license option. Specify **BYOL**.

4. Creating an instance
   Use the EC2 service from the AWS Management Console to create an instance from an imported virtual machine image. Click **Launch Instance** on the EC2 dashboard, and follow the on-screen instructions to create an instance by referring to the table below.

Step		Item	Setting Details
1. Choose AMI		-	Select a virtual machine image you have imported from **My AMIs**.
2. Choose Instance Type		-	Select a type that meets the requirements listed in "A.1 Virtual Appliance Specifications."
3. Configure Instance		Number of instances	1
		Network	Select the network you set up in step 1. For this instance, select a network (VPC) to which you can log in remotely via ssh.
		Subnet	Select the subnet you set up in step 1. For this instance, select a subnet to which you can log in remotely via ssh.
		Auto-assign Public IP	**Use subnet settings (Enable)**
		Other	(As necessary)
4. Add Storage	System area	Size	100GiB
		Volume Type	**General Purpose SSD (gp2)** recommended
		Other	(As necessary)
	Cache area	Volume Type	**EBS**
		Device	Select an item from the top of the menu.
		Snapshot	Do not enter any value.
		Size	Enter the capacity you estimated according to the procedure described in "2.1.2 Cache Capacity"
		Volume Type	**General Purpose SSD (gp2)** recommended
		Other	(As necessary)
5. Add Tags		-	(As necessary)

Step	Item	Setting Details
6. Configure Security Group	Assign a security group	**Select an existing security group**
	Security group	Select the security group you set up in step 1.
7. Review	Select a key pair	**Proceed without a key pair**

Point

- In step 4 ("Add Storage"), only the system area storage is built automatically. Click **Add New Volume** to build storage for the cache area.
- The device name you select in step 4 ("Add Storage") is in the /dev/sda or /dev/sdb format. However, on the console of this product, the name is recognized in the /dev/xvda or /dev/xvdb format.
- If you add the "Name" key in step 5 ("Add Tags"), you can set a name for the instance and volume.
- Click **Launch** in step 7 ("Review") to open the key pair selection screen.
- After creating an instance, it is recommended that you include the instance name in the **Name** sections for the instance, storage (volume), and automatically allocated network interface to make these items easier to find in the future. For the storage (volume), it is recommended that you also include the device name.

5. Allocating an Elastic IP

Point

- A public IP is automatically allocated to each created instance. This public IP is released when the corresponding instance is stopped. The next time you start the instance, a different public IP is allocated. If you want to fix a public IP, allocate an Elastic IP first.
- When adding a network interface to configure multiple networks, be sure to allocate an Elastic IP.

- Allocating a new address
  Click **Elastic IPs** on the EC2 dashboard menu.
  Click **Allocate new address** and follow the on-screen instructions.
- Associating the address
  Select the created Elastic IP and select **Associate address** from **Actions**. Refer to the table below and follow the on-screen instructions.

Item	Setting Details
Resource type	**Network interface**
Network interface	Select the network interface that was automatically allocated when the instance was created.
Private IP	Select the IP address that was automatically allocated when the instance was created.

6. Setting up a virtual appliance
   When adding a network interface to configure a system with multiple networks, be sure to allocate an Elastic IP according to the procedure described in step 5 and then set up a virtual appliance. Refer to "2.3 Setting Up Virtual Appliances" for details on how to set up a virtual appliance.

7. Adding the network interfaces
   When configuring a system with multiple networks, follow the procedure below to add the network interfaces.

Note

Before adding the network interfaces, follow the procedure described in step 5 to allocate an Elastic IP, and then set up a virtual appliance according to the procedure described in step 6.

- Stop the instance.
  If the instance of this product is operating, stop it.
  Use the administrator account (administrator) to log in to the console of this product and stop the instance with the following command.

```
# csgadm power stop
```

- Create a network interface.
  Click **Network Interfaces** on the EC2 dashboard menu.
  Click **Create Network Interface** and follow the on-screen instructions to create a network interface by referring to the table below.

Item	Setting Details
Description	Entering a description that includes the instance name is recommended to easily find the interface.
Subnet	Select a subnet set up in step 1 that is in the same region as the subnet you selected to create the instance.
IPv4 Private IP	**auto assign** recommended
Security groups	Select the security group set up in step 1.

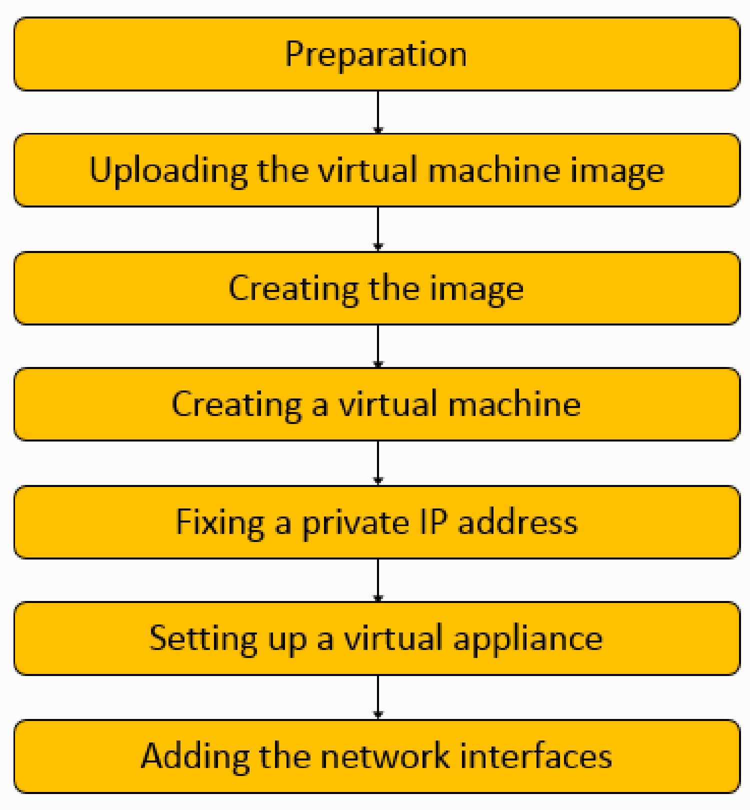
- Attach the interface to an instance.
  Select the created network interface, and then select **Attach** from **Actions**. Follow the on-screen instructions to attach the interface to the created instance.

Point

Including the instance name in the **Name** section of the interface is recommended to easily find the created network interface for future operations.

2.2.5 Installing to Microsoft Azure

The procedure for installing a virtual machine in a Microsoft Azure environment for this product is described below.
Perform the following operations from the Azure portal.



Preparation

Uploading the virtual machine image

Creating the image

Creating a virtual machine

Fixing a private IP address

Setting up a virtual appliance

Adding the network interfaces

1. Preparation
   Set up the following items according to your environment.

   - Virtual network

   - Subnet

   - Network security group

2. Uploading the virtual machine image
   Upload a virtual machine image to the Blob storage.
   The uploaded virtual machine image is a vhd file included in the virtual machine image for Microsoft Azure (CSG_v120_Azure.zip).

   Note

   The size of the system disk for this product is 100 GB. There are two types of vhd files: the fixed size type and the variable size type. Azure only supports the fixed size type. Therefore, the zip file contains a 100-GB vhd file. Before extracting the zip file, make sure there is at least 100 GB of free space in your environment.

   - Creating a storage account
     Navigate to the **Storage accounts** service on the Azure portal, and click **Add**.
     Refer to the table below, and follow the on-screen instructions to create a storage account.

Tab	Item	Setting Details
Basics	Subscription	Enter a subscription.
	Resource group	Enter a resource group.
	Storage account name	Enter a storage account name
	Location	Enter a location.
	Performance	**Standard** recommended
	Account kind	**StorageV2 (general purpose v2)**

Tab	Item	Setting Details
	Replication	**Locally-redundant storage (LRS)** recommended
	Access tier	**Cool** recommended
Advanced	Secure transfer required	**Enabled** recommended
	Allow access from	Select an item.
	Hierarchical namespace	Select an item.
Tags	-	(As necessary)

- Creating a container
  Select a storage account you have created.
  Select **Blobs** on the **Blob service** menu of your storage account.
  Click **Container**.
  Refer to the table below, and follow the on-screen instructions to create a container.

Item	Setting Details
Name	Enter a name.
Public access level	**Private**

- Uploading virtual machine image
  To upload a virtual machine image, use Azure Storage Explorer.
  Select a storage account you have created, and then click **Open in Explorer.**
  If you are launching this software for the first time, follow the on-screen instructions, download Azure Storage Explorer, and install it.
  Navigate to the tree in Azure Storage Explorer, and select a container you have created.
  Click **Upload**, and select **Upload Files...**.
  Refer to the table below, and follow the on-screen instructions to upload a virtual machine image.

Item	Setting Details
Files	A vhd file of the virtual machine image
Blob type	**Block Blob** Select the **Upload .vhd/vhdx files as page blobs** checkbox.

Point

Using Azure Storage Explorer, be sure to add account for Azure Storage Explorer and set a proxy as necessary. You can add up **View - Account Managemen**t - **Add an account...** for account. You can set up **Edit - Configure Proxy** for proxy. Refer to Microsoft Azure documents about Azure Storage Explorer for details.

3. Creating an image
   Navigate to the **Images** service on the Azure portal, and click **Add**.
   Refer to the table below, and follow the on-screen instructions to create an image.

Item	Setting Details
Name	Enter a name.
Subscription	Enter a subscription.
Resource group	Enter a resource group.
Location	Enter a location.
Zone resiliency	**Off** (if available)
OS type	**Linux**

Item	Setting Details
Storage blob	Select a virtual machine image you have uploaded.
Account type	**Standard HDD** recommended
Host caching	**Read/write**
Data disks	Do not add any new items.

4. Creating a virtual machine
   Navigate to the **Virtual machines** service on the Azure portal, and click **Add**.
   Refer to the table below, and follow the on-screen instructions to create an image.

Tab	Item	Setting Details	
Basics	Subscription	Enter a subscription.	
	Resource group	Enter a resource group.	
	Virtual machine name	Enter a virtual machine name.	
	Region	Enter a region.	
	Availability options	**No infrastructure redundancy required**	
	Image	Go to **My Items**, and select an image you have created.	
	Size	Select a size that meets the requirements listed in "A.1 Virtual Appliance Specifications." Select a size that has a temporary storage size larger than 4 GB.	
	ADMINISTRATOR ACCOUNT	Authentication type: **Password** Username: **dummy** Password: (Any password)	
	Public inbound ports	Select **None** here since you are going to configure this parameter under in the **Networking** tab.	
Disks	OS disk type	Select a system disk type here. The recommended type is **Standard SSD**. If the **Enable Ultra SSD compatibility** option is available, select **No**.	
	Data disks	These disks are used for the cache area Create a disk by clicking **Create and attach a new disk**.	
		Disk type	**Standard SSD** recommended
		Name	Including the virtual machine name is recommended to easily find the created image for future operations.
		Size	Enter the capacity you estimated according to the procedure described in "2.1.2 Cache Capacity".
		Source type	**None (empty disk)**
		Host caching	**Read/write** This option becomes available after you create a disk. This is not available for some virtual machine sizes.
	Use managed disks	**Yes** Click **Advanced** to see the available options.	
Networking	Virtual network	Select the virtual network you set up in step 1.	
	Subnet	Select the subnet you set up in step 1.	
	Public IP	Select None if a public IP is not required. If you want to create a new one, click Create new, and set the following items.	

Tab	Item	Setting Details	
		Name	Enter a name.
		SKU	**Basic**
		Assignment	Enter an assignment.
	NIC network security group	Select **Advanced**, and then select the network security group you set up in step 1.	
	Accelerated networking	Enter an accelerated networking.	
	Place this virtual machine behind an existing load balancing solution?	**No**	
Management	Boot diagnostics	**On**	
	OS guest diagnostics	**Off**	
	Diagnostics storage account	Enter a diagnostics storage account.	
	System assigned managed identity	**Off**	
	Enable auto-shutdown	**Off**	
Advanced	-	Do not enter any value.	
Tags	-	(As necessary)	

Note

- The procedure for creating a virtual machine includes configuring the **Administrator account** settings. For this product, however, the administrator account is not created and cannot be used.
- If **Dynamic** is set for the public IP assignment, a new IP address is assigned every time you stop and start the virtual machine. If you wish to continue using the same IP, select **Static**.
- When you are logged in to this product with a public IP, a timeout error occurs if the product is left unused for a certain amount of time. To change the timeout period, after creating a virtual machine, click the public IP address in the **Overview** section for the virtual machine and change the parameter in **Idle timeout**.

5. Fixing a private IP address
   You can also assign a private IP address to a network interface to which a public IP address has been allocated. This IP address is also allocated as a new address every time you stop and start the virtual machine. Follow the procedure below if you wish to continue using the same IP.

   a. Go to the **Virtual machines** service on the Azure portal, and click the virtual machine name.

   b. Select **Networking** on the **Settings** menu, and click the network interface name.

   c. Select **IP configurations** on the **Settings** menu, and click the line that contains the private IP address.

   d. Change the assignment setting of the private IP address to **Static**.

6. Setting up a virtual appliance
   Before adding network interfaces in order to build a system with multiple networks, set up the virtual appliance first. Refer to "2.3 Setting Up Virtual Appliances" for details on how to set up a virtual appliance.

7. Adding network interfaces
   When configuring a system with multiple networks, follow the procedure below to add network interfaces.

Note

Before adding network interfaces, follow the procedure described in step 6 to set up the virtual appliance.

- Stopping the virtual machine
  Go to the **Virtual machines** service on the Azure portal, select a virtual machine, and click **Stop** to stop the virtual machine.

- Creating and attaching a network interface
  Select **Networking** on the **Settings** menu for the virtual machine, and click **Attach network interface**.
  Click **Create network interface** and follow the on-screen instructions to create an interface by referring to the table below, and then attach it to the virtual machine.

Item	Setting Details
Name	Including the virtual machine name is recommended to easily find the created image for future operations.
Subnet	Select the subnet you set up in step 1.
Private IP address assignment	Enter a private IP address assignment
Private IP address	If **Private IP address assignment** is set to **Static**, you must specify an unused IP address.
Network security group	Select the network security group you set up in step 1.
Private IP address (IPv6)	Do not select this option.
Resource group	Specify the same resource group as the one to which the created virtual machine belongs.

Point

If you set the private IP address assignment to **Dynamic**, an unused private IP address can be assigned automatically. In this case, a new IP address is assigned every time you stop and start the virtual machine. In order to continue using the same IP address, follow the procedure described in step 5 to fix the private IP address.

2.3 Setting Up Virtual Appliances

After starting the virtual appliance for this product, use the Configuration Wizard to perform setup. The procedure is described below.

1. Log in to the console with the administrator account (administrator) and the default password (Admin123#).

2. Run csgsetup in the current directory.

3. When the Configuration Wizard starts, follow the instructions to perform setup.
   The default keymap is "us". Please be careful while entering information (e.g. changing password) before setting the keymap.
   The following items are displayed:

   - **Change Administrator Password**
   - **Change sftpadmin Password**
   - **Network selection(*2)**
   - **Configure DHCP(*2)**
   - **Setting Hostname**
   - **Configure Network(*1) (*2)**
   - **Configure DNS**
   - **Configure Domain**

- Configure Keymap
- Configure NTP
- Configure time zone

4. A message is displayed asking you to restart the system. Select **OK** to restart the system.

Note

- A default password is set for the administrator account. For security purposes, be sure to change this password under **"Change Administrator Password"** of the Configuration Wizard. The password must be between 8 to 64 characters long. You must use at least three of the following four character types: uppercase letters, lowercase letters, numbers, and symbols (!"#$&'()*+,-./@[\]^_`{|}~:;<=>?).
- Because a default password is not set for the SFTP account (sftpadmin), SFTP cannot be used by default. To use SFTP, change the password by executing "Change sftpadmin Password" of the Configuration Wizard. The same conditions as the administrator password are applied for the allowed characters. The SFTP account (sftpadmin) is a dedicated account for file transfers using SFTP. Unlike the administrator account, this account cannot be used to log in to the console of this product.
- For single network configurations, network selection items are skipped.
- If you choose to use DHCP in the DHCP settings, the settings marked with the (*1) symbol are skipped.
- The Configuration Wizard can set only one network even for multi-network configurations. For multi-networks, the first network is set. For information on setting the second and subsequent networks, refer to "2.5.7 Configuring Multi-network Configurations".
- The following addresses cannot be set as an IP address:
  - The IP addresses set for the second and subsequent networks
  - The gateway address set for the second and subsequent networks
  - The loopback address (127.0.0.1)
- You can set up default gateway in the Configuration Wizard of network setting.
- If the following types of servers are in different subnets, only the network where the default gateway is set can be used to communicate with these servers.
  DNS server, NTP server, mail server (SMTP server), external authentication server (Active directory server).
- For operations with an AD server, be sure to synchronize the clock between this product and the AD server. If NTP is not set, synchronize the clock manually. Refer to "2.5.1 Setting the System Clock" for details.
- If an external authentication server (Active Directory server) is used with SMB, DNS server settings are required.
- For Amazon EC2 and Microsoft Azure environments
  - When you create a virtual machine, an IP address is allocated to the network interface via DHCP. If you run the Configuration Wizard, this network interface is set as the first network. This setting cannot be changed. The settings marked with the (*2) symbol are skipped in Amazon EC2 and Microsoft Azure environments.
  - When adding network interfaces to the virtual machine in order to configure multiple networks, be sure to run the Configuration Wizard in advance.

2.4 Allocating Local Storage to Storage Pool for Cache

Use the following procedure to allocate the local storage to a storage pool for cache (with the name fixed to "CsgStoragePool").

Note

The following procedure uses VMware vSphere, or Hyper-V as an example.
For KVM, change "/dev/sdX" to "/dev/vdX."
For Amazon EC2, change "/dev/sdX" to "/dev/xvdX."

In Microsoft Azure, "/dev/sdaX" and "/dev/sdbX" represent the virtual disks for the system area. The virtual disks for the cache area are marked "/dev/sdc."

1. Log in to the console using the administrator account (administrator).
2. Execute the following command to confirm that the virtual disk for the cache area that you added in "2.2 Deploying Virtual Appliances" is recognized.
   In the following example, the virtual disk that was added is recognized as "/dev/sdb".

```
# csgadm storagepool diskscan
  /dev/sda1 [     953.00 MiB]
  /dev/sda2 [      27.94 GiB]
  /dev/sda3 [      27.94 GiB]
  /dev/sda5 [      27.94 GiB]
  /dev/sda6 [       3.72 GiB]
  /dev/sdb  [     100.00 GiB]
  1 disk
  5 partitions
  0 LVM physical volume whole disks
  0 LVM physical volumes
```

3. Execute the following command to allocate local storage to a storage pool for cache.

```
# csgadm storagepool create -disk /dev/sdb
```

4. Execute the following command to confirm that local storage has been allocated to a storage pool for cache.

```
# csgadm storagepool show
  PV         VG             Fmt  Attr PSize   PFree
  /dev/sdb   CsgStoragePool lvm2 a--  100.00g 100.00g

  VG             #PV #LV #SN Attr   VSize   VFree
  CsgStoragePool   1   0   0 wz--n- 100.00g 100.00g
```

Information

Execute the following command to delete a storage pool for cache.

```
# csgadm storagepool remove
```

You can delete a storage pool only if there is no cache in the storage pool. Refer to "7.1.2 Deleting a Datastore" for details about how to delete the cache.
If the cache exists in the storage pool, the Csgadm storagepool show command displays the following:

```
# csgadm storagepool show
  PV         VG             Fmt  Attr PSize     PFree
  /dev/sdb   CsgStoragePool lvm2 a--  61436.00m 10236.00m

  VG             #PV #LV #SN Attr   VSize     VFree
  CsgStoragePool   1   1   0 wz--n- 61436.00m 10236.00m

  LV   VG             Attr       LSize     Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  ds1  CsgStoragePool -wi-ao---- 51200.00m
```

Note

If the data store fails to be created due to a system down or system failures, the cache may remain in the storage pool. If you cannot delete the cache using the procedure in "7.1.2 Deleting a Datastore", forcibly delete the storage pool by using the following command:

```
csgadm storagepool remove -force
```

2.5 Environment Setup

2.5.1 Setting the System Clock

Use the following procedure to set the system clock.
You do not need to perform this procedure if the NTP server is set to be used with **Configure NTP** in the Configuration Wizard.

1. From the console, log in to the virtual machine as the administrative user in which this product is running.

2. Confirm the current time.

```
# csgadm time show
      Local time: Wed 2017-04-05 02:25:41 UTC
  Universal time: Wed 2017-04-05 02:25:41 UTC
                        :
```

3. Set the time and date.

```
# csgadm time set-time date time
```

Example

The following example shows the command for setting the time and date to 11:26 November 30, 2017.

```
# csgadm time set-time 2017-11-30 11:26:00
```

Information

If you change the date and time in this procedure after setting up the environment, restart the system.
Verify that there is no business impact, and then restart by running the following command:

```
# csgadm power restart
```

Note

If you change the date and time in the opposite direction, the log or performance graph may not be displayed correctly because the log and performance data for this product are duplicated in the time slot before and after the change.

