FUJITSU Software
Cloud Storage Gateway V1.0.0

User's Guide

J2UL-2275-01ENZ0(00)
April 2018

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 or KVM)
- 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.

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
	Red Hat(R) Enterprise Linux(R) 7.3 (for Intel 64)	RHEL

Type	Formal Name	Abbreviation
	Red Hat(R) Enterprise Linux(R) 7.4 (for Intel 64)	
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

- Microsoft, Windows, and other Microsoft products are registered trademarks of Microsoft Corporation in the United States and other countries.
- 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.
- All other brand and product names are trademarks or registered 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)

Notice

- No part of this manual may be reproduced without permission.

- This manual is subject to change without advance notice.

Copyright

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