2.5.2 Setting a Proxy

If the cloud provider requires access via a proxy, perform the following procedure.

1. From the console, log in to the virtual machine as the administrative user in which this product is running.

2. Execute the following command to set a proxy.

```
# csgadm httpclient set -proxy http://proxyHost:proxyPort -proxy-user userName -proxy-password
password
```

3. Execute the following command to check the value that has been set for the proxy.

```
# csgadm httpclient show
```

4. Execute the following command to restart the system.

```
# csgadm power restart
```

Note

For the proxy server address specified with the "-proxy" argument, specify the "http://" or "https://" protocol according to the proxy server specification.

If there is no specification for the protocols in the proxy server, specify "http://" for the argument.

Specify according to the proxy server specifications, not the cloud provider protocol.

Information

To delete the proxy setting, specify "" for each item.

```
# csgadm httpclient set -proxy "" -proxy-user "" -proxy-password ""
```

2.5.3 Browser Settings

Web GUI is operated from a Web browser of a PC terminal. Perform the Web browser settings in advance. For Web browsers that can be used, refer to "A.3 Support List".

2.5.3.1 JavaScript Settings

The CSG Web GUI needs JavaScript to be enabled in the web browser.

For Internet Explorer

1. Click the **Tools** menu, and then click **Internet Options**.
   The **Internet Options** dialog box is displayed.

2. On the **Security** tab, select **Trusted sites**. Then, click **Sites**.
   The **Trusted sites** dialog box is displayed.

3. Enter the IP address of this product, and then click **Add**. If the addition is finished, click **Close** to close the **Trusted sites** dialog box.
   The **Internet Options** dialog box is displayed again.

4. Click **Custom level** with **Trusted sites** selected.
   The **Security Settings** dialog box is displayed.

5. Scroll down the **Security Settings** list until you reach the **Scripting** section. Under the **Active scripting**, select **Enable**.

For Microsoft Edge

No action is required because JavaScript is enabled in the initial settings.

For Chrome

Follow the procedure listed in the Chrome support site to enable JavaScript.

https://support.google.com/chrome

2.5.3.2 Cookie Settings

The CSG Web GUI needs cookies to be enabled in the web browser.

For Internet Explorer

1. Click the **Tools** menu, and then click **Internet Options**.
   The **Internet Options** dialog box is displayed.

2. On the **Privacy** tab, click **Advanced**.
   The **Advanced Privacy Settings** dialog box is displayed.

3. Check the **Override automatic cookie handling** checkbox, and check **Accept** in the First-party Cookies

For Microsoft Edge

1. Click the **More** (...) on the upper right of the screen, and then click **Settings**.
   The Settings screen is displayed.

2. Click **View advanced Settings** of the **Advanced settings** category.
   The Advanced settings screen is displayed.

3. Select **Don't Block Cookies** in **Cookies** of **Privacy and services**.

Note

The button names may vary depending on the version of Microsoft Edge.

For Chrome

Follow the procedure listed in the Chrome support site to enable cookie.

https://support.google.com/chrome

2.5.3.3 Internet Explorer Compatibility View Settings

When using Internet Explorer, disable Compatibility View.

The procedure to disable it is as follows:

For Internet Explorer

1. Click the Tools menu, and then click **Compatibility View Settings**.
   The **Compatibility View Settings** dialog box is displayed.

2. If the IP address or host name of the virtual machine in which this product is running is displayed in Websites you've added to Compatibility View, select that address and then click **Remove**.

3. Uncheck the **Display intranet sites in Compatibility view** checkbox.

Note

Performing the above step 3. setting may disable a Compatibility View enabled site and change its screen view.

For a site whose screen view is changed, causing a trouble to operation, add URL separately on the Compatibility View

Settings window to enable Compatibility View.

On the Compatibility View Settings dialog box, the following checkbox is Internet site configuration and no setting is required.

- "Use Microsoft compatibility lists"

2.5.4 Setting the CSG Web GUI Communication

2.5.4.1 Setting an HTTPS Communication

This product uses an HTTPS communication with web browsers and uses a security certificate for encrypting and performing mutual authentication of communication data. By default, a self-signed certificate is used when this product is installed. For safe networks such as an intranet that is protected by a firewall, there is no problem with using a self-signed certificate. However, the following warning messages might be generated if the web browser is used to access the Internet.

- When the web browser is started and a connection is made for the first time, a warning message is displayed regarding the security certificate.

To disable this warning message, create a certificate for the IP address of this product or host name (FQDN) that is entered in the web browser and import it into the web browser.

Creating a Certificate

From your terminal (Windows or Linux), execute the openssl command on the virtual machine in which this product is running in order to create a certificate.

Example

The following example shows the command for setting a certificate with an expiration period of 20 years (-days 7300) for a virtual machine (in which this product is running) with an IP address of 192.0.2.10.

1. Edit openssl.cnf, and add for the IP address of this product or host name (FQDN).

   - Define the “req_extensions = v3_req” in the [req] section.

   ```
   [ req ]

   req_extensions = v3_req
   ```

   - Define the ”subjectAltName = @alt_names” in the [v3_req] section.

   ```
   [ v3_req ]

   subjectAltName = @alt_names
   ```

   - Define the [alt_names] section, and IP address in the section.
     If defining host name (FQDN), define it in the format “DNS.1 = “.

   ```
   [ alt_names ]
   IP.1 = 192.0.2.10
   ```

2. Execute the following command with the edited openssl.cnf specified to create a certificate.

   ```
   >..\bin\openssl.exe req -extensions v3_req -sha256 -new -x509 -nodes -newkey rsa:2048 -out
   server.crt -keyout server.key -days 7300 -config openssl.cnf <RETURN>
   Generating a 2048 bit RSA private key
   ..+++
   ....................................................+++
   writing new private key to 'server.key'
   -----
   You are about to be asked to enter information that will be incorporated into your certificate
   request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [XX]:<RETURN>
   State or Province Name (full name) []:<RETURN>
   ```

```
Locality Name (eg, city) [Default City]:<RETURN>
Organization Name (eg, company) [Default Company Ltd]:<RETURN>
Organizational Unit Name (eg, section) []:<RETURN>
Common Name (eg, your name or your server's hostname) []:192.0.2.10<RETURN>
Email Address []:<RETURN>
```

Option

-out

Specify the name of the crt file to be generated.

-keyout

Specify the name of the key file to be generated.

-days

Specify the period for which the certificate is valid.
This option is counted from the date when the command is executed. Enter a sufficiently long number of days, up to January 19th, 2038.

-config

Specify the openssl.cnf.

Input Items

Item	Required?	Description
Country Name	Optional	The two-letter abbreviation for your country (ISO-3166)
State or Province Name	Optional	The state or province where this product is located
Locality Name	Optional	The city where this product is located
Organization Name	Optional	The exact legal name of your organization
Organizational Unit Name	Optional	Optional for additional organizational information
Common Name	Required	Enter the IP address or the host name (FQDN) of the virtual machine in which this product is running. Examples are shown below. - When specifying an IP address: 192.0.2.10 - When specifying a host name: myhost.example.com
Email Address	Optional	Contact E-mail address

Setting a Certificate

After a certificate has been created, register it in this product.

1. Transfer the certificate (key file and crt file) that has been created via SFTP to the virtual server in which this product is running.
    - Transfer destination: /Administrator/ftp
    - User: sftpadmin
    - Password: The password set under "Change stpadmin Password" in the Configuration Wizard.
2. Log in to the console using the administrator account (administrator).
3. Execute the following command to register the certificate in this product.

```
# csgadm sslcert set -key /Administrator/ftp/server.key -crt /Administrator/ftp/server.crt
```

4. Execute the following command to confirm that the certificate is registered correctly.

```
# csgadm sslcert show
```

5. Execute the following command to restart the HTTP service.

```
# csgadm service restart fjsvcsgcp-webserver.service
```

Importing a Certificate

Import the certificate to the web browser that you are using. Refer to "A.3 Support List" for details about the supported web browsers. Follow the procedure for the web browser you are using to import the certificate.

Information

You can use the following procedure to export the SSL server certificate that is registered in this product.

1. From the console, log in to the virtual machine as the administrative user in which this product is running.
2. Execute the following command.

```
# csgadm sslcert export -dir /Administrator/ftp
```

You can use SFTP to download the SSL server certificate that you have exported.

2.5.4.2 Setting the HTTPS Port Number

Use the following procedure to set the HTTPS port number.
You do not need to perform this procedure if you use the default HTTPS port number (9856).

1. From the console, log in to the virtual machine as the administrative user in which this product is running.
2. Execute the following command to set the HTTPS port number.
   Set a number in the range from 5001 to 9999.

```
# csgadm service modify -port portNumber
```

Example

The following example shows the command for changing the port number to 5001.

```
# csgadm service modify -port 5001
```

3. After executing the command in step 2, you are asked if you want to reboot the system. Select "y" to reboot the system.

2.5.5 Starting CSG Web GUI

Use the following procedure to start CSG Web GUI.

1. Start the web browser.
   Refer to "A.3 Support List" for details about the supported web browsers.
2. Enter the following URL in the address bar on the web browser:

```
https://hostName:portNumber/
```

For *hostName*, specify the IP address or FQDN of the virtual machine in which this product is running.
For *portNumber*, specify the port number that is set in "2.5.4.2 Setting the HTTPS Port Number". If you have not changed the default HTTPS port number (9856), set this value to 9856.

Note

- For the URL in the web browser, enter either the IP address or FQDN that you specified for **Common Name** when you performed the procedure for "Creating a Certificate" in "2.5.4.1 Setting an HTTPS Communication".
- If the URL is different from the certificate such as in the following examples, a certificate warning message is displayed. To prevent the warning message, create a certificate for the IP address or FQDN that you entered for the URL:
    - A certificate created with an FQDN is accessed using the URL that is specified with an IP address
    - A certificate created with an IP address is accessed using the URL that is specified with an FQDN
    - The virtual machine in which this product is running has multiple IP addresses and the IP address used in the URL is different from the one specified for the certificate

3. The initial user creation screen is displayed.
Enter the required items and click **Done**.

- Input Items

Item	Required?	Description
Name	Required	Specify a username. Alphanumeric characters and symbols (!-._) can be used. The specifiable character string is 1 to 64 characters.
Password	Required	Specify a password. Alphanumeric characters and symbols (!"#$&'()*+,-./@[\]^_`{|}~:;<=>?) can be used. The specifiable character string is 8 to 64 characters. A minimum of three of the four following character types must be used: uppercase letters, lowercase letters, numbers and symbols.
Role	Required	Permission of the user. The role is fixed to Administrator.
Mail address	Optional	Specify an E-mail address for the user specified in the "Name" item.
Description	Optional	Enter a description of the user that is specified in the "Name" item.

After you have completed the above procedure, the CSG Web GUI dashboard is displayed.

See

An initial user can be created with the CSG REST API. Refer to "Initial User Creation" in the "Reference Guide".

Note

- To log in to CSG Web GUI, enter the username and password for the user that was created in the initial user creation screen.
- If the browser URL is forcibly changed, you might see the following message during login: "The operation failed. Login failed. This user is already logged in on the same terminal." In such a case, please restart the login browser and try to login again.
Depending on the browser settings, you might see the same error message even after restarting the browser. In such a case, please clear the browser cookies and try to login again.
- The following message may be displayed during the operation of CSG Web GUI.

```
st10500001: Internal error occurred.
```

If the message occurs even if the operation is re-executed, reboot this product and try again. If the problem persists, collect the information required for troubleshooting and contact our customer support department.

Point

When CSG Web GUI is started for the first time, the following charts and graphs are not displayed:

- Pie chart on the **Used cache capacity** panel
- Pie chart on the **Used datastore capacity** panel
- Line graph on the **Cache I/O performance** panel
- Line graph on the **Cloud transfer performance** panel

These charts and graphs are displayed after you have defined and started operation of the datastore.

2.5.6 Registering a License

Use the following procedure to register a license for this product.

1. In CSG Web GUI, click [⚙] on the global pane.
2. The **Settings** dialog box is displayed.
   Click **License** on the left pane.
3. The **License** screen is displayed on the right pane.
   Click **Add** in the **Action** on the right.
4. The **Add license** screen is displayed.
   Enter your license key, and then click **Done**.
5. In the **License** screen, confirm that the license you registered appears.

After you register a license, the following license information appears on the CSG Web GUI global pane.

Table 2.4 License Information Displayed on the CSG Web GUI Global Pane

Registered License	License Information
Unregistered	"Any license is not applied" is displayed.
Trial license	The valid period (number of days remaining) for the trial license is displayed. When the valid period expires, "Trial period expired" is displayed.
Regular license	Nothing is displayed.

Note

Two types of regular licenses are available: Basic license and Additional capacity license.
To register the Additional capacity license, the Basic license must be registered in advance.

See

You can also register your license with the CSG REST API. Refer to "License" in the "Reference Guide" for how to register.

2.5.7 Configuring Multi-network Configurations

For multi-network configurations, set up the first network with the Configuration Wizard. The second and subsequent networks are configured with the CSG REST API by using the first network.
For information about the Configuration Wizard, refer to "2.3 Setting Up Virtual Appliances"
In addition, refer to "Network" in the "Reference Guide" for instructions on setting up the CSG REST API.

Network Information

You can browse information about the network that you set up.
You can also browse information about the first network. The network ID of the first network is "0" and the Network Name "NET#00".

Registering your network

Set the IP address of the network where you assigned the virtual appliance.

Note

If your network registration fails, your registration information may remain. Browse the network information to see which network registrations failed. Then, after you have deleted the network, you must register the network again.

Changing the network

Change the settings for the network that you added.
You can only change the network name for the first network.

Note

- If you are using CSG Web GUI/CSG REST API, NAS access, and cloud forwarding, communication errors will occur. Stop use of the CSG Web GUI/CSG REST API and NAS access in advance. Simply changing the network name will not cause an error.

- If the network cannot communicate with the DHCP server, changing from a fixed IP to DHCP fails. When communication with the DHCP server is available, perform the switch to the DHCP server again.

Deleting a network

Delete a network that you added.
You cannot delete the first network.

Note

The network that you are using to communicate with the cloud provider cannot be deleted by default.

2.5.8 Monitoring Settings

Configure the settings in "2.5.8.1 E-mail Server Settings" and "2.5.8.2 E-mail Notification Settings" to send E-mail notifications regarding events that occur in this product.

2.5.8.1 E-mail Server Settings

Setting Procedure

The procedure for setting the E-mail server is described below.

1. In CSG Web GUI, click [⚙] on the global pane.

2. The **Settings** dialog box is displayed.
   Click **Monitoring** > **Mail server** on the left pane.

3. The **Mail server** screen is displayed on the right pane.
   Enter the required information, and then click **Apply**.

Input Items

Item	Required?	Description
SMTP server	Required	Specify the address of the SMTP server. Specify up to 64 characters in either IPv4 format or FQDN format for the address of the SMTP server.
Sender mail address	Required	Specify the E-mail address for the person sending the E-mail.
SMTP port	Optional	Specify the port number for the SMTP server. If omitted, the setting defaults to 25.
Authentication method	Required	Specify the authentication method to be used when connecting to the SMTP server. - none Connects to the SMTP server without using authentication. - cram-md5 The device uses cram-md5 for the authentication method. - plain The device uses plain for the authentication method. - login The device uses login for the authentication method.
User name	Required	When the authentication method is specified as something other than none, specify the user name for connecting to the SMTP server.
Password	Required	When the authentication method is specified as something other than none, specify the password for the user for connecting to the SMTP server.

See

You can also configure the Mail Server with CSG REST API. Refer to "Mail Server" in the "Reference Guide" for how to configure this.

2.5.8.2 E-mail Notification Settings

Setting Procedure

The procedure for setting E-mail notifications is described below.

1. In CSG Web GUI, click [⚙] on the global pane.
2. The **Settings** dialog box is displayed.
   Click **Monitoring** > **Mail notification** on the left pane.
3. The **Mail notification** screen is displayed on the right pane.
   Enter the required information, and then click **Apply**.

Input Items

Item	Required?	Description
Mail address 1	Optional	Enter an E-mail address for sending event notifications.
Mail address 2	Optional	Same as above
Mail address 3	Optional	Same as above

Content of Notifications

The content of notifications sent by E-mail is described below.
If the same event occurs successively within 20 seconds, additional notification is not sent.

- Event E-mail

Item	Content
Subject	Cloud Storage Gateway Event Mail
From	The sender's E-mail address that was specified in "2.5.8.1 E-mail Server Settings".
To	The notification E-mail addresses that were specified in "2.5.8.2 E-mail Notification Settings". If there are multiple notification E-mail addresses, notification is sent simultaneously to all registered E-mail addresses.
Text	Severity: <Event log level (Warning or Error)> Date: <Date and time the event occurred> Appliance Address: <IP address of the virtual machine in which this product is running> Target Name: <Cloud provider name/bucket name or "System"> Message ID: <Message ID> Message: <Message>

See

Refer to the "Reference Guide" for details about "Messages".

- Test E-mail

Item	Content
Subject	Cloud Storage Gateway Test Mail
From	The sender's E-mail address that was specified in "2.5.8.1 E-mail Server Settings".
To	The notification E-mail addresses that were specified in "2.5.8.2 E-mail Notification Settings". If there are multiple notification E-mail addresses, notification is sent simultaneously to all registered E-mail addresses.
Text	Severity: Information Date: <Date and time when the E-mail was sent> Appliance Address: <IP address of the virtual machine in which this product is running> Target Name: - Message ID: - Message: TEST MAIL

See

You can set the email notification destination with the CSG REST API. Refer to "Mail Notification" in the "Reference Guide" for how to configure this.

2.6 Setting CSG Web GUI / CSG REST API Users

Follow the procedure described below to access CSG Web GUI or CSG REST API as a user that was not created in "2.5.5 Starting CSG Web GUI"

- With a local authentication user

  You can register a local authenticated user in this product, and then access CSG Web GUI and CSG REST API via that account.

2.6.1 Settings When Using CSG Web GUI and CSG REST API with the Local Authentication User

When using CSG Web GUI and CSG REST API with the local authentication user, register the local authentication user in this product in advance.

Setting Procedure

The procedure for registering a local authenticated user in this product is described below.

1. In CSG Web GUI, click [⚙] on the global pane.
2. The **Settings** dialog box is displayed.
   Click **Authentication** > **Local authentication user** on the left pane.
3. The Local authentication user list screen is displayed.
   Click **Create** in the Action on the right.
4. The Create local authentication user screen is displayed.
   Enter the required information, and then click **Done**.
5. In the **Local authentication user list** screen, confirm that the local authenticated user you registered appears.

Point

You can register up to 100 users.

Input Items

Item	Required?	Description
Name	Required	Specify a user name. You can use single-byte alphanumeric characters and symbols (!-._). Specify from 1 to 64 characters.
Password	Required	Specify a password. You can use alphanumeric characters and symbols (!"#$&'()*+,-./@[\]^_`{|}~:;<=>?). Specify from 8 to 64 characters. You must use at least three of the following four types of characters: uppercase letters, lowercase letters, numbers, and symbols.
Role	Required	Specify the user's privileges. - Administrator Administrator privileges - Monitor Viewing only
Mail address	Optional	Specify the E-mail address for the user specified under "Name". An E-mail address of a user that is already registered cannot be specified.
Description	Optional	Enter a description for the user specified under "Name".

See

You can also register an internal authentication user with the CSG REST API. Refer to "Local Authentication User" in the "Reference Guide" for how to register.

2.7 Setting NAS Access Users

Define the NAS authentication information that is required to access the shared folders in this product from the backup server.

When using SMB for authentication, you can select either a local authentication user (the method of defining a user for accessing the NAS) or an external authentication user (the method of using an AD server).
When using NFS for authentication, you can only select a local authentication user.

2.7.1 Settings When Accessing the NAS with the Local Authentication User

When accessing the NAS with the local authentication user, perform the procedures in "2.7.1.1 NAS Access Group Settings" and "2.7.1.2 NAS Access User Settings".

2.7.1.1 NAS Access Group Settings

Setting Procedure

The procedure for registering an NAS access group is described below.

1. In CSG Web GUI, click [⚙] on the global pane.
2. The **Settings** dialog box is displayed.
   Click **NAS access** > **NAS access group** on the left pane.
3. The **NAS access group** screen is displayed on the right pane.
   Click **Add** in the Action on the right.
4. The **Add NAS access group** screen is displayed.
   Enter the required information, and then click **Done**.

Point

You can register up to 100 groups.

Input Items

Item	Required?	Description
Name	Required	Specify a NAS access group name. You can use single-byte alphanumeric characters and symbols ($-_). Specify from 1 to 32 characters. The dollar sign ($) can only be used as the last character of the name. The first character in the name must be an alphanumeric character or an underscore (_). The name is not case sensitive. - The name cannot contain only numbers. - You cannot specify a group that already exists. - You cannot use the following reserved keywords: adm, audio, bin, BUILTIN_Administrators, BUILTIN_BackupOperators, BUILTIN_Users, cdrom, cgred, chrony, csgadm, daemon, dbus, dialout, dip, disk, floppy, ftp, games, input, kmem, ldap, lock, lp, mail, man, mem, nfsnobody, nobody, nscd, polkitd, postdrop, postfix, postgres, root, rpc, rpcuser, sharegroup$, sshd, ssh_keys, sys, systemd-bus-proxy, systemd-journal, systemd-network, tape, tss, tty, users, utempter, utmp, vauser, video, wbpriv, wheel - When the NAS authentication server is registered in this product, the group name registered in the NAS authentication server cannot be set.
Group ID	Optional	Specify a number from 500 to 999 as the ID for the local group to be created. If this setting is omitted, the system automatically assigns a number.

See

You can also register your NAS access group with the CSG REST API. Refer to "NAS Access Group" in the "Reference Guide" for how to register this.

2.7.1.2 NAS Access User Settings

Setting Procedure

The procedure for registering a NAS access user in this product is described below.

1. In CSG Web GUI, click [⚙] on the global pane.
2. The **Settings** dialog box is displayed.
   Click **NAS access** > **NAS access user** on the left pane.
3. The **NAS access user** screen is displayed on the right pane.
   Click **Add** in the Action on the right.
4. The **Add NAS access user** screen is displayed.
   Enter the required information, and then click **Done**.

Point

You can register up to 100 users.

Input Items

Item	Required?	Description
Name	Required	Specify a NAS access user name. You can use single-byte alphanumeric characters and symbols ($-_). Specify from 1 to 32 characters. The dollar sign ($) can only be used as the last character of the name. The first character in the name must be an alphanumeric character or an underscore (_). The name is not case sensitive. - The name cannot contain only numbers. - You cannot use the following reserved keywords: adm, administrator, bin, chrony, daemon, dbus, ftp, games, halt, lp, mail, nfsnobody, nobody, nscd, nslcd, operator, polkitd, postfix, postgres, root, rpc, rpcuser, shutdown, sshd, sync, systemd-bus-proxy, systemd-network, tss, vauser - When the NAS authentication server is registered in this product, the user name registered in the NAS authentication server cannot be set.
Password	Required	Specify a password. You can use single-byte alphanumeric characters and symbols (!"#$&'()*+,-./ @[\]^_`{|}~:;<=>?). Specify from 8 to 32 characters. You must use at least three of the following four types of characters: uppercase letters, lowercase letters, numbers, and symbols.
User ID	Optional	Specify a number from 500 to 999 as the ID for the user to be created. If this setting is omitted, the system automatically assigns a number.
Primary group	Optional	Specify 1 primary group to which the local user belongs. If you do not specify, sharegroup$(451) is set automatically.
Secondary group	Optional	Specify secondary groups to which the local user belongs. You can specify up to 16 secondary groups. You cannot specify the same secondary group more than once. If you do not specify, no secondary groups are set.

See

You can also register a NAS access user with the CSG REST API. Refer to "NAS Access User" in the "Reference Guide" for how to register.

2.7.2 Settings When Accessing the NAS with the External Authentication User

When accessing the NAS with the external authentication user, perform the procedure in "2.7.2.1 NAS Authentication Server Settings".

2.7.2.1 NAS Authentication Server Settings

Setting Procedure

The procedure for registering a NAS authentication server in this product is described below.

- When setting up an SMB authentication server

  1. In CSG Web GUI, click [⚙] on the global pane.
  2. The **Settings** dialog box is displayed.
     Click **NAS access** > **NAS authentication server** on the left pane.
  3. The **NAS authentication server list** screen is displayed on the right pane.
     Click **Add** in **Action** on the right.
  4. The **Register authentication server** screen is displayed.
     Enter the required information, and then click **Done**.
  5. On the **NAS authentication server list** screen, confirm that the AD server you registered has appeared.
  6. Select a registered authentication server, and run **Test** in **Action** on the right. If the test fails, check whether the input items for the registered authentication server have been entered correctly.

Note

- You can only set one authentication server (AD server) to be used with SMB. If no server is set, authentication is performed based on the NAS Access User Settings.
- For operations with an AD server, be sure to set up a DNS server for domain name resolutions. Refer to "2.3 Setting Up Virtual Appliances" for details.
- For operations with an AD server, be sure to synchronize the clock between this product and the AD server. It is recommended that you perform automatic clock calibration via NTP. Refer to "2.3 Setting Up Virtual Appliances" or "2.5.1 Setting the System Clock" for details.
- For operations that use an AD server, specify a user that belongs to the "Domain Admins" group for the bind user.
- If an authentication server is registered, modified, or deleted, NAS access to the current shared folder is suspended. Confirm that there is no NAS access before performing an operation.
- When specifying the user name (the owner name) and the group name for setting a shared folder and accessing from a client, append the domain name to them.
- When performing a test of the authentication server or when accessing the NAS from a client, specify the username using one of the following formats:
  - **User logon name**(*username@domain*)
  - **User logon name** (pre-Windows 2000)(*workgroup\username*)

Input Items

- When setting up an SMB authentication server

Item	Required?	Description
IP address	Required	Specify the IP address of the AD authentication server.
Domain	Required	Specify the domain name.
Bind user	Required	Specify a bind user using one of the following formats: **User logon name**(*username@domain*) or **User logon name** (pre-Windows 2000)(*workgroup\username*). You can omit the *domain* and *workgroup*
Password	Required	Specify the bind user password for AD authentication.
Description	Optional	Enter a description

See

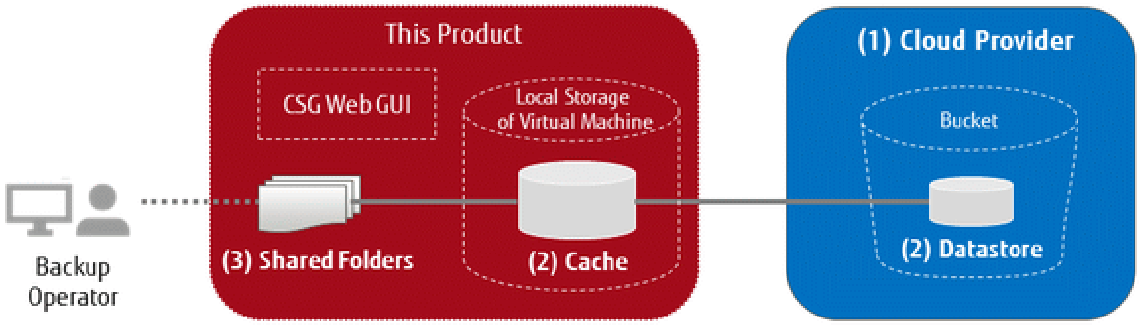
You can also register an authentication server with CSG REST API. Refer to "NAS Authentication Server" in the "Reference Guide" for details on the registration process.

Chapter 3 Configuring Operating Environments

To configure an operating environment, register the following components that constitute this product in order:

1. Cloud provider
2. Datastore and cache
3. Shared folders

Figure 3.1 Components that Constitute This Product



The CSG REST API that corresponds to the operation described in this chapter is as follows:

Table 3.1 Support for Chapter 3 CSG Web GUI and CSG REST API

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
3.1 Registering a Cloud Provider	Cloud Provider
3.2.2 Information Required for Registering a Datastore/Cache	Datastore
3.3 Registering a Shared Folder	Shared Folder

3.1 Registering a Cloud Provider

Register a cloud provider that is the storage destination for your data. You can register up to four cloud providers.

Point

Before performing this work, you must first obtain a contract with a cloud provider and create a bucket.

There are several types of buckets (Blob Storage) that can be created in Microsoft Azure/FUJITSU Cloud Service for Microsoft Azure. You must use the Block Blob type as the bucket for this product.

Note

In a system with multiple networks, you can specify a network you want to use for communicating with the cloud provider.
To specify a network, use the network name in CSG Web GUI and the network ID in CSG REST API.

3.1.1 Supported Cloud Providers

This product supports the following cloud providers:

- FUJITSU Cloud Service for OSS Object Storage
- Amazon S3
- Microsoft Azure Blob Storage / FUJITSU Cloud Service for Microsoft Azure Blob Storage

- NIFCLOUD Object Storage / FUJITSU Cloud Service for VMware NC Object Storage
- OpenStack Swift

3.1.2 Information Required for Registering a Cloud Provider

FUJITSU Cloud Service for OSS Object Storage

Item	Description
Provider name	A name used for identifying the cloud provider. You can use up to 32 alphanumeric characters and symbols (!@#$%^&*()_+-=[]{}|').
URI	A URI for connecting to the cloud provider. Specify the URI of the region where your bucket is located. [Example] For a bucket in Western Japan region 2, Specify "https://identity.jp-west-2.cloud.global.fujitsu.com/v3". For information about regions and URIs (endpoints), see the FUJITSU Cloud Service for OSS website.
Account	An account name for accessing FUJITSU Cloud Service for OSS Object Storage.
Password	A password for accessing FUJITSU Cloud Service for OSS Object Storage.
Domain ID	A domain ID for accessing FUJITSU Cloud Service for OSS Object Storage.
Project ID	A project ID for accessing FUJITSU Cloud Service for OSS Object Storage.
Network name or network ID (for systems with multiple networks)	A network name or network ID used for communicating with the cloud provider.

Amazon S3

Item	Description
Provider name	A name used for identifying the cloud provider. You can use up to 32 alphanumeric characters and symbols (!@#$%^&*()_+-=[]{}|').
URI	A URI for connecting to the cloud provider. Specify the URI of the region in which the bucket to be used exists. Example: - If the bucket is in the Asia Pacific (Tokyo) region, specify one of the following URIs: https://s3-ap-northeast-1.amazonaws.com/ or https://s3.ap-northeast-1.amazonaws.com/ - If the bucket is in the US East (Northern Virginia) region, specify the following URI: https://s3.us-east-1.amazonaws.com/ For information about the region and the URI (endpoint), check the Web site of Amazon Web Services.
Access key ID	A component of the security authentication information (access key) required for accessing Amazon S3. It is used as the user ID for accessing the cloud provider service.
Secret access key	A component of the security authentication information (access key) required for accessing Amazon S3. It is used as the password for accessing the cloud provider service.
Network name or network ID (for systems with multiple networks)	A network name or network ID used for communicating with the cloud provider.

Note

To specify a URI, use one of the following formats that include the region. (XXXXX: region)

- https://s3-XXXXX.amazonaws.com/
- https://s3.XXXXX.amazonaws.com/

Any other formats are unsupported.

[Examples of unsupported URIs]

- s3.dualstack.XXXXX.amazonaws.com
- s3.amazonaws.com
- s3-external-1.amazonaws.com

Microsoft Azure Blob Storage / FUJITSU Cloud Service for Microsoft Azure Blob Storage

Item	Description
Provider name	A name used for identifying the cloud provider. You can use up to 32 alphanumeric characters and symbols (!@#$%^&*()_+-=[]{}|').
URI	A URI for connecting to the cloud provider. Specify the URI of the storage account in which the bucket to be used exists. Example: - If the storage account name is "xyz", specify the following URIs: https://xyz.blob.core.windows.net/
Account	An account name for the Microsoft Azure storage account.
Access key	An access key for the Microsoft Azure storage account.
Network name or network ID (for systems with multiple networks)	A network name or network ID used for communicating with the cloud provider.

Note

In the description above, replace "Microsoft Azure" with "FUJITSU Cloud Service for Microsoft Azure" for the required information to register FUJITSU Cloud Service for Microsoft Azure Blob Storage.

NIFCLOUD Object Storage / FUJITSU Cloud Service for VMware NC Object Storage

Item	Description
Provider name	A name used for identifying the cloud provider. You can use up to 32 alphanumeric characters and symbols (!@#$%^&*()_+-=[]{}|').
URI	A URI for connecting to the cloud provider. Specify the URI of the region where your bucket is located. [Example] If a bucket exists in the East region East-2, specify "https://jp-east-2.os.cloud.nifty.com/". For information about regions and URIs (endpoints), see the NIFCLOUD Web site.
Access key ID	A component of the security authentication information (access key) required for accessing NIFCLOUD Object Storage. It is used as the user ID for accessing the cloud provider service.
Secret access key	A component of the security authentication information (access key) required for accessing NIFCLOUD Object Storage. It is used as the password for accessing the cloud provider service.

Item	Description
Network name or network ID (for systems with multiple networks)	A network name or network ID used for communicating with the cloud provider.

Note

In the description above, replace "NIFCLOUD" with "FUJITSU Cloud Service for VMware NC" for the required information to register FUJITSU Cloud Service for VMware NC Object Storage.

OpenStack Swift

Item	Description
Provider name	A name used for identifying the cloud provider. You can use up to 32 alphanumeric characters and symbols (!@#$%^&*()_+-=[]{}|').
URI	A URI for connecting to the cloud provider.
Account	An account name for accessing the cloud provider.
Password	A password for accessing the cloud provider.
Domain ID	A domain ID for accessing the cloud provider.
Project ID	A project ID for accessing the cloud provider.
Network name or network ID (for systems with multiple networks)	A network name or network ID used for communicating with the cloud provider.

Point

For accounts or access key IDs, grant permission to allow referencing and updating to the cloud storage.

For details about permissions, check the user's guide of each cloud provider.

3.1.3 Procedure for Registering a Cloud Provider

The procedure for registering a cloud provider in this product is as follows.

1. In CSG Web GUI, click **Cloud Provider** on the global pane.
2. The **Cloud Provider** screen is displayed.
   Click **Add** in **Action** on the right.
3. The **Register cloud provider** screen is displayed.
   Select a type of cloud service from the type pull-down menu and then click **Next**.
4. The **Enter connection settings** screen is displayed.
   Enter the required information and then click **Next**. Refer to "3.1.2 Information Required for Registering a Cloud Provider" for details about the information that must be entered.
5. The **Confirm** screen is displayed.
   Confirm that there is no problem with the registered content that is displayed and then click **Done**.
6. In the **Cloud Provider** screen, confirm that the cloud provider you registered is displayed.

See

You can also register your Cloud provider with the CSG REST API. See "Cloud Provider" in the "Reference guide" for how to register.

3.2 Registering a Datastore and Cache

When the datastore is created, the cache is created at the same time. The datastore and cache have a 1-to-1 correlation.
When you register a datastore, that datastore is created on a bucket.

3.2.1 Datastore/Cache Specifications

Refer to "A.2 Functional Specifications" for details about the datastore and cache specifications.

3.2.2 Information Required for Registering a Datastore/Cache

Information Required in the Basic Settings Screen

Item	Required?	Description
Provider name	Required	The name of the provider where the datastore is created.
Datastore name	Required	A name used for identifying the datastore. You can use up to 32 alphanumeric characters and symbols (!@#$%^&*()_+-=[]{}|').
Datastore capacity	Required	The capacity of the datastore. Set this item to a value of 100 GB or more, but less than or equal to the total of license capacity.
Cache capacity	Required	The capacity of the cache area. Set a value that is 10% of the datastore or larger (at least 20 GB) and less than or equal to the free space of a storage pool for cache that is connected to the virtual machine in which this product is running.

Information Required in the Bucket Selection Screen

Item	Required?	Description
Bucket name	Required	The name of the bucket where the datastore is created. The bucket information is automatically acquired according to the provider name selected in the basic settings screen and is displayed in the pull-down list. Select one of the buckets displayed in the list.

Information Required in the Advanced Settings Screen

Item	Required?	Description
Compression	Optional	Determines whether to compress the data when storing it in the datastore. The default setting is "Enable".
Datastore encryption	Optional	Determines whether to encrypt the data when storing it in the datastore. The default setting is "Disable".
Datastore encryption password	Optional	The password used to decrypt the encrypted data when **Datastore encryption** is set to "Enable".
Traffic control	Optional	Determines whether to set the maximum amount of data transfer when storing data in the datastore. The default is "Disable". If "Enable" is specified, the data transfer limit is set.

Item	Required?	Description
		You can specify 0 or 4-10240. The unit is Mbit/s. If 0 is specified, the setting of the upper bound value is disabled.

3.2.3 Procedure for Registering a Datastore and Cache

The procedure for registering a datastore and cache in this product is as follows.

1. In CSG Web GUI, click **Datastore** on the global pane.
2. The **Datastore** screen is displayed.
   Click **Add** in Action on the right.
3. The **Enter basic settings** screen is displayed.
   Refer to "Information Required in the Basic Settings Screen" in "3.2.2 Information Required for Registering a Datastore/Cache" to enter the required information and then click **Next**.
4. The **Select bucket** screen is displayed.
   Refer to "Information Required in the Bucket Selection Screen" in "3.2.2 Information Required for Registering a Datastore/Cache" to enter the required information and then click **Next**.
5. The **Enter advanced settings** screen is displayed.
   Refer to "Information Required in the Advanced Settings Screen" in "3.2.2 Information Required for Registering a Datastore/Cache" to enter the required information and then click **Next**.
6. The **Confirm** screen is displayed.
   Confirm that there is no problem with the registered content that is displayed and then click **Done**.
7. In the **Datastore** screen, confirm that the datastore you registered is displayed.

Note

If you create a new datastore, select a bucket that has no data.

If you select a bucket that has data, a datastore creation is successful, but registration of the shared folder fails.

See

You can also register data stores and caches with the CSG REST API. Refer to "Datastore" in the "Reference Guide" for how to register.

3.3 Registering a Shared Folder

Register a shared folder.
When you register a shared folder, that folder is created.

3.3.1 Shared Folder Specifications

Refer to "A.2 Functional Specifications" for details about the shared folder specifications.

3.3.2 Information Required for Registering a Shared Folder

Information Required in the Basic Settings Screen

Item	Required?	Description
Shared folder name	Required	The name used for identifying the shared folder. You can enter up to 76 characters (single-byte alphanumeric characters or double-byte characters with UTF-8

Item	Required?	Description
		encoding). The following characters cannot be used: - Single-byte space - The following symbols: \/:*?"<>|=,;[]%+ - ".snap", "global", "homes", "printers", "ipc$", "." (one dot), and ".." (two dots) (case insensitive) - Character strings starting with "@gmt" (case insensitive) - If omitted, the name "SF # nnn" is set. NNN indicates a three-digit number starting with 1. Change this based on the NAS client (e.g. backup software) or the operation.
Datastore name	Required	The name of the datastore where a shared folder is created. Select a datastore name from the pull-down list.
Owner	Optional	Information regarding the owner of the shared folder. If omitted, "root" is set. When specifying an AD server user, specify it using the "User logon name (pre-Windows 2000)" format.
Group	Optional	The name of the group to which the shared folder belongs. If omitted, "root" is set. When specifying an AD server group, specify it using the "Group name (pre-Windows 2000)" format. However, do not specify group names containing "@".
Protocol	Optional	Select either NFS or SMB as the protocol. The default selection is NFS.
Activation status	Optional	Select whether to enable the shared folder. If you only want to define the shared folder but not allow access, select "Disable". The default selection is "Enable". For the NFS protocol, if the activation status is changed to "Disable", a mount can be performed using the shared folder name, but the mounted folder cannot be used as a shared folder.

Information Required in the Advanced Settings Screen (When NFS Is Selected for the Protocol)

Item	Required?	Description
NFS allow hosts	Optional	Host information for which NFS access is granted. The following can be specified: 1. FQDN, IPv4 address 2. IPv4 Network (*1) 3. FQDN including "*" Up to 10 can be specified. To specify multiple values, separate each item with a comma. If more than one item is specified, the priority will differ according to the specified format and order. The highest priority is one and the lowest is three. For items with the same priority, the item described first (left side) has the higher priority. If omitted, all hosts are granted NFS access.
NFS root squash hosts	Optional	Hosts specified in NFS allow hosts and granted root access. The following can be specified: 1. FQDN, IPv4 address 2. IPv4 Network (*1) 3. FQDN including "*"

Item	Required?	Description
		Up to 10 can be specified. To specify multiple values, separate each item with a comma. If more than one item is specified, the priority applied will be different according to the specified format and the specified order. For the priority, the highest is one and the lowest is three. In the case of the same priority, the priority of the item described first (left side) is higher. If omitted, root access is not granted for any host. You must set the same string specified for the item in the NFS-allowed host. This is case sensitive. The following specifications are not allowed. - NFS-allowed Host: *. example.com - NFS Root Access-allowed Host: srv01.example.com

Information Required in the Advanced Settings Screen (When SMB Is Selected for the Protocol)

Item	Required?	Description
SMB encryption	Optional	Select whether to encrypt the communication. The default selection is "Disable".
Oplocks	Optional	Define whether to enable Oplocks (Windows function for improving network efficiency). The default selection is "Disable".
SMB allow hosts	Optional	Host information for which SMB access is granted. The following can be specified: - FQDN - IPv4 Address - IP network (* 1) - Domain name starting with "." - EXCEPT(*2) Up to 10 can be specified. To specify multiple values, separate each item with a comma. If multiple items are specified, the priority of the item described first (left side) is higher. If this setting is omitted, all hosts are granted SMB access. In addition, if the definition of this item and the SMB deny hosts overlap, the specification of this item takes priority(* 3).
SMB deny hosts	Optional	Host information for which SMB access is not granted. The following can be specified: - FQDN - IPv4 Address - IPv4 Network (*1) - Domain name starting with "." - EXCEPT(*2) Up to 10 can be specified. To specify multiple values, separate each item with a comma. If multiple items are specified, the priority of the item described first (left side) is higher.

Item	Required?	Description
		If this setting is omitted, all hosts are granted SMB access. In addition, if the definition of this item and the SMB allow hosts overlap, the SMB allow hosts specification takes priority(* 3).

Note

(*1) Specify an IPv4 network in any one of the following formats:

- CIDR notation (prefix notation)
  Example: 192.168.10.0/24

- Subnet notation
  Example: 192.168.10.0/255.255.255.0

(*2) Specify with the "<List 1> EXCEPT <list 2>" format. <List 1>,<list 2> is a space delimited list consisting of one or more of the following items.

- FQDN

- IPv4 Address

- IPv4 Network (*1)

- Domain name starting with "."

Of the items specified by <list 1>, allow or reject access from the items specified in <list 2>. There is no limit to the number of characters specified using this format.

Example	SMB allow hosts	SMB deny hosts	Access allowed
1	192.168.10.2	192.168.10.2	- 192.168.10.2 is accessible (deny hosts settings are ignored)
2	192.168.10.2	192.168.10.1/24	- Only 192.168.10.2 is accessible (deny hosts settings are ignored)
3	192.168.10.1/24	192.168.10.2	- Accessible from all 192.168.10.1/24 IP addresses (also accessible from 192.168.10.2) (deny hosts settings are ignored)
4	192.168.10.1/24 EXCEPT 192.168.10.2	(None)	- Accessible from all 192.168.10.1/24 IP addresses, except for 192.168.10.2
5	(None)	192.168.10.1/24 EXCEPT 192.168.10.2	- Not accessible from all 192.168.10.1/24 IP addresses except 192.168.10.2 - Accessible from all networks other than 192.168.10.2 and 192.168.10.1/24 non-network access

[Example]

- 192.168.10.1/24 EXCEPT 192.168.10.2

- 192.168.0.0/16 EXCEPT 192.168.0.0/24

- 192.168.0.0/16 EXCEPT 192.168.0.0/24 192.168.1.1

- .example1.com EXCEPT host1.example.com host2.example.com

- .example1.com .example2.com EXCEPT host1.example.com host3.example.com

This product does not support definitions of nested structures such as "a EXCEPT (b EXCEPT C)".

(*3) A search to determine if access is allowed is performed in order from SMB-allowed hosts to SMB-rejected hosts, and ends when an IP address match is found.

3.3.3 Procedure for Registering a Shared Folder

The procedure for registering shared folders in this product is as follows.

1. In CSG Web GUI, click **Shared Folder** on the global pane.
2. The **Shared folder** screen is displayed.
   In Action on the right, click **Add**.
3. The **Enter basic settings** screen is displayed.
   Refer to "Information Required in the Basic Settings Screen" in "Information Required for Registering a Shared Folder" to enter the required information and then click **Next**.
4. The **Enter advanced settings** screen is displayed.
   Refer to "Information Required in the Advanced Settings Screen (when NFS is selected for the protocol)" or "Information Required in the Advanced Settings Screen (when SMB is selected for the protocol)" in "Information Required for Registering a Shared Folder" to enter the required information and then click **Next**.
5. The **Confirm** screen is displayed.
   Confirm that there are no problems with the registered content displayed and then click **Done**.
6. In the **Shared folder** screen, confirm that the registered shared folder is displayed.

See

You can also register shared folders with the CSG REST API. Refer to "Shared Folder" in the "Reference Guide" for how to register.

3.3.4 Administrator Privilege Setting for Shared Folders

Depending on the backup software that is being used, you must be able to access shared folders with administrator privileges.
To access the shared folders in this product with administrator privileges, perform the following.

Administrator privilege setting (when NFS is selected for the protocol)

When creating a shared folder, set "NFS root squash hosts".
The root user of the set host can access with administrator privileges.

Administrator privilege setting (when SMB is selected for the protocol)

After creating a shared folder, log in to the console of this product using the administrator account (administrator) and execute the following command.

```
# csgadm smbconf set -share 'shared folder name' -key 'admin users' -value 'user name,@group name'
```

For "shared folder name", specify the name of the created shared folder.
Specify at least one NAS access user or NAS access group to set with administrator privileges in "user name, @group name". To specify multiple values, separate each item with a comma. When specifying NAS access groups, specify "@" at the beginning of the name.

The following is an example of assigning NAS access user "User A" and NAS access group "Group G" with administrator privileges for shared folder "SF#001".

```
# csgadm smbconf set -share 'SF#001' -key 'admin users' -value 'User A,@Group G'
```

As shown below, user names or group names can be enclosed in double quotes.

```
# csgadm smbconf set -share 'SF#001' -key 'admin users' -value '"User A","@Group G"'
```

If the setting is successful, the setting details are displayed as follows.

```
admin users = "User A","@Group G"
```

To check the current setting, execute the following command. The information that is displayed is the same as when the setting succeeded.

```
# csgadm smbconf show -share 'SF#001' -key 'admin users'
admin users = "User A","@Group G"
```

This command overwrites the existing settings. Therefore, to change or add a NAS access user or NAS access group based on the ones already set, check the existing settings and specify according to the displayed content. The following is an example of adding NAS access user "User B" when the above example is the current state.

```
# csgadm smbconf set -share 'SF#001' -key 'admin users' -value '"User A","@Group G","User B"'
```

To delete the settings, execute the following.

```
# csgadm smbconf unset -share 'SF#001' -key 'admin users'
```

Point

- For the NAS access usernames and NAS access group names that can be specified, refer to "Owner" and "Group" in "3.3.2 Information Required for Registering a Shared Folder".
- If the shared folder name, NAS access user name, or NAS access group name includes multibyte characters, log in to this product from a terminal that can use UTF-8 and execute this command.
- The specifiable character string length for "-value" is up to 2000 bytes.

Note

Before assigning the target shared folder as a network drive, execute this command. If the shared folder has already been assigned as a network drive, execute this command and then temporarily release the network drive assignment.

Chapter 4 Operation

This chapter explains how to operate this product.

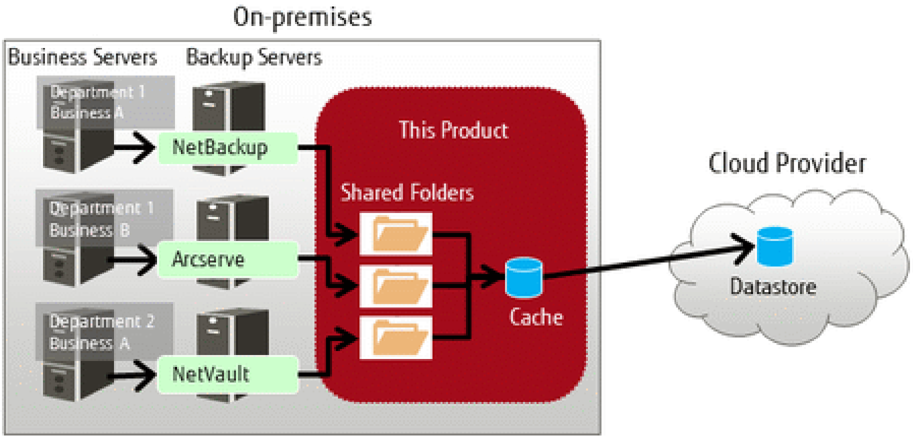
The CSG REST API that corresponds to the operation described in this chapter is as follows:

Table 4.1 Support for CSG Web GUI and CSG REST API in Chapter 4.

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
4.5 Performance Checking	Performance

4.1 Backing up to Cloud Provider

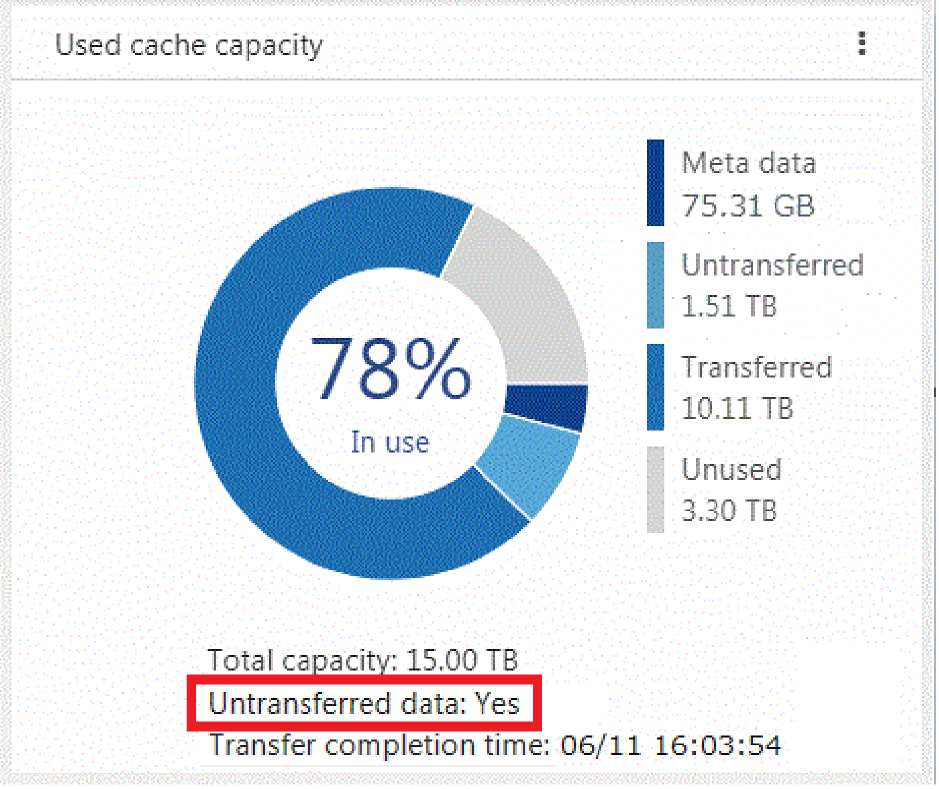
Figure 4.1 Flow of Data from Business Server to the Cloud Provider



The procedure for using backup software to back up business data to the cloud provider is as follows.

1. Connect the shared folders of this product to the backup server on the network.
2. Set a shared folder of this product as the backup data storage destination for the backup software.
   Refer to the manual of the backup software for details about how to configure this setting.
3. Use the backup software to perform a backup.
   Refer to the manual of the backup software for details about how to perform a backup.

4. Confirm in CSG Web GUI that the transfer to the cloud provider is completed.
   Check whether **Untransferred data** is **No** in the **Used cache capacity** panel that is in the dashboard of CSG Web GUI.



Used cache capacity

Total capacity: 15.00 TB

Untransferred data: Yes

Transfer completion time: 06/11 16:03:54

Information

If other backup processes that share the cache exist, "**Untransferred data**" remains "**Yes**" until all transfer processes are completed.

Note

For this product, "Writing Completed" is returned to the backup software when the data is written to cache.

Because of that, even if an abnormality occurs in communication with the cloud provider while writing, the writing is completed.

However, if the backup process is accompanied by a read and a communication abnormality with the cloud provider continues for three minutes or more, the process may terminate with an error.

If the backup process terminates with an error due to a communication abnormality, remove the cause of the error and execute a backup again.

4.2 Restoring Data

The procedure for using the backup software to restore business data that was backed up using the procedure in "4.1 Backing up to Cloud Provider" is as follows.

1. Connect the shared folders of this product to the backup server on the network.
2. Use the backup software to perform a restore.
   Refer to the manual of the backup software for details about how to perform a restore.
3. Refer to the recovery information of the backup software to confirm that the restore process has been completed normally.

Point

If the backup data is in this product cache, the data is restored from cache. If the backup data is not in this product cache, the backup data is loaded in the background from the cloud provider back into cache and then restored from cache.

4.3 Status Checking

If you configure the E-mail notification settings in "2.5.8 Monitoring Settings", E-mail notifications are sent to the administrator whenever an error occurs in this product.

When you receive an E-mail, check the status of this product on CSG Web GUI. In addition, if the state of the resource is "Warning" or "Error", check the details on the **Logs** panel of the CSG Web GUI dashboard.

4.3.1 Overall Status

The overall status is displayed on the global pane at the top of CSG Web GUI.

Figure 4.2 Overall Status

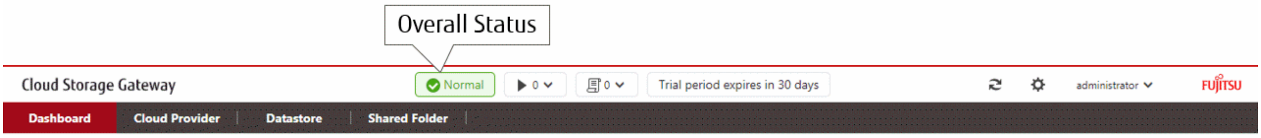


Table 4.2 Types and Meanings of Icons Displayed in Overall Status

Icon	Status	Meaning
✓ Normal	Normal state	All resources displayed on the **Status** panel are operating normally.
⚠ Warning	Immediate attention from the user is required	One or more resources on the **Status** panel require your attention.
✖ Error	An error has occurred	An error has occurred in one or more resources on the **Status** panel.

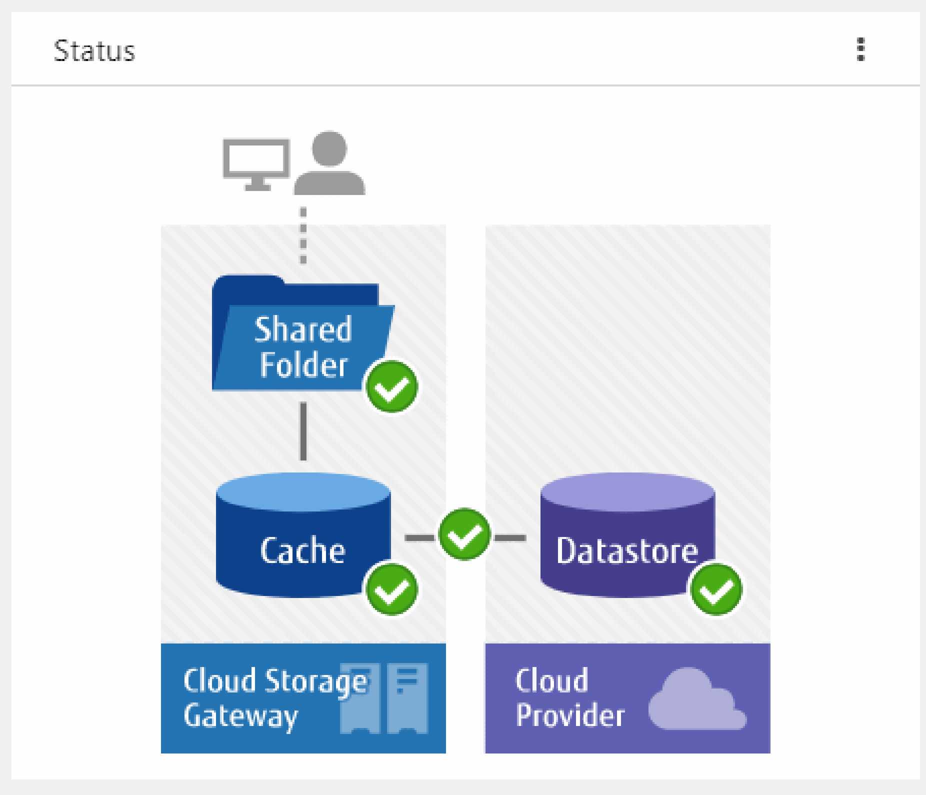
Point

If there is a mix of resources with "Warning" states and "Error" states, "Error" is displayed as the overall status.

4.3.2 Status

The status is displayed on the **Status** panel of the CSG Web GUI dashboard.

Figure 4.3 Example of Information Displayed on the Status Panel



The statuses of the shared folders, cache, datastores, and networks are displayed on this panel.

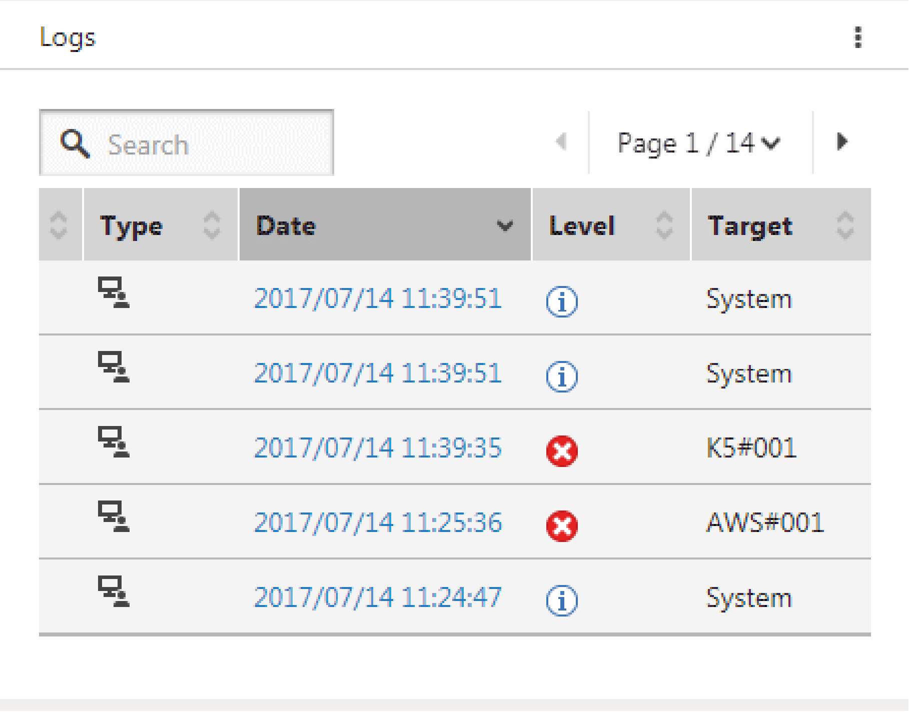
Table 4.3 Types and Meanings of Status Icons

Icon	Meaning
✓	Normal operation.
⚠	This product is operating, but your attention is required. For example, the used cache capacity is approaching the threshold value. Refer to "Appendix B Status Information" for details.
✖	An error has occurred and the operation has stopped. Check the **Logs** panel and take appropriate action.
?	Unable to acquire the status information.
ⓘ	A cloud provider, a datastore, or a shared folder has not been defined. For example, when the dashboard is in the initial state.

4.3.3 Logs

The log is displayed on the **Logs** panel of the CSG Web GUI dashboard.

Figure 4.4 Example Information Displayed on the Logs Panel



Type	Date	Level	Target
🖧	2017/07/14 11:39:51	ⓘ	System
🖧	2017/07/14 11:39:51	ⓘ	System
🖧	2017/07/14 11:39:35	✖	K5#001
🖧	2017/07/14 11:25:36	✖	AWS#001
🖧	2017/07/14 11:24:47	ⓘ	System

See

Refer to "6.1 Checking Logs" for details about the **Logs** panel.

Note

If a backup or restore fails for the following reasons, check the logs and the status from the dashboard. In case no errors are detected, check the status of the network and each server.

- A network error has occurred between the business server/backup server and this product.
- An error has occurred in the DHCP server, DNS server, or authentication server.

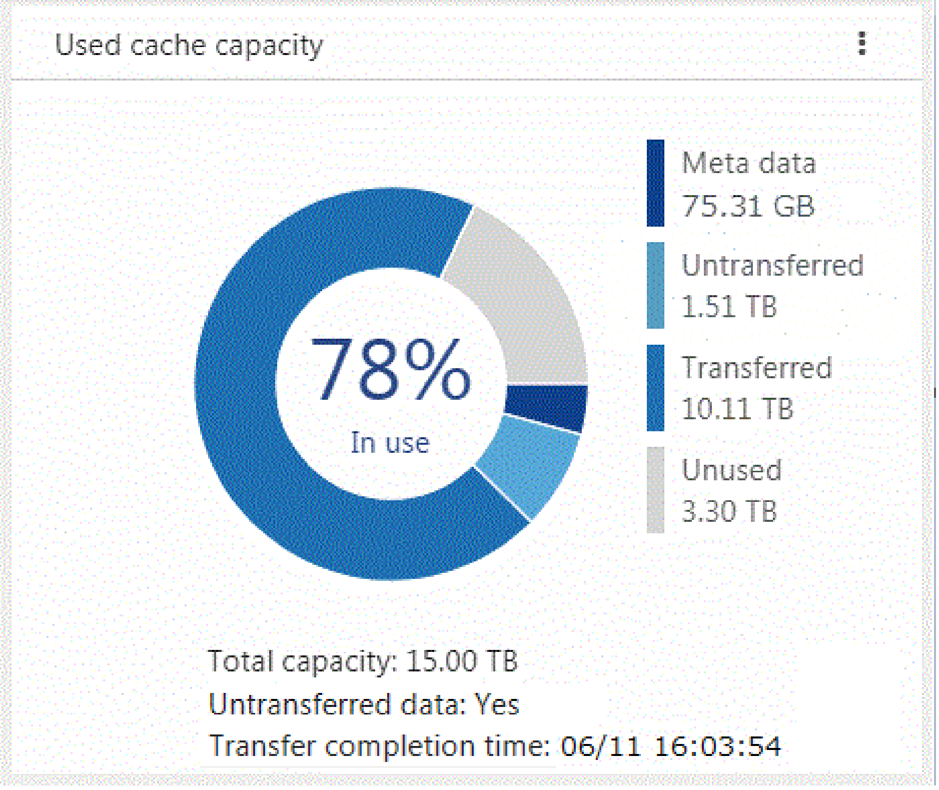
4.4 Capacity Checking

You can check the cache usage and the datastore usage on the CSG Web GUI dashboard.
Information regarding the usage capacity is updated every 60 seconds.

4.4.1 Used Cache Capacity

The cache usage is displayed on the **Used cache capacity** panel of the CSG Web GUI dashboard.

Figure 4.5 Example Information Displayed on the Used Cache Capacity Panel



Total capacity: 15.00 TB

Untransferred data: Yes

Transfer completion time: 06/11 16:03:54

Used cache capacity is displayed as a pie chart.

The values of "metadata", "untransferred", "transferred", "unused", and "total capacity" are displayed to the second decimal point.

When the datastore is not registered, a pie chart and legend are not displayed.

Table 4.4 Displayed Items

Item	Description
Meta data	Displays the **Meta data** capacity, which is data used for the management of file systems, deduplication/compression, and as a data storage destination used by the cloud provider.
Untransferred	Displays the total capacity of the data in the cache but not yet transferred to the cloud provider.
Transferred	Displays the total capacity of the data in the cache and transferred to the cloud provider.
Unused	Displays the capacity of areas that are reserved for cache but not yet used.
In use(%)	Displays the rate of the used amount (the total value for **Meta data**, **Untransferred**, and **Transferred**) among the areas that are reserved for the cache area as a percentage.
Total capacity	Displays the size of areas reserved for cache.
Untransferred data	The presence/absence of data that is untransferred to the cloud provider is indicated by Yes/No. When the datastore is not registered, a hyphen "-" is displayed.
Transfer completion time	Displays the time when "Untransferred data" changes to "No". The display format is a two-digit number that starts in order from the month, day, hour (24 hr-format), minute, and second. If data has never been transferred to the datastore, a "-" (hyphen) is displayed.

Note

Values displayed in Transferred differ from the values displayed in "**In use**" in the Used datastore capacity panel.

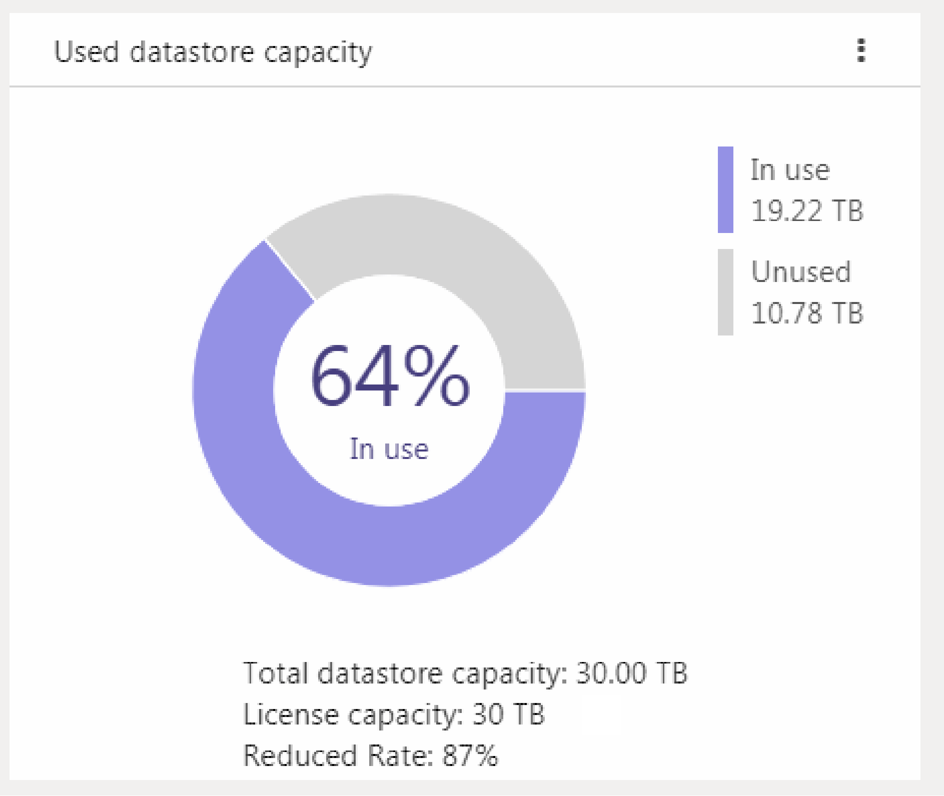
"**Transferred**" indicates the capacity of data that is kept as cache from all the data transferred to the cloud provider.

Data transfers to the cloud provider are performed sequentially, but if the file is created or deleted intermittently, or if data is written, the transfer completion time may not be updated because the untransferred data does not change to "None".

4.4.2 Used Datastore Capacity

The datastore usage is displayed on the **Used datastore capacity** panel of the CSG Web GUI dashboard.

Figure 4.6 Example Information Displayed on the Used Datastore Capacity Panel



Total datastore capacity: 30.00 TB
License capacity: 30 TB
Reduced Rate: 87%

Used datastore capacity is displayed as a pie chart.

The values of "In use", "Unused", and "Total datastore capacity" are displayed to the second decimal point.

When the datastore is not registered, a pie chart and legend are not displayed.

Table 4.5 Displayed Items

Item	Description
In use	Displays the datastore capacity currently in use.
Unused	Displays the area reserved as the datastore capacity but currently not in use.
In use(%)	Displays the rate of In use to Total datastore capacity as a percentage.
Total datastore capacity	Displays the total capacity reserved for the datastore. Displays the total value for **In use** and **Unused**.
License capacity	Displays the total capacity for licenses that are enabled.
Reduced rate(%)	Displays how much the current storage amount has been reduced by (after deduplication/compression) when compared to the total data capacity (before deduplication/compression) stored in this product. The reduced rate can be found according to the following formula. Reduced rate (%) = (1 - the amount of data after deduplication and compression / the amount of data before deduplication and compression) x 100.

Note

Values displayed in **In use** differ from the values displayed in **Transferred** in the **Used cache capacity** panel.

"**In use**" indicates the capacity of all the data that was transferred to the cloud provider including the data not kept in cache.

4.5 Performance Checking

You can check the cache I/O performance and the cloud transfer performance on the CSG Web GUI dashboard.
Information regarding performance is updated every 60 seconds.

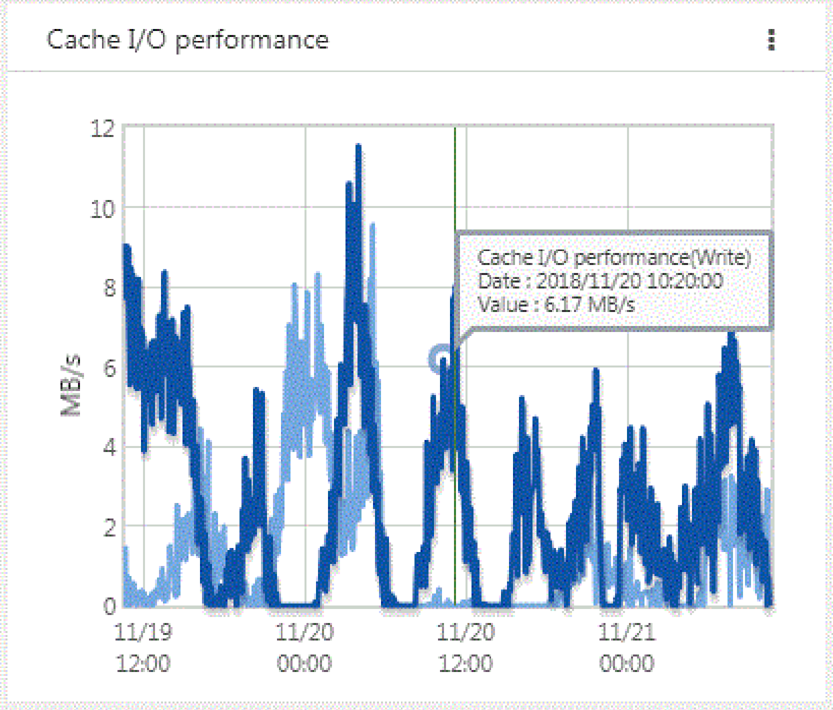
See

You can also check performance with CSG REST API. Refer to "Performance" in the "Reference Guide" for information on how to confirm.

4.5.1 Cache I/O Performance

Cache I/O performance is displayed on the **Cache I/O performance** panel of the CSG Web GUI dashboard.
You can check the cache I/O performance to determine if the cache performance is creating a bottleneck when transferring to the cloud provider.

Figure 4.7 Example Information Displayed on the Cache I/O Performance Panel



Cache I/O performance is displayed as a line graph in 5 minutes increments. The display range covers 2 days (fixed).
The light blue line graph indicates **Cache I/O performance(Read)**, and the dark blue line graph indicates **Cache I/O performance(Write)**.

If you focus any area on the graph, the date, time, and performance information is displayed for that tooltip on the graph.

Table 4.6 Displayed Items

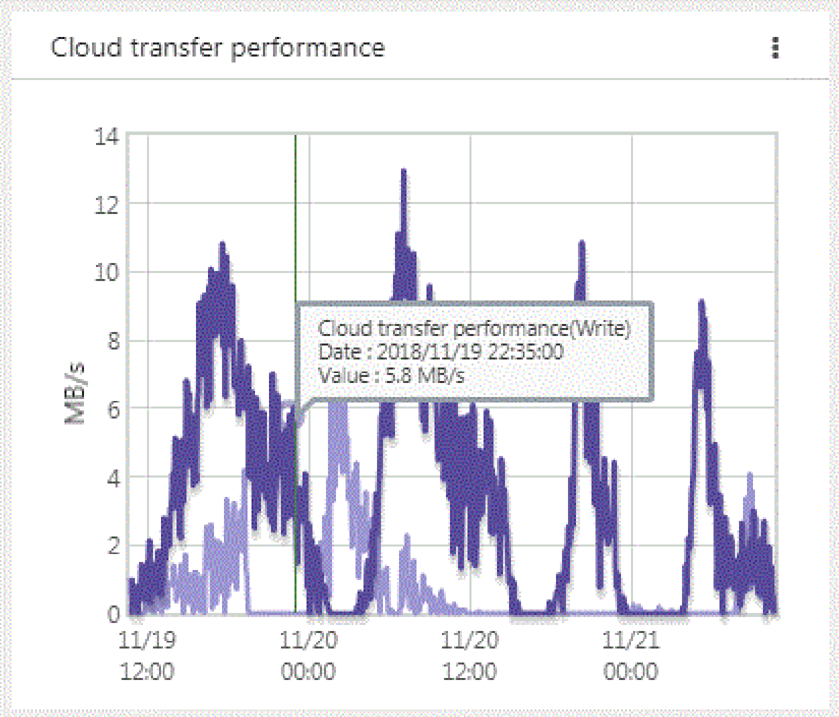
Item	Description
Vertical axis	Displays the performance value. The default range is 0 to 10 MB/s. If part of the performance data exceeds the default range, the range is automatically adjusted so that the entire performance data can be displayed.

Item	Description
Horizontal axis	Displays the date and time. The time zone of the virtual machine where this product is running is used to display the time. The display period is fixed to 2 days.
Light blue line graph	Displays the Read throughput to cache when reading from shared folders. The average value per 5 minutes is displayed by the graph.
Dark blue line graph	Displays the Write throughput to cache when writing to shared folders. The average value per 5 minutes is displayed by the graph.

4.5.2 Cloud Transfer Performance

Cloud transfer performance is displayed on the **Cloud transfer performance** panel of the CSG Web GUI dashboard.
You can check the cloud transfer performance to determine if there is sufficient network bandwidth and estimate the backup transfer performance.

Figure 4.8 Example Information Displayed on the Cloud Transfer Performance Panel


Cloud transfer performance
MB/s
14
12
10
8
6
4
2
0
11/19 12:00
11/20 00:00
11/20 12:00
11/21 00:00
Cloud transfer performance(Write)
Date : 2018/11/19 22:35:00
Value : 5.8 MB/s

The cloud transfer performance is displayed as a line graph in 5 minutes increments. The display covers 2 days (fixed).
The light purple line graph indicates **Cloud transfer performance(Read)** and the dark purple line graph indicates **Cloud transfer performance(Write)**.

If you focus any area on the graph, the date, time, and performance information is displayed for that tooltip on the graph.

Table 4.7 Displayed Items

Item	Description
Vertical axis	Displays the performance value. The default range is 0 to 10 MB/s. If part of the performance data exceeds the default range, the range is automatically adjusted so that the entire performance data can be displayed.
Horizontal axis	Displays the date and time. The time zone of the virtual machine where this product is running is used to display the time. The display period is fixed to 2 days.
Light purple line graph	Displays the transfer performance from a cloud provider (Read) during a restore as the Read throughput. The average value per 5 minutes is displayed by the graph.

Item	Description
Dark purple line graph	Displays the transfer performance from the cache to a cloud provider (Write) as the Write throughput. The average value per 5 minutes is displayed by the graph.

Chapter 5 Changing Operating Environments

This chapter describes how to change the operating environment for this product.

The CSG REST API that corresponds to the operation described in this chapter is as follows:

Table 5.1 Support for CSG Web GUI and CSG REST API in Chapter 5.

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
5.1 Changing Shared Folder Settings	Shared Folder
5.2 Changing Datastore Settings	Datastore
5.3 Changing Cloud Provider Settings	Cloud Provider

5.1 Changing Shared Folder Settings

If changes to a shared folder are required after starting an operation, use CSG Web GUI to change the settings of the shared folder.

5.1.1 Shared Folder Information that Can be Changed

The shared folder information that can be changed is shown below.
Refer to "Information Required to Register a Shared Folder" for descriptions related to the specification value of each item.

- If the protocol is NFS
    - Owner
    - Group
    - Activation status
    - NFS allow hosts
    - NFS root squash hosts
- If the protocol is SMB
    - Owner
    - Group
    - Activation status
    - SMB encryption
    - Oplocks
    - SMB allow hosts
    - SMB deny hosts

See

To allow the user access to the shared folders with administrator privileges, refer to "3.3.4 Administrator Privilege Setting for Shared Folders".

Note

If you delete the setting for the following items, "root" is set as the default for each item.

- Owner
- Group

If you change the following items, also specify the allowed hosts and denied hosts that are already set.

- NFS allow hosts
- NFS root squash hosts
- SMB allow hosts
- SMB deny hosts

5.1.2 Procedure for Changing Shared Folder Settings

The procedure for changing the shared folder settings is as follows.

1. Confirm that no users are accessing the target shared folder.
   If the shared folder is being accessed, either wait until the shared folder is no longer being accessed or stop the operation that is accessing the shared folder.
2. In CSG Web GUI, click **Shared Folder** on the global pane.
3. The **Shared folder** screen is displayed.
   Click the radio button for the target shared folder and then click **Modify** in the Action on the right.
4. The Enter basic settings screen is displayed.
   Change the information for the appropriate item and then click **Next**.
5. The **Enter advanced settings** screen is displayed.
   Change the information for the appropriate item and then click **Next**.
6. The **Confirm** screen is displayed.
   Confirm that there is no problem with the displayed content of the changes and then click **Done**.
7. In the **Shared folder** screen, confirm that the setting information of the shared folder has been changed correctly.

Point

- For the SMB protocol, even if the activation status is changed to "Disable", access is available until the client connection is disconnected.
  To prevent access, manually disconnect the network drive from the client.
- For the NFS protocol, if the activation status is changed to "Disable", a mount can be performed using the shared folder name, but the mounted folder cannot be used as a shared folder.

See

You can change the settings for shared folders using the CSG REST API. Refer to "Shared Folder" in the "Reference Guide" for information on how to change the settings.

5.2 Changing Datastore Settings

If changes to a datastore are required after starting an operation, use CSG Web GUI to change the settings of the datastore.

5.2.1 Datastore Information that Can be Changed

The datastore information that can be changed is as follows.
Refer to "3.2.2 Information Required for Registering a Datastore/Cache" for descriptions related to the specification value of each item.

- Datastore name
- Datastore capacity

- Cache capacity
- Compression
- Traffic Control

Note

- The data that is already registered is not compressed.
- If you are using a datastore that was created in a version earlier than 1.1.0, the minimum cache capacity equals 20% of the datastore capacity, and the maximum datastore capacity is five times the cache capacity.

5.2.2 Procedure for Changing Datastore Settings

The procedure for changing the datastore settings is described below.

1. In CSG Web GUI, click **Shared Folder** on the global pane.
2. The **"Shared folder"** screen is displayed.
   To change the following items, confirm that the activation state of all shared folders is "Disable" for the datastore.
   - Datastore name
   - Datastore capacity (only when shrinking)
   - Compression

   If a shared folder has an activation status of "Enable", use the procedure described in "5.1.2 Procedure for Changing Shared Folder Settings" to change the activation status to "Disable".
3. Click **Datastore** on the global pane.
4. The **Datastore** screen is displayed.
   Click the radio button for the target datastore and then click **Modify** in the Action on the right.
5. The Enter basic settings screen is displayed.
   Change the information for the appropriate item and then click **Next**.
6. The Enter advanced settings screen is displayed.
   Change the information for the appropriate item and then click **Next**.
7. The **Confirm** screen is displayed.
   Confirm that there is no problem with the displayed content of the changes and then click **Done**.
8. In the **Datastore** screen, confirm that the setting information for the datastore has been changed correctly.

See

You can also change the datastore settings using the CSG REST API. Refer to "Datastore" in the "Reference Guide" for information on how to change the settings.

5.3 Changing Cloud Provider Settings

If changes to a cloud provider are required after starting an operation, use CSG Web GUI to change the settings of the cloud provider.

5.3.1 Cloud Provider Information that Can be Changed

The cloud provider information that can be changed is shown below.
Refer to "3.1.2 Information Required for Registering a Cloud Provider" for descriptions related to the specification value of each item.

- Provider name

- URI
- Account/Access key ID
- Password/Secret access key/Access key
- Network name or network ID (for systems with multiple networks)

Point

- If you change the cloud provider account/access key ID or password/secret access key/access key, you must also change the cloud provider definition for this product.
- Some cloud providers set passwords with an expiration date. It is recommended that you periodically change your passwords.

Note

If this product is restarted before the cloud provider definition is changed, the csgdp01006 message is output and the shared folders become inaccessible.
If this occurs, change the cloud provider definition and restart this product.

5.3.2 Procedure for Changing Cloud Provider Settings

The procedure for changing the cloud provider settings is described below.

However, start from Step 3 for the following situations.

- When changing the account or access key ID only
- When changing the password, secret access key, or access key only
- When changing the account or access key ID as well as the password, secret access key, or access key

1. From CSG Web GUI, click **Shared Folder** on the global pane.
2. The **"Shared folder"** screen is displayed.
   Check whether the activation status of all the shared folders related to the target cloud provider is "Disable".
   If shared folders in which the activation status is "Enable" exist, change the activation status to "Disable" with the procedure described in "5.1.2 Procedure for Changing Shared Folder Settings".
3. Click Cloud provider on the global pane.
4. The "**Cloud provider**" screen is displayed.
   Click the radio button for the target cloud provider and then click **Modify** in the Action on the right.
5. The Enter connection settings screen is displayed.
   Change the information for the appropriate item and then click **Next**.
6. The **Confirm** screen is displayed.
   Confirm that there is no problem with the displayed content of the changes and then click **Done**.
7. In the **"Cloud provider"** screen, confirm that the setting information of the cloud provider has been changed correctly.

See

You can change your Cloud provider settings using the CSG REST API. Refer to "Cloud Provider" in the "Reference Guide" for information on how to change the settings.

5.4 Changing System Set Parameters

The following items that you configured in "2.3 Setting Up Virtual Appliances" can be changed.

- Change Administrator Password
- Change Password of Dedicated SFTP Account (sftpadmin)
- Configure DHCP
- Setting Hostname
- Configure Network
- Configure DNS
- Configure Domain
- Configure Keymap
- Configure NTP
- Configure time zone

The change procedure is as follows.

1. Log in to the console using the administrator account (administrator).
2. Execute csgsetup.
3. When the wizard starts, follow the instructions to change the settings.
4. A message is displayed asking you to restart the system. Select "OK" to restart the system.

Information

In the wizard, the existing setting values are displayed.

5.5 Adding Licenses

You can add licenses after an operation has already been started. Refer to "2.5.6 Registering a License" for details.

Chapter 6 Maintenance

This chapter describes how to perform maintenance for this product.

The CSG REST API that corresponds to the operation described in this chapter is as follows:

Table 6.1 Support for CSG Web GUI and CSG REST API in Chapter 6.

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
6.1 Checking Logs	Operation Log
	Event Log
6.2 Checking Performance Data	Performance
6.3 Troubleshooting	Troubleshooting Data Download
6.4 Restoring the Environment	Meta Data Recovery
	Shared Folder List (on Recovery)

6.1 Checking Logs

The logs of this product are displayed on the Logs panel in the CSG Web GUI dashboard.

6.1.1 Log List

The logs that are displayed on the Logs panel are shown below:

- Operation log
- Event log

Logs for 30 days (for the current day and 29 past days) are displayed on the Logs panel.

Table 6.2 Items Displayed on the Logs panel.

Displayed Item	Description
	The [●] icon is displayed for unconfirmed logs. Once the log is referenced, the icon is no longer displayed.
Type	For operation logs, the [🖧] icon is displayed. For event logs, the [☰] icon is displayed.
Date	For operation logs, the latest modification date and time is displayed. For event logs, the date and time the event occurred is displayed. Displayed in the following format: YYYY/MM/DD hh:mm:ss.
Level	For operation logs, the results of the operation are displayed. For event logs, the event level is displayed. - [ℹ]Information: Successful completion/Information event - [⚠]Warning: Timeout/Warning event - [✖]Error: Failure/Error event
Target	The cloud provider name or bucket name, or "System" is displayed.
User name	For operation logs, the username that performed the operation is displayed. For event logs, a hyphen "-" is always displayed.
Action	For operation logs, the action name is displayed. For event logs, a hyphen "-" is always displayed.
State	For operation logs, the execution state of the process is displayed.

Displayed Item	Description
	- Submit: Execution waiting - Start: Executing - Complete: Completed For event logs, a hyphen "-" is always displayed.
Result	For operation logs, the execution result of the process is displayed. - [✓]Success: Successful completion - [⚠]Warning: Timeout - [✖]Failed: Failed For event logs, a hyphen "-" is always displayed.
Detail	The details of the resource name for the target and settings in the screen are displayed. For event logs, a hyphen "-" is always displayed.
Message	A message is displayed.

See

You can also view the list of logs with the CSG REST API. Refer to "Operation Log" and "Event Log" in the "Reference Guide".

6.1.2 Changing the Content Displayed for Logs

You can change the content that is displayed on the **Logs** panel.

To change the current settings, click **Modify** in the common menu of the **Logs** panel and change the settings in the configuration dialog box that is displayed.

The items that can be configured in the configuration dialog box and the method for configuring them are shown in the following table.

Table 6.3 Configurable Items and Configuration Method

Item	Description	Method
Default sort	Field for specifying the column name that is sorted according to the initial configuration and the display order for the sorted information.	Select the column name to be sorted from the pull-down menu. Use the radio buttons to select whether the items are displayed in ascending(Asc) or descending(Desc) order.
Select column	Field for specifying display columns. At least one column name must be selected.	Use the check boxes to select the column names of the items to be displayed. If a check box is unselected, that column is not displayed.
Filter column	If you enter the display conditions for fields matching a column name in the information display area, only information that matches these conditions is displayed.	Select a column name and the conditions for that column, and then click **Add**. You can specify up to 30 conditions at the same time.
Record count	Field for specifying the number of lines that are displayed in a panel.	Configure by selecting from the pull-down menu. You can select 5, 10, or 50.

In the display content change screen for logs, you can change the status of all the logs to a checked status in a single step.

The procedure is as follows.

1. Click **Modify** in the common menu on the **Logs** panel.

2. The configuration dialog box is displayed.
   In the configuration dialog box, click **Mark all logs as confirmed**.

6.1.3 Detailed Log Display

You can display detailed information for specific logs.
The procedure is as follows.

1. In the Logs panel, click the date of the log to display the detailed information.
   The detailed information of the selected log is displayed in the detail dialog box.

Table 6.4 Items Displayed in the Operation Log

Displayed Item	Description
Update date	Date and time when the operation log was last updated. Displayed in the following format: YYYY/MM/DD hh:mm:ss.
Action	Operation name.
User name	**Name of the user performing the operation.**
Target	The cloud provider name or bucket name of the operation target or "System" is displayed. If there is no target, a hyphen "-" is displayed.
State	Execution state of the operation. **("Submit", "Start", or "Complete" is displayed.)**
Result	Process execution result. (Success: Successful completion, Warning: Warning (Timeout), Failed: Failed)
Detail	Parameters of the operation.
Message	Detail message for the operation.

Table 6.5
Items Displayed in the Event Log

Displayed Item	Description
Event level	Level of the event. ("Information", "Warning", or "Error" is displayed.)
Date	Date and time when the event occurred. Displayed in the following format: YYYY/MM/DD hh:mm:ss.
Target	The cloud provider name or bucket name of the event target or "System" is displayed. If there is no target, a hyphen "-" is displayed.
Message ID	Message ID for the event.
Message	Message for the event.

See

You can also view the log details using the CSG REST API. Refer to "Operation Log" and "Event Log" in the "Reference Guide".

6.1.4 Downloading Logs

The logs of this product can be downloaded using the CSG REST API.
For information on how to download the logs, refer to "Operation Log" in the "Reference Guide".

The logs that you can download are as follows. (The following logs are collectively referred to as "audit log" in the documentation of this product.)

- Operation logs

- Command operation logs using the console

The audit log file format is CSV and the encoding is UTF-8 (BOM).

Point

- The retention specifications of the audit log are as follows:
    - Operation log: a maximum of 50,000 items and a maximum of 32 days (current day plus the previous 31 days)
    - Command operation log using console: retains five generations of the CSV file per command (maximum 5MB per file)
- For the operation log, you can specify the period of the log to download.
- The download file is a compressed zip file. The audit log is extracted when the file is unzipped.

6.2 Checking Performance Data

The performance data of the product is displayed in the "Cache I/O performance" and "Cloud transfer performance" panels in the CSG Web GUI dashboard. For a description of the panel, refer to "4.5 Performance Checking".

6.2.1 List of Performance Data

The performance data of this product can be listed using the CSG REST API. The listed performance data is as follows:

- Cloud transfer Read throughput (MB/s)
- Cloud transfer Write throughput (MB/s)
- Cache I/O Read throughput (MB/s)
- Cache I/O Write throughput (MB/s)

Refer to "Performance" in the "Reference Guide" for information on how to view the list of performance data.

6.2.2 Download Performance Data

The performance data for this product can be downloaded using the CSG REST API. The performance data listed in "6.2.1 List of Performance Data" is downloadable.
For information on how to download performance data, refer to "Performance" in the "Reference Guide".
The file format for the performance data is CSV, and the encoding is UTF-8 (BOM).

Point

- You can specify how long the performance data will be downloaded in a range of up to 32 days (the same day and the previous 31 days).
- The download file is a zipped compressed file. The performance data is expanded when extracting it.

6.3 Troubleshooting

If a problem occurs in the system where this product is used, and a message instructing you to contact our customer support department is output to a log, use the following procedure to collect the troubleshooting data and contact our customer support department.

1. In CSG Web GUI, click [⚙] on the global pane.
2. The *Settings* dialog box is displayed.
   Click **Maintenance** > **Troubleshooting** on the left pane.
3. The "Download troubleshooting data" screen is displayed on the right pane.
   Click **Download**.

4. The "Download troubleshooting data" dialog box is displayed.
   Click **Download**.

5. The dialog box for specifying the location to save the troubleshooting data is displayed.
   Specify the location to save the troubleshooting data.

6. Confirm that the compressed file "csgsnap_date.zip" is saved to the location you specified in step 5.

Note

- After the download starts, other users are unable to operate this product for a short time.

- As time passes after a problem occurs, it becomes more likely that the troubleshooting data required to investigate the problem is lost. Therefore, collect the troubleshooting data immediately after a problem occurs.

- If CSG Web GUI cannot be used, use the following procedure to collect the troubleshooting data.

  a. Log in to the console using the administrator account (administrator).

  b. Collect the troubleshooting data by executing the following command. The collected troubleshooting data is output to "/Administrator/ftp/csgsnap.tgz".

  ```
  # csgsnap
  ```

  c. Download the collected troubleshooting data with SFTP.
     User: sftpadmin
     Password: The password set in "Change sftpadmin Password" of the Initial Setup Wizard.

See

It is also possible to collect survey materials with the CSG REST API. Refer to "Troubleshooting Data Download" in the "Reference Guide".

6.4 Restoring the Environment

If data in the on-premises environment is lost due to a hardware failure or disaster, you can use the data backed up to the cloud provider to restore the environment.

Note

If you restore the system with data that was backed up to the cloud provider using an earlier version of this product, the restored environment retains the characteristics of the earlier version described in "Appendix E Incompatibility Information".

- "E.1.2 Amount of Resources Used by Virtual Appliances"

- "E.1.3 Minimum Cache Capacity"

- "E.1.4 Status Change Triggers"

6.4.1 Restoration Procedure

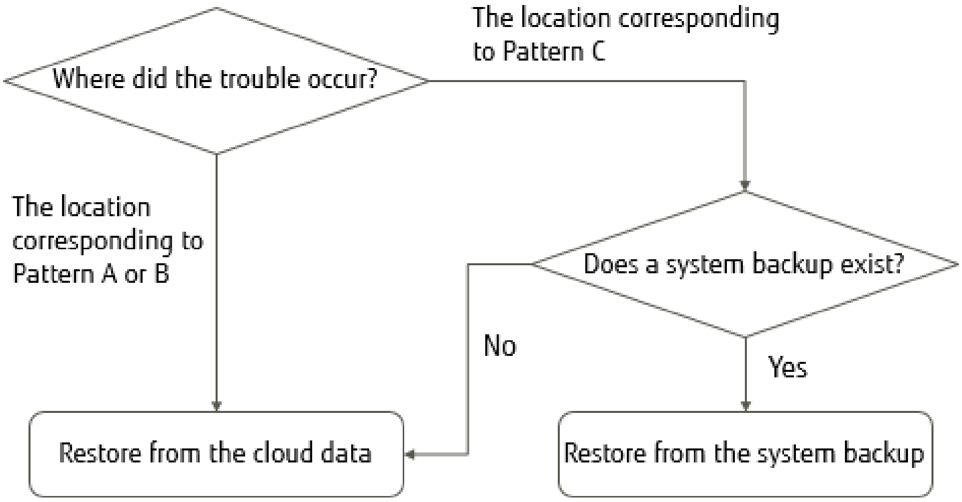
6.4.1.1 Overview of the Disk Restoration Procedure

Table 6.6 Areas where Disk Failure Occurs

Pattern	System Area	Data Area
A	Failure	Failure
B	Normal	Failure

Pattern	System Area	Data Area
C	Failure	Normal

Figure 6.1 Workflow for Restoration after Disk Failure


Where did the trouble occur?
The location corresponding to Pattern C
The location corresponding to Pattern A or B
Does a system backup exist?
No
Yes
Restore from the cloud data
Restore from the system backup

If a disk failure occurs, perform the restoration procedure described in "Figure 6.1 Workflow for Restoration after Disk Failure".

1. Check which pattern shown in "Table 6.6 Areas where Disk Failure Occurs" applies for the area where the disk failure occurred.

   - If Pattern A or Pattern B applies
     Use the data that is backed up to the cloud provider to restore the entire system.
     Refer to "6.4.1.2 Restoring from Cloud Provider Data" for details about the restoration procedure.

   - If Pattern C applies
     The restoration procedure varies depending on whether a system backup exists.

     - If there is no system backup
       Use the data that is backed up to the cloud provider to restore the entire system.
       Refer to "6.4.1.2 Restoring from Cloud Provider Data" for details about the restoration procedure.

     - If there is a system backup
       Perform a system restore to restore the system while retaining the data area.
       Refer to "6.4.1.3 Restoring from a System Backup" for details about the restoration procedure.

     Note

     - When backing up the system, make sure that the network MAC address assigned to the virtual appliance is carried over.

     - If you make any structural changes, such as adding or removing a shared folder, after you have backed up the system, restore the entire system according to the procedure described in "6.4.1.2 Restoring from Cloud Provider Data".

6.4.1.2 Restoring from Cloud Provider Data

The procedure for restoring the system using data backed up to the cloud provider is described below.

1. Replace the failed physical disk with one that operates normally.

2. From the server virtualization software, delete the virtual machine that is on the physical disk where the failure occurred, and in which this product was running.

Information

If Pattern B in "Table 6.6 Areas where Disk Failure Occurs" applies for the area where the disk failure occurred, this step also deletes the virtual disk from the system area that resides on the normal physical disk.

3. Deploy the virtual appliance of this product on the server virtualization software.
   Refer to "2.2 Deploying Virtual Appliances" for details about how to deploy a virtual appliance.

4. Configure the virtual appliance settings for this product.
   Perform the work described in the sections from "2.3 Setting Up Virtual Appliances" to "2.7 Setting NAS Access Users".

5. Register a cloud provider.
   Refer to "3.1 Registering a Cloud Provider" for details about how to register a cloud provider.

6. Create a datastore on the cloud provider that you registered in step 5.
   Refer to "3.2 Registering a Datastore and Cache" for details about how to create a datastore.

Note

- Enter the same content as before the failure occurred for the item.
  In particular, if the content of the following items differ from the content before the failure occurred, the restoration process will fail.

  - "**Cache capacity**" and "**Provider name**", which are required in the basic settings screen

  - "**Bucket name**", which is required in the bucket selection screen

  - "**Datastore encryption**" and "**Datastore encryption password**", which are required in the advanced settings screen

- If the cache capacity is smaller than before the failure occurred, the restoration process will fail due to insufficient cache capacity. Delete the datastore and then start the procedure from step 6.
  If a bucket that has no data is selected, the restoration process cannot be performed even by performing step 7. Delete the datastore and then start the procedure from step 5 or step 6.
  For the selected bucket, if the settings for "Datastore encryption" and "Datastore encryption password" do not match, step 6 will fail. Perform the procedure again from step 6.

- Specify the bucket that was used before the failure occurred.
  If the registration of the datastore and cache is performed, the csgdp03002 message is output. This message indicates that the specified bucket is already in use.
  When restoring from cloud provider data, this message is output because a bucket that has data is specified. Ignore this message and continue the restoration procedure.
  If a bucket that has no data is specified, this message is not output. Check whether the bucket specification is correct.

7. Use the following procedure to perform meta data recovery for the datastore that was created in step 6. When you perform meta data recovery, the meta data that is in the cloud provider is restored to the cache.

   a. Execute the following CSG REST API to perform meta data recovery for the datastore. You can check the ID in the **Datastore** screen of CSG Web GUI.

   ```
   POST /v1/datastores/{id}/metadata/recovery
   ```

   b. Execute the following CSG REST API periodically as you wait for meta data recovery for the datastore to complete.

   ```
   GET /v1/datastores/{id}/metadata/recovery
   ```

   You can check the progress of the meta data recovery with the status key for CSG REST API response.

   - While the process is in progress
     The status key is "Active".

   - When this product is accessible with the read-only mode
     The status key is "Active (Readable)".
     Registering the shared folders allows data to be read.

Use the event log to check the last time when the untransferred data became "None".
Use the checked time when performing a restoration with the backup software.

- When the process is completed
  The status key is "N/A".
  Use the event log to check that the meta data recovery is completed.

- If a process error occurs
  The status key is "Error".
  You can determine the cause of the process error from the event log. Reboot the system after identifying and removing the cause of the error.
  A reboot will automatically restart the meta data recovery.
  If you restart the meta data recovery but it still terminates with an error, you must re-execute the procedure from step 2.

See

The event log for this product appears in the "Log" pane of the CSG Web GUI dashboard.

Note

In the read-only mode state, creating, deleting, and writing files to the shared folders cause errors.

8. Use the following procedure to allow NAS access for the shared folders on the datastore.

   a. Execute the following CSG REST API to check the names of the shared folders in the datastore.
      The datastore_id parameter can be checked from the **Datastore** screen of CSG Web GUI.

```
GET /v1/datastore_folders
```

   b. Specify a shared folder name that you checked in step a to register that shared folder.
      Refer to "3.3 Registering a Shared Folder" for details about how to register a shared folder.

Point

Perform this procedure for each shared folder in the datastore.

Note

For configurable items (shared folder name, owner, and group) of the shared folder, the values must be the same as before the failure.
During the read-only mode, if you enter content that differs from before the failure, registration of the shared folder terminates with an error.
If you enter content that differs from before the failure after the recovery is complete, the content you entered will be set to the shared folder. (The shared folder is registered based on the information that you entered.)

See

Refer to the "Reference Guide" for details about the "CSG REST API" mentioned in step 7 and step 8.

Fast recovery function

Depending on the amount of data, the recovery may take some time before being complete. This product provides a fast recovery function that can perform read only in advance even if a recovery process is running. This allows the restore to start before the meta data recovery is completed.

In meta data recoveries, the execution state transitions in the order of "Processing (active)" -> "Read-only mode(Active (Readable))" -> "Completed (N/A)" according to the progress of the process. The recovered data can be referenced in the "Read-only mode(Active (Readable))" and subsequent states, and can be updated in the "Completed (N/A)" state.

Table 6.7 Metadata recovery status and access type

Status (Status key display)	Type of Access	
	Reference	Update
Active	NG	NG
Active(Readable)	OK	NG
N/A	OK	OK

The state of the meta data recovery transitions from top to bottom in this table.

Note

- Because the Active (Readable) state is a state in which only a restore for meta data that are referenced is complete, a data transfer from the cloud provider is always generated when the file is first accessed. This may require more processing time than an access after the restore is complete.
- If you are restoring from the Active (Readable) state using a backup software that requires writing, you will need to copy and restore the data to a temporary area of the local storage.
- In the Active (Readable) state, mounting can be performed in the read-write mode, but creating and writing files will cause errors.
- In the Active or Active (Readable) state, the status of the datastore on the GUI is Normal.

6.4.1.3 Restoring from a System Backup

The procedure for using a system backup to restore the system is described below.

1. Replace the failed physical disk with one that operates normally.
2. Restore the system backup.
   Refer to the manual of the backup software for details about how to perform a restore.

   Note

   Only the system area gets restored. For the data area, use an existing disk that functions normally.

3. Use the following procedure to activate the datastore function.

   a. Log in to the console using the administrator account (administrator).

   b. Execute the following command to activate the datastore function. datastoreID, which is specified as the command operand, is the datastore ID. You can check the datastore ID in the Datastore screen of CSG Web GUI (by selecting "ID" in "Display settings").

   ```
   # csgadm datastore activate datastoreID
   ```

   Information

   The reason why the datastore function becomes disabled after restoring a system backup is to prevent corruption of data in the bucket in case a restore is performed accidentally while the backup source system is running. In case the datastore function has become disabled, NAS access is not available.

4. Execute the following command to restart the system.

   ```
   # csgadm power restart
   ```

If, when restoring from a system backup, the network MAC address that you assigned to the virtual appliance is not carried over, use the following procedure to reset the IP address.

Note

Because communication with the cloud provider is disabled until the IP address is reset, the system takes approximately ten minutes or longer to restart.

- For single network configurations
  Run the Configuration Wizard to change the IP address in "Network settings".
  Refer to "6.7.1 For a Single Network Configuration" for how to set the IP address.
  The system restarts at the end of the work procedure, so please restart the system at this time. If you did not choose when asked, restart the system using the following command.

  ```
  # csgadm power restart
  ```

- For multi-network configurations

  1. Set the IP address of the first network set in the Configuration Wizard.
     For the configuration method, refer to "6.7.1 For a Single Network Configuration".
     Perform the following procedure from the first network.

  2. Delete the second and all subsequent networks.
     The CSG REST API is used to remove the second and all subsequent networks.
     By default, the network that is being used to communicate with the cloud provider cannot be deleted. Delete it by specifying the option that forcibly deletes networks.

  3. Re-register all networks from the second one.
     Prevent the network ID that is used for communication with the cloud provider from being changed.
     Use the CSG REST API to check the network ID specified for the cloud provider.

     - If there is a cloud provider that uses the network whose ID is "1", make sure to register a network that can communicate with the relevant cloud provider first.

     - If there is a cloud provider that uses the network whose ID is "2", make sure to register a network that can communicate with the relevant cloud provider next.

     If only networks whose ID is "0" are used to communicate with the cloud provider, networks can be registered in any order.
     Refer to "2.5.7 Configuring Multi-network Configurations" for registering the network.

  4. Restart the system.
     Log in to the console using the administrator account (administrator) and execute the following command to restart the system.

     ```
     # csgadm power restart
     ```

See

You can also recover the environment using the CSG REST API. Refer to "Meta Data Recovery" and "Shared Folder List (on Recovery)" in the "Reference Guide".

6.5 Updating Software

This section describes the procedure for upgrading and applying update patches to this product.
Update patches are available on the support desk website or in similar locations.
The archive file for the upgrade are included on the DVD of the new product you want to upgrade.
In this document, update patches and archive file for the upgrade are collectively referred to as "update module."

Note

If you continue using any datastores you created with an earlier version of this product after the upgrade, the environment retains the characteristics of the earlier version for the following items described in "Appendix E Incompatibility Information".

- "E.1.2 Amount of Resources Used by Virtual Appliances"
- "E.1.3 Minimum Cache Capacity"
- "E.1.4 Status Change Triggers"

6.5.1 Software Update Procedure

The procedure for updating the software of this product is described below.

1. Preparation
2. Stopping operation
3. Creating a snapshot
4. Updating software
5. Deleting the snapshot
6. Restarting operation

Point

Creating a snapshot is optional. However, create a snapshot to revert the system back to the previous environment in case the software update is canceled or the software update fails.

6.5.1.1 Preparation

Follow the steps described below before upgrading the previous 1.1 version of this product.

- Check the cloud provider URI.
  If you are using Amazon S3 as your cloud provider, confirm that the URI format matches the one described in "3.1.2 Information Required for Registering a Cloud Provider." If the format is different, change the URI to the correct format.
  Refer to "5.3 Changing Cloud Provider Settings" for details on how to change the cloud provider URI.

- Check the NAS access user for local authentication.
  If the name of the NAS access user for local authentication is set to "sftpadmin," change the name. To change the name, delete the corresponding user first, and then create another one under a new name. Next, change the owner of the shared folder to the NAS access user under the new name.
  Refer to "2.7.1 Settings When Accessing the NAS with the Local Authentication User" for details on how to change the name of the NAS access user. Refer to "5.1 Changing Shared Folder Settings" for details on how to change the owner of the shared folder.

- Check the shared folder settings
  If the following items of the shared folder are specified with spaces using CSG REST API, delete the settings. Refer to "5.1.2 Procedure for Changing Shared Folder Settings" to delete the shared folder settings.

  - NFS allow hosts (nfs_allow_hosts)
  - NFS root squash hosts (nfs_no_root_squash_hosts)
  - SMB allow hosts (smb_allow_hosts)
  - SMB deny hosts (smb_deny_hosts)

6.5.1.2 Stopping Operation

Follow the procedure described below to stop operation.

1. Make sure that the shared folder is not being accessed. If it is being accessed, wait until the access is completed or stop the operation that is accessing it.

2. In the **Used cache capacity** panel of CSG Web GUI, check that Untransferred data is indicating **No**. If it is indicating **Yes**, wait until it changes to **No**. You can estimate the completion time of the data transfer as follows:

   a. Calculate the average cloud transfer performance (MB/s) from the performance data in the **Cloud transfer performance** panel of CSG Web GUI.

   b. Check the **Untransferred** value (GB) in the **Used cache capacity** panel of CSG Web GUI.

   c. Estimate the transfer completion time using the following formula with the values obtained above in a and b.
   Estimated transfer completion time (s) = (*amount of untransferred data* + 1) x 1024 / *average cloud transfer performance*

3. Log out of CSG Web GUI, and close the web browser.

4. Stop the virtual machine of this product.

   - For environments other than Microsoft Azure
     Use the administrator account (administrator) to log in to the console of this product, and stop the virtual machine with the following command.

     ```
     # csgadm power stop
     ```

   - For Microsoft Azure environments
     Go to the **Virtual Machines** service on the Azure portal, select the virtual machine of this product, and click **Stop**.

Note

The virtual machine of this product may be restarted during the software update procedure. However, do not access the shared folder until the update procedure is completed. It is recommended that you disable the shared folder before stopping this product. Refer to "5.1 Changing Shared Folder Settings" for details on how to change the settings of the shared folder.

6.5.1.3 Creating a Snapshot

Refer to "D.1 Creating a Snapshot" for details on how to create a snapshot.

6.5.1.4 Updating Software

Follow the procedure described below to update the software.

1. Start the virtual machine of this product.

   Note

   Do not access the shared folder after you start the virtual machine.

2. Log in to this product via SFTP, and transfer the update module to this product.
   Log in as "sftpadmin" via SFTP. Transfer the module to the following directory.

   ```
   /Administrator/ftp/
   ```

   Point

   When updating an unpatched version (V1.1.0) of this product, log in using "administrator" and transfer with FTP.

3. Use the administrator account (administrator) to log in to the console, and update the software.
   In the example below, the file name of the update module is CSG120UP.tgz.
   Change the file name according to the update module you want to use.

   ```
   # csgadm system patch-add -file /Administrator/ftp/CSG120UP.tgz
   ```

4. Stop the virtual machine of this product.

   - For environments other than Microsoft Azure
     Use the administrator account (administrator) to log in to the console of this product, and stop the virtual machine with the following command.

     ```
     # csgadm power stop
     ```

   - For Microsoft Azure environments
     Go to the **Virtual Machines** service on the Azure portal, select the virtual machine of this product, and click **Stop**.

Note

- If step 3 fails, remove the cause of the failure, use the snapshot to restore the system, and then re-perform the procedure described in "6.5.1.4 Updating Software" Refer to "D.2 Snapshot Restoration for details on how to restore the system with a snapshot.

- Follow the message may be output to the console during the operation of updating software. Ignore this message and do not have to take any action.

```
blk_update_request: I/O error, dev fd0, sector0
```

6.5.1.5 Deleting the Snapshot

Delete the snapshot you created using the procedure described in "6.5.1.3 Creating a Snapshot" and apply the software updates to the virtual machine of this product.
Refer to "D.3 Deleting a Snapshot" for details on how to delete the snapshot.

6.5.1.6 Restarting Operation

Start the virtual machine of this product to restart operation.
If you disabled the shared folder, enable it now.
If an unpatched version (V1.1.0) of this product is updated, run the Configuration Wizard and set a password for the SFTP account to use SFTP for file transfers. In addition, if you will only be using SFTP for file transfers and will not be using FTP from this point forward, run the following command to disable the FTP function in this product. Use the administrator account (administrator) to log in to the console and run the command.

```
# csgadm system ftp-disable
```

Log in to this product via SFTP and then delete the update module that is transferred to this product in "6.5.1.4 Updating Software". If an unpatched version (V1.1.0) of this product is updated and the above command is not executed, deletions can be performed with FTP.

Note

In order to use CSG Web GUI in the same web browser as before the software update, be sure to clear the web browser cache first. If you do not clear the cache, CSG Web GUI may not be displayed correctly.

6.5.2 Procedure to Roll Back to the Previous Environment after Terminating the Software Update Process

This section describes the procedure to roll back to the previous environment when the software update process is terminated due to unforeseen circumstances.
Follow the procedure described below to roll back to the previous environment.

- For KVM environments
  Follow the procedure described in "D.3.2 Deleting Snapshots in KVM Environments" to delete the snapshot.

  Note

  Do not perform step 3 described in "D.3.2 Deleting Snapshots in KVM Environments" since that is the procedure for applying updates.

- For other environments
  Follow the steps below according to the environment.

  1. Follow the procedure described in "D.2 Snapshot Restoration" to restore the system with a snapshot.

  2. Follow the procedure described in "D.3 Deleting a Snapshot" to delete the snapshot.

6.6 Stopping and Rebooting the System

The procedures for stopping and rebooting this product are described below.

6.6.1 How to Stop the System

Use the following procedure to stop this product.

1. Start CSG Web GUI.

2. Refer to the **Logs** panel on the CSG Web GUI and confirm that no processes are currently in progress.

3. Stop CSG Web GUI.

4. From the console, log in to the virtual machine as the administrative user in which this product is running.

5. Execute the following command.

```
# csgadm power stop
```

6.6.2 How to Reboot the System

Use the following procedure to restart this product.

1. Start CSG Web GUI.

2. Refer to the **Logs** panel on the CSG Web GUI and confirm that no processes are currently in progress.

3. Stop CSG Web GUI.

4. From the console, log in to the virtual machine as the administrative user in which this product is running.

5. Execute the following command.

```
# csgadm power restart
```

6.7 Changing the IP Address of This Product

The procedures for changing the IP address of the virtual appliance where this product is running are described below.

6.7.1 For a Single Network Configuration

1. Stop access to the shared folder.
   If a shared folder has been mounted from a business server or a backup server, unmount it. If you have settings that correspond to the mount, remove them.

2. Disable all the shared folders that are enabled.
   For the operation procedure, refer to "5.1 Changing Shared Folder Settings".

3. 3. Run the Configuration Wizard to change the IP address in "Network settings".
   For the operation procedure, refer to "2.3 Setting Up Virtual Appliances". The system requests a restart at the end of the operation procedure, so restart the system. If you did not choose to restart the system when requested, use the following command to restart the system.

   ```
   # csgadm power restart
   ```

4. Enable all the shared folders.
   For the operation procedure, refer to "5.1 Changing Shared Folder Settings".

5. 5. Resume access to the shared folder.
   Mount the shared folder from the business server or the backup server or configure settings that correspond to the mount.

6.7.2 For Multi-network Configurations

The procedure for changing the IP address of the first network set in the Configuration Wizard is the same as "6.7.1 For a Single Network Configuration".

When changing the IP address of the second and subsequent networks set in CSG REST API:

Perform the operation from a network different from the one you want to change.

- To change the network that you are using to access shared folders

  1. 1Stop access to the shared folder.
     If a shared folder is mounted from a business server or a backup server, unmount it. If you have settings that correspond to the mount, remove them.

  2. Disable all the shared folders that are enabled.
     For the operation procedure, refer to "5.1 Changing Shared Folder Settings".

  3. Change the IP address.
     For the operation procedure, refer to "6.7.2 For Multi-network Configurations".

  4. Enable all the shared folders.
     For the operation procedure, refer to ""5.1 Changing Shared Folder Settings"".

  5. Resume access to the shared folder.
     Mount the shared folder from the business server or the backup server or configure settings that correspond to the mount.

- To change a network that is not used to access shared folders

  1. Change the IP address.
     For the operation procedure, refer to "6.7.2 For Multi-network Configurations".

6.8 Expanding the Cache Area by Adding Virtual Disks

You can expand the cache area dynamically by adding virtual disks to the virtual appliance.

Note

The following procedure uses VMware vSphere, or Hyper-V as an example.
For KVM, change "/dev/sdX" to "/dev/vdX."
For Amazon EC2, change "/dev/sdX" to "/dev/xvdX."
In Microsoft Azure, "/dev/sdaX" and "/dev/sdbX" represent the virtual disks for the system area. The virtual disks for any additional cache area start from "/dev/sdd."

1. 1. Add virtual disks to the virtual appliance.
   You can add up to 31 virtual disks.
   For virtual disk requirements, refer to "A.1 Virtual Appliance Specifications".
   For more information about how to add virtual disks, refer to the documentation for your server virtualization software and cloud services.

2. Expand the cache storage pool.

   a. Log in to the console of this product using the Administrator account (administrator).

   b. Verify that the added virtual disk is recognized by executing the following command.
      The following example shows how to add a 200GB virtual disk.
      The disk is recognized as "/dev/sdc".

```
# csgadm storagepool diskscan
  /dev/sda1 [     953.00 MiB]
  /dev/sda2 [      27.94 GiB]
  /dev/sda3 [      27.94 GiB]
  /dev/sda5 [      27.94 GiB]
  /dev/sda6 [       3.72 GiB]
  /dev/sdb  [     100.00 GiB] LVM physical volume
  /dev/sdc  [     200.00 GiB]
  1 disk
  5 partitions
  1 LVM physical volume whole disk
  0 LVM physical volumes
```

   c. f. Add a virtual disk to the cache storage pool by executing the following command.
      If you are adding more than one virtual disk, execute the command for each virtual disk.

```
# csgadm storagepool extend -disk /dev/sdc
```

   d. Verify that the virtual disk has been added to the cache storage pool by executing the following command:

```
# csgadm storagepool show
  PV         VG             Fmt  Attr PSize      PFree
  /dev/sdb   CsgStoragePool lvm2 a--  102396.00m 102396.00m
  /dev/sdc   CsgStoragePool lvm2 a--  204796.00m 204796.00m

  VG             #PV #LV #SN Attr   VSize      VFree
  CsgStoragePool   2   0   0 wz--n- 307192.00m 307192.00m
```

3. Change the cache capacity.
   For information on how to change the settings, refer to "5.2 Changing Datastore Settings".

Chapter 7 Deleting Operating Environments

This chapter describes how to delete the operating environments of this product.

The CSG REST API that corresponds to the operation described in this chapter is as follows:

Table 7.1 Support for CSG Web GUI and CSG REST API in Chapter 7

Operating the CSG Web GUI based on the User's Guide	CSG REST API based on the corresponding Reference Guide
7.1 Deleting Defined Information	Shared Folder
	Datastore
	Cloud Provider

7.1 Deleting Defined Information

This section describes how to delete the defined information related to the following resources.

- Shared Folders
- Datastores
- Cloud Providers

7.1.1 Deleting Shared Folders

The procedure for deleting a shared folder from this product is as follows.

1. Confirm that no users are accessing the shared folder to be deleted.
   If the shared folder is being accessed, either wait until the shared folder is no longer being accessed or stop the operation that is accessing the shared folder.
2. Delete all the data in the shared folder to be deleted.
3. In CSG Web GUI, click **Shared Folder** on the global pane.
4. The **Shared folder** screen is displayed.
   Click the radio button for the target shared folder and click **Modify** in the **Action** on the right.
5. The Enter basic settings screen is displayed.
   After changing the **Enable** state to "Disable", click **Next**.
6. The **Enter advanced settings** screen is displayed.
   Click **Next**.
7. The Confirm screen is displayed.
   After confirming that there is no problem changing to the displayed content, click **Done**.
8. Confirm that the **"Enable"** state of the shared folder is changed to "Disable" on the **Shared folder** screen.
9. Click the radio button for the deletion target shared folder on the **Shared folder** screen and click **Delete** in the **Action** on the right.
10. The **Confirm** screen is displayed.
    Click **Done**.
11. In the **Shared folder** screen, confirm that the shared folder to be deleted no longer appears.

7.1.2 Deleting a Datastore

The procedure for deleting a datastore from this product and for deleting the data in a cache and datastore is as follows.

1. Delete all the shared folders in the deletion target datastore.
2. In CSG Web GUI, click **Datastore** on the global pane.

3. The **Datastore** screen is displayed.
   Click the radio button for the datastore to be deleted and then click **Delete** in the Action on the right.

4. The confirmation screen is displayed.
   Click **Done**.

5. In the **Datastore** screen, confirm that the datastore to be deleted no longer appears.

6. Delete the objects on the bucket.
   Even if the datastore is deleted, part of the objects remain in the bucket.
   Directly operate the cloud provider to delete all the objects in the bucket.

Information

After performing Step 1, it is not necessary to wait until the deletion of the objects in the bucket is completed.

7.1.3 Deleting Cloud Providers

The procedure for deleting a cloud provider from this product is as follows.

1. Delete all the datastores in the deletion target cloud provider.

2. In CSG Web GUI, click **Cloud Provider** on the global pane.

3. The **Cloud provider** screen is displayed.
   Click the radio button for the cloud provider to be deleted and then click **Delete** in the **Action** on the right.

4. The confirmation screen is displayed.
   Click **Done**.

5. In the **Cloud provider** screen, confirm that the cloud provider to be deleted no longer appears.

7.2 Deleting the Entire Operating Environment

This section describes how to delete the entire operating environment of this product.

The procedure for deleting the entire operating environment of this product is as follows.

1. Delete the virtual appliance.
   Refer to the virtualization software manual to delete the virtual machine in which this product is running from the virtualization software.

2. Delete the objects on the bucket that were used by this product.
   Directly operate the cloud provider to delete all the objects in the bucket.

Appendix A Specifications List

A.1 Virtual Appliance Specifications

Resource	Requirements	
Physical CPU	Intel Xeon	
Virtual CPU	Required	2CPU
	Recommended	3CPU or more
Memory	Add the following to the 6.0GB - Datastore per 1TB, 0.6 GB - 8 MB per SMB connection	
Server virtualization software	For VMware vSphere	VMware vSphere 6.0 VMware vSphere 6.5 VMware vSphere 6.7 VMware vSphere 7.0 Redundant configuration: VMware vSphere High Availability
	For KVM	Red Hat(R) Enterprise Linux(R) 7.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 7.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 7.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 8.1 (for Intel64) Redundant configuration: Non-supported
	For Hyper-V	Windows Server 2016 Windows Server 2019 Redundant configuration: Non-supported
	IaaS Redundant configuration: Non-supported	Amazon EC2
		Microsoft Azure Virtual Machines
Network adapter	For VMware vSphere	VMXNET3
	For KVM	Virtio
	Hyper-V	None
	Amazon EC2	None
	Microsoft Azure Virtual Machines	None
Virtual disk	System area	100 GB
	Data area	Greater than or equal to (cache capacity + 1MB). However, it should be at least 20 GB. Each virtual disk must be at least 1G in size.
	VMware vSphere (hard disk)	Disk Provisioning: Thick Provisioning (Eager zeroed) Virtual device nodes: SCSI RAID1 + 0 is recommended for the disk area when deploying virtual disks
	KVM (Storage volume)	Format: Raw Bus Type: VirtIO

Resource	Requirements	
		RAID1 + 0 is recommended for the disk area when deploying virtual disks
	Hyper-V (Virtual hard disk)	Format: "VHDX" recommended Type: Fixed size RAID1 + 0 is recommended for the disk area when deploying virtual disks
	Amazon EC2 (EBS volume)	Volume type: "General Purpose SSD" recommended
	Microsoft Azure Virtual Machines	Disk type: "Standard SSD" recommended

Note

Live Migration is not supported.

A.2 Functional Specifications

Item	Content
Number of cloud providers	Up to 4
Number of datastores	1
Datastore size	Minimum: 100 GB Maximum: Total of license capacity
Number of caches	1
Cache size	10% of the datastore (at least 20 GB) Maximum: Size of the virtual disk connected to the virtual machine in which this product is running
Number of shared folders	128
Number of concurrent SMB connections	500
Number of files (per datastore)	10 million or less
Number of files (per directory)	100,000 or less
Number of directories (per datastore)	10 million or less
Number of files opened simultaneously	5,000 or less
List of allowed hosts (per shared folder)	NFS allowed hosts: Up to 10 NFS no root squash hosts: Up to 10 SMB allowed hosts: Up to 10 SMB denied hosts: Up to 10
Supported protocols	NFS v4.0 SMB 3.0
Types of supported files	Normal files, directories, symbolic links, hard link (However, directory hard links are not supported.)
Administrative user authentication	Local authentication
NAS user authentication	Local authentication, Active Directory
Data encryption	Available (AES256)
Deduplication method	Inline variable length

Note

ACLs are not supported.

A.3 Support List

Item	Content
Cloud providers	FUJITSU Cloud Service for OSS Object Storage Amazon S3 Microsoft Azure Blob Storage / FUJITSU Cloud Service for Microsoft Azure Blob Storage NIFCLOUD Object Storage / FUJITSU Cloud Service for VMware NC Object Storage OpenStack Swift
Web browsers	Internet Explorer 11 Microsoft Edge 38 or later Chrome 58 or later

A.4 Supported Backup Software

In general, backup software that supports the NAS interface provided with this product can be used.

A.5 REST API Specifications List

Item	Specifications	Remarks
Communication method	HTTPS	HTTP cannot be used.
Communication port	9856 (Default)	To change the default setting, refer to "2.5.4.2 Setting the HTTPS Port Number".
HTTPS communication protocol	TLS 1.0, 1.1, 1.2	SSL2.0 and 3.0 cannot be used.
Request format	UTF-8 is used for encoding (no BOM).	Encoding varies depending on the file that is uploaded.
Response format	JSON UTF-8 is used for encoding (no BOM).	Encoding varies depending on the file that is uploaded.
Number of requests that can be processed simultaneously	256	"Process" described here refers to the process starting when a request is issued until the time when a response is returned (CSG REST API synchronous processing).
Number of asynchronous processes that can be received simultaneously	256	
Timeout duration	15 minutes	

A.6 Used Port Number

Communication Source	Communication Destination	Port Number	Used Purpose
Operation terminal	This product	22	SSH/SFTP
		9856 (Can be changed)	HTTPS

Communication Source	Communication Destination	Port Number	Used Purpose
This product	Mail server	25 (Can be changed)	SMTP
	DNS server	53	DNS
	NTP server	123	NTP
	AD server	389 (Can be changed)	AD authentication
Backup server	This product	137	SMB
		138	
		139	
		445	
		2049	NFS v4

Appendix B Status Information

B.1 Status of Shared Folders

Status	Overview	Timing
Normal	Normal state	When operations are running normally. Also, when the system returns to the Normal state from another state (automatically returning to the "Normal" state).
Warning	Immediate attention from the user is required	-
Error	An error has occurred	When the folder status of a shared folder that is set to enabled or disabled does not match the actual status.
Unknown	Status is unknown	When one of the following events occurs: - When a status acquisition of the shared folder fails. - When the NFS service or the SMB service is stopped. If the "Unknown" state continues and the shared folder cannot be accessed, the NFS service or the SMB service may have stopped abnormally. Therefore, collect the troubleshooting data and contact our customer support department.

B.2 Cache Status

Status	Overview	Timing
Normal	Normal state	When operations are running normally. Also, when the system returns to the Normal state from another state (automatically returning to the "Normal" state).
Warning	Immediate attention from the user is required	When there is a risk of using up the cache capacity. When there is a risk that the memory where CSG is operating will run out after the cache management memory is acquired.
Error	An error has occurred	When one of the following events occurs: - The cache capacity is used up - Error in cache disk When the cache management memory cannot be acquired.
Unknown	Status is unknown	When one of the following events occurs: - When a status acquisition of the cache fails. - When the datastore service is stopped. If the "Unknown" state continues and the shared folder cannot be accessed, the datastore service may have stopped abnormally. Therefore, collect the troubleshooting data and contact our customer support department.

B.3 Network Status

Status	Overview	Timing
Normal	Normal state	When operations are running normally. Also, when the system returns to the Normal state from another state (automatically returning to the "Normal" state).
Warning	Immediate attention from the user is required	-

Status	Overview	Timing
Error	An error has occurred	When one of the following events occurs: - Authentication failed when a datastore is connected - Failed to connect to a datastore
Unknown	Status is unknown	When one of the following events occurs: - When a status acquisition of the network connection fails. - When the datastore service is stopped. If the "Unknown" state continues and the shared folder cannot be accessed, the datastore service may have stopped abnormally. Therefore, collect the troubleshooting data and contact our customer support department.

B.4 Datastore Status

Status	Overview	Timing
Normal	Normal state	When operations are running normally. Also, when the system returns to the Normal state from another state (automatically returning to the "Normal" state).
Warning	Immediate attention from the user is required	When there is a risk of using up the available capacity of the datastore.
Error	An error has occurred	When one of the following events occurs: - Communication error returned from the datastore - The available capacity of the datastore has been used up. - The account or access key ID of the cloud provider does not have write permission.
Unknown	Status is unknown	When one of the following events occurs: - When a status acquisition of the datastore fails. - When the datastore service is stopped. If the "Unknown" state continues and the shared folder cannot be accessed, the datastore service may have stopped abnormally. Therefore, collect the troubleshooting data and contact our customer support department.

Appendix C Upgrading from an Old Product

This appendix describes how to upgrade an environment that was configured with an earlier version of Cloud Storage Gateway to an environment for the current version of Cloud Storage Gateway.

The upgradeable versions are as follows:

Table C.1 Earlier versions that can be upgraded

Upgrade Target Versions	Upgrade Availability	Remarks
V1.1.x	OK	- "x" stands for 0, 1, 2, etc. - Including environments with the update patch applied
Other versions	NG	

The upgrade procedure is identical to the procedure for applying the update patch. Refer to "6.5 Updating Software" for details.

Note

If you continue using any datastores you created with an earlier version of this product after the upgrade, the environment retains the characteristics of the earlier version for the following items described in "Appendix E Incompatibility Information".

- "E.1.2 Amount of Resources Used by Virtual Appliances"
- "E.1.3 Minimum Cache Capacity"
- "E.1.4 Status Change Triggers"

Appendix D Snapshots

This appendix describes how to use snapshots for this product in various virtualization software environments.

Note

- Snapshots for this product are not to create backups but to ensure that the system can be reverted to its original state if a patch update fails or if an upgrade process fails.
- Before using the snapshot function, be sure to stop the virtual machine of this product. Before stopping the virtual machine, stop any operations that are accessing the shared folder. Next, go to the **Used cache capacity** panel of CSG Web GUI, check that **Untransferred data** is indicating **No**, and then stop the virtual machine.
- The way a public cloud service is operated may change. For the latest information on how to operate each public cloud service, refer to the documentation of each service.

D.1 Creating a Snapshot

This section describes how to create a snapshot.

D.1.1 Creating Snapshots in VMware vSphere Environments

The procedure for vSphere Host Client is described below.

1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

   ```
   # csgadm power stop
   ```

2. A list of virtual machines is displayed in vSphere Host Client.
3. Right-click the virtual machine of this product to open the menu.
4. To create a snapshot, select **Take Snapshot** in **Snapshots**.
   Enter a name.
   Deselect the following checkboxes.

   - Snapshot the virtual machine's memory
   - Quiesce guest file system

D.1.2 Creating Snapshots in KVM Environments

1. 1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

   ```
   # csgadm power stop
   ```

2. Log in to the KVM host.
3. Use the qemu-img command to create a qcow2 image based on the virtual disk images for the system and cache areas.
   The following example shows how to create CSG_v110_kvm_tmp.qcow2 from the CSG_v110_kvm.qcow2 virtual disk file for the system area and how to create CSG_v110_cache_tmp.qcow2 from the CSG_v110_cache.raw virtual disk file for the cache area.

   ```
   # cd /var/lib/libvirt/images
   # qemu-img create -f qcow2 -b CSG_v110_kvm.qcow2 CSG_v110_kvm_tmp.qcow2
   # qemu-img create -f qcow2 -b CSG_v110_cache.img CSG_v110_cache_tmp.qcow2
   ```

4. Change the settings of the virtual machine to use the created qcow2 image by using the virsh edit command.
   In the virtual disk file for the system area, change the file attribute of the <source> tag to the created qcow2 image.
   In the virtual disk file for the cache area, change the type attribute of the <driver> tag from raw to qcow2 and the file attribute of the

<source> tag to the created qcow2 image.
The following is an execution example. Domain names are virtual machine names displayed in the virtual machine manager.
[Execution example]

```
# virsh edit domain_name
```

The following example illustrates how to change the parameters. The highlighted parts need to be changed.

[Before the change]

```
  <devices>
     <emulator>/usr/libexec/qemu-kvm</emulator>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/var/lib/libvirt/images/CSG_v110_kvm.qcow2'/>
       <target dev='hda' bus='ide'/>
       <address type='drive' controller='0' bus='0' target='0' unit='0'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='raw'/>
       <source file='/var/lib/libvirt/images/CSG_v110_cache.img'/>
       <target dev='vda' bus='virtio'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
     </disk>
```

[After the change]

```
  <devices>
     <emulator>/usr/libexec/qemu-kvm</emulator>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/var/lib/libvirt/images/CSG_v110_kvm_tmp.qcow2'/>
       <target dev='hda' bus='ide'/>
       <address type='drive' controller='0' bus='0' target='0' unit='0'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/var/lib/libvirt/images/CSG_v110_cache_tmp.qcow2'/>
       <target dev='vda' bus='virtio'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
     </disk>
```

Note

If you are using multiple virtual disk files for the cache area, create a qcow2 image for each one of them and change the virtual machine settings.

D.1.3 Creating Snapshots in Hyper-V Environments

1. Stop the virtual machine of this product if it is running. Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

```
# csgadm power stop
```

2. Start Hyper-V Manager.

3. Right-click the virtual machine of this product to open the menu.

4. Select **Checkpoint** to create a checkpoint.

D.1.4 Creating Snapshots in Amazon EC2 Environments

1. Stop the instance of this product if it is running.
   Log in to the console of this product using the administrator account to stop the instance with the following command.

```
# csgadm power stop
```

2. Select the instance of this product on the EC2 dashboard.

3. Perform the following operations for all the block devices that are displayed in the **Description** tab of the instance.

   a. Click the device name.
      The names of block devices for the system area are displayed as "/dev/sda1."
      Detailed information about the selected block device is displayed.

   b. Click the EBS ID shown in the detailed information of the block device.
      The volume information of the selected block device is displayed.

      Point

      If the **Name** section has not been set for the volume, configuring the setting that includes the instance name and device name is recommended to easily find the volume for future operations.

   c. To create a snapshot, select **Create Snapshot** from **Actions**.

      Point

      - Including the instance name and device name in the **Description** section is recommended to easily find the created snapshot for future operations.
      - After creating a snapshot, including the instance name and device name in the **Name** section is also recommended.

D.1.5 Creating Snapshots in Microsoft Azure Virtual Machines Environments

1. Go to the **Virtual machines** service on the Azure portal and select the virtual machine of this product.

2. Stop the virtual machine of this product if it is running.
   Click **Stop** to stop the virtual machine.

3. Select **Disks** on the **Settings** menu, and perform the following operations for all of the disks that are displayed (OS disk and Data disks).

   a. Click the disk name.

   b. To create a snapshot, click **Create snapshot**.
      Configure the settings as follows.

Item	Setting Details
Name	Including the virtual machine name is recommended to easily find the created snapshot for future operations. In addition, if multiple data disks exist, enter names to easily identify the order of their connection.
Resource group	Use the same setting as for the snapshot source disk.
Account type	**Standard HDD**

D.2 Snapshot Restoration

This section describes how to restore the system with a snapshot.
By restoring a snapshot, you can revert this product to the point when that snapshot was created.

D.2.1 Snapshot Restoration for VMware vSphere Environments

The procedure for vSphere Host Client is described below.

1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

   ```
   # csgadm power stop
   ```

2. A list of virtual machines is displayed in vSphere Host Client.

3. Right-click the virtual machine of this product to open the menu.

4. To restore the system with a snapshot, select **Revert to snapshot** in **Snapshot**.

D.2.2 Snapshot Restoration for KVM Environments

1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

   ```
   # csgadm power stop
   ```

2. Log in to the KVM host.
   Delete the qcow2 image created in step 3 of "D.1.2 Creating Snapshots in KVM Environments."
   The following example shows how to delete the system area qcow2 image (CSG_v110_kvm_tmp.qcow2) and the cache area qcow2 image (CSG_v110_cache_tmp.qcow2).

   ```
   # cd /var/lib/libvirt/images
   # rm CSG_v110_kvm_tmp.qcow2
   # rm CSG_v110_cache_tmp.qcow2
   ```

3. Perform step 3 of "D.1.2 Creating Snapshots in KVM Environments" to create a new qcow2 image.

D.2.3 Snapshot Restoration for Hyper-V Environments

1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

   ```
   # csgadm power stop
   ```

2. Start Hyper-V Manager.

3. Select the virtual machine of this product.

4. Right-click a checkpoint shown in the **Checkpoints** section.

5. Select **Apply** to apply the checkpoint.

D.2.4 Snapshot Restoration for Amazon EC2 Environments

To restore the system, delete the current volume, and create a new volume from a snapshot.

Note

Before deleting a volume, make sure a snapshot has been created for that volume.

1. Stop the instance of this product if it is running.
   Log in to the console of this product using the administrator account to stop the instance with the following command.

   ```
   # csgadm power stop
   ```

2. Follow the procedure below to delete all the existing volumes from the instance of this product.

   a. Open the volume list on the EC2 dashboard.

   b. Select all of the volumes in the corresponding instance.

   c. Select **Detach Volumes** from **Actions** to detach the volumes from the instance.

   d. Select **Delete Volumes** from **Actions** to delete the volumes.

3. Create new volumes from all the snapshots of the instance of this product.
   Perform the following procedure for all the snapshots of the corresponding instance.

   a. Open the snapshot list on the EC2 dashboard.

   b. Select one of the snapshots in the corresponding instance.

   c. Select **Create Volume** from **Actions** to create a volume.

   Point

   - If you follow the procedure to create a volume according to the on-screen instructions, the volume ID appears at the end. Do not click **Close**. Click the volume ID. Information about the created volume is displayed.

   - Because volume creation takes time, the volume information may not appear immediately after the volume ID is clicked. If it is not displayed after some time, click the refresh button on the upper right corner of the volume screen.

   - Including the instance name and device name in the **Name** section of the created volume is recommended to easily find the created volume for future operations.

   Note

   In this procedure, step 3 is not necessary for snapshots with the **Created by AWS-VMImport service...** remark in the description section.

4. Attach the created volumes to the instance of this product.
   Perform the following procedure for all the volumes of the corresponding instance in order of the device name.

   - Open the volume list on the EC2 dashboard.

   Point

   If a single volume is found in step 3, click the **Volumes** menu on the EC2 dashboard, or clear the volume search bar and perform a new search to display all of the volumes.

   - Select one of the volumes in the corresponding instance.

   - Select **Attach Volume** from **Actions** to attach the volume to the instance.
     Select the corresponding instance in the **Instance** section.
     Enter the device name of the volume to attach in the **Device** section.
     The device name of the system area is "/dev/sda1."

D.2.5 Snapshot Restoration for Microsoft Azure Virtual Machines Environments

1. Stop the virtual machine of this product if it is running.
   Go to the Virtual machines service on the Azure portal, select a virtual machine, and click Stop to stop the virtual machine.

2. Use snapshots to create new disks.
   Click Add in the Disks service of the Azure portal and then use all the snapshots of the virtual machine of this product to create new disks (OS disk and Data disks).
   Configure the settings as follows.

Item	Setting Details
Name	Including the virtual machine name is recommended to easily find the created volume for future operations. In addition, if multiple data disks are attached, including a name to easily identify the connection order is recommended.
Subscription	Use the same setting as for the snapshot source disk.
Resource group	Use the same setting as for the snapshot source disk.
Location	Use the same setting as for the snapshot source disk.
Account type	Standard SSD
Source type	Snapshot
Source snapshot	Snapshot in the virtual machine of this product
Size	Use the same setting as for the snapshot source disk.

3. Use Azure CLI to replace the OS disk with the disk created in step 2.

   - Execute the following command to check the ID of the created OS disk.

```
az disk show --name "disk name" --resource-group "resource group name"
```

Include the following information in the command.

Item	Setting Details
disk name	Name of the OS disk specified in step 2
resource group name	Name of the resource group specified in step 2

The "id" value in the output results represents the disk ID.

   - Run the following command to replace the OS disk with the created disk.

```
az vm update -n "virtual machine name" -g "resource group name" --os-disk "id"
```

Include the following information in the command.

Item	Setting Details
virtual machine name	Name of the virtual machine of this product
resource group name	Name of the resource group for the virtual machine of this product
id	Disk ID

   - Confirm that the OS disk have been replaced.
     Go to the Virtual machine service on the Azure portal, and click the virtual machine name for this product. Select Disks from the Settings menu, and check the names of the OS disk.

Point

- For details about Azure CLI, refer to the Microsoft Azure document "Azure Command-Line Interface (CLI)."
- Azure CLI can also be started by clicking the Cloud Shell icon (>_) on the Azure portal.

4. Detach all of the data disks from the virtual machine.

   a. Go to the **Virtual machines** service on the Azure portal, and click the virtual machine name.

   b. Select **Disks** on the **Settings** menu of the virtual machine, and click **Edit**.

   c. To detach the data disks, click a detach icon to the right side of each line where a data disk is displayed. Click **Save** when you finish detaching disks.

5. Add all of the data disks from step 2 in the order in which they were connected to the virtual machine.
   Click **Add data disk** to select and add data disks. If the **HOST CACHING** option is available, make sure the settings match the previous data disks. Click **Save** when you finish adding disks.

6. Delete all the previous data disks connected to the virtual machine of this product.
   Perform the following operations for all of the previous data disks.

   a. Go to the **Disks** service on the Azure portal, and click the disk name.

   b. Click **Delete** to delete the disk.

D.3 Deleting a Snapshot

This section describes how to delete a snapshot.
If a snapshot is deleted, the updates that occur after creating a snapshot are applied to this product.

D.3.1 Deleting Snapshots in VMware vSphere Environments

The procedure for vSphere Host Client is described below.

1. Stop the virtual machine of this product if it is running. Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

```
# csgadm power stop
```

2. A list of virtual machines is displayed in vSphere Host Client.

3. Right-click the virtual machine of this product to open the menu.

4. Select **Manage Snapshots** from **Snapshots**.

5. Select the latest snapshot on the snapshot management screen.

6. Click **Delete** to delete the snapshot.

D.3.2 Deleting Snapshots in KVM Environments

1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

```
# csgadm power stop
```

2. Log in to the KVM host.

3. 3. Use the qemu-img command to apply the qcow2 image created in step 3 of "D.1.2 Creating Snapshots in KVM Environments" to the base file.

Note

If you want to stop the process of applying an update patch or upgrading the system in order to return to the previous environment, do not perform step 3 of this procedure. Proceed to step 4.

The example below shows how to apply both the CSG_v110_kvm_tmp.qcow2 image for the system area and the CSG_v110_cache_tmp.qcow2 image for the cache area to the base file.

```
# cd /var/lib/libvirt/images
# qemu-img commit CSG_v110_kvm_tmp.qcow2
# qemu-img commit CSG_v110_cache_tmp.qcow2
```

4. Delete the qcow2 image created in step 3 of "D.1.2 Creating Snapshots in KVM Environments."
   The example below shows how to delete the CSG_v110_kvm_tmp.qcow2 image for the system area and the CSG_v110_cache_tmp.qcow2 image for the cache area.

```
# cd /var/lib/libvirt/images
# rm CSG_v110_kvm_tmp.qcow2
# rm CSG_v110_cache_tmp.qcow2
```

5. Use the virsh edit command to change the settings of the virtual machine to use the base file.
   In the virtual disk file for the system area, change the file attribute of the <source> tag to the base file.
   In the virtual disk file for the cache area, change the type attribute of the <driver> tag from qcow2 to raw and the file attribute of the <source> tag to the base file.
   An example is provided below. Domain names are virtual machine names displayed in the virtual machine manager.
   [Execution example]

```
# virsh edit domain_name
```

The following example illustrates how to change the parameters. The highlighted parts need to be changed.

[Before the change]

```
  <devices>
     <emulator>/usr/libexec/qemu-kvm</emulator>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/var/lib/libvirt/images/CSG_v110_kvm_tmp.qcow2'/>
       <target dev='hda' bus='ide'/>
       <address type='drive' controller='0' bus='0' target='0' unit='0'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/var/lib/libvirt/images/CSG_v110_cache_tmp.qcow2'/>
       <target dev='vda' bus='virtio'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
     </disk>
```

[After the change]

```
  <devices>
     <emulator>/usr/libexec/qemu-kvm</emulator>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/var/lib/libvirt/images/CSG_v110_kvm.qcow2'/>
       <target dev='hda' bus='ide'/>
       <address type='drive' controller='0' bus='0' target='0' unit='0'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='raw'/>
       <source file='/var/lib/libvirt/images/CSG_v110_cache.img'/>
       <target dev='vda' bus='virtio'/>
```

```
    <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
  </disk>
```

D.3.3 Deleting Snapshots in Hyper-V Environments

1. Stop the virtual machine of this product if it is running.
   Log in to the console of this product using the administrator account to stop the virtual machine with the following command.

   ```
   # csgadm power stop
   ```

2. Start Hyper-V Manager.

3. Select the virtual machine of this product.

4. Right-click a checkpoint shown in the **Checkpoints** section.

5. Select **Delete Checkpoint** to delete the checkpoint.

D.3.4 Deleting Snapshots in Amazon EC2 Environments

1. Stop the instance of this product if it is running.
   Log in to the console of this product using the administrator account to stop the instance with the following command.

   ```
   # csgadm power stop
   ```

2. Open the snapshot list on the EC2 dashboard.

3. Select all of the snapshots in the instance of this product.

   Note

   Do not select any snapshots with the **Created by AWS-VMImport service...** remark in the description section.

4. Select **Delete** from **Actions** to delete the snapshots.

D.3.5 Deleting Snapshots in Microsoft Azure Virtual Machines Environments

1. Stop the virtual machine of this product if it is running.
   Go to the **Virtual machines** service on the Azure portal, select a virtual machine, and click **Stop** to stop the virtual machine.

2. Delete all the snapshots of the virtual machine for this product.
   Perform the following operation for all the snapshots of the virtual machine for this product.

   a. Go to the **Snapshots** service on the Azure portal and click the snapshot name.

   b. Click **Delete** to delete the snapshot.

Point

If a snapshot has been restored once, any source disks (OS disk and Data disks) used for creating the snapshot remain registered. After deleting the snapshots, go to the **Disks** service on the Azure portal, check the disks that are not connected to the virtual machine (such as disks where the **OWNER** section is blank), and delete those that were used for creating the snapshots.

Appendix E Incompatibility Information

E.1 Information on the Incompatibility with Versions before v1.2.0.

This appendix provides information on the incompatibility with versions before v1.2.0.

E.1.1 URI Format for Amazon S3

For the URI specified when a cloud provider is registered or changed, the supported URI format has changed as follows for Amazon S3.

Table E.1 Changes in the URI format for Amazon S3

Changes	V1.1.0	V1.2.0
Supported URI format	No format specified	Only one of the following formats is supported. (XXXXX indicates region information): https://s3-XXXXX.amazonaws.com/ https://s3.XXXXX.amazonaws.com/

E.1.2 Amount of Resources Used by Virtual Appliances

The amount of resources used by virtual appliances has changed as follows.

Table E.2 Amount of resources used by virtual appliances

Changes	V1.1.0	V1.2.0
Memory	The following amounts are added to 4.0 GB: - 1.2 GB for each 1 TB datastore - 8 MB for every SMB connection	The following amounts are added to 6.0 GB: - 0.6 GB for each 1 TB datastore - 8 MB for every SMB connection

E.1.3 Minimum Cache Capacity

The minimum cache capacity has changed as follows.

Table E.3 Minimum cache capacity

Changes	V1.1.0	V1.2.0
Minimum cache capacity	20% of the datastore capacity	10% of the datastore capacity (at least 20 GB)

E.1.4 Status Change Triggers

The triggers that cause the cache status to change has changed as follows.

Table E.4 Status change triggers

Changes	V1.1.0	V1.2.0
Warning	When there is a risk of using up the cache capacity.	When there is a risk of using up the cache capacity. When there is a risk that the memory where CSG is operating will run out after the cache management memory is acquired.
Error	When one of the following events occurs: - The cache capacity is used up. - An error occurs on the cache disk.	When one of the following events occurs: - The cache capacity is used up. - An error occurs on the cache disk. When the cache management memory cannot be acquired.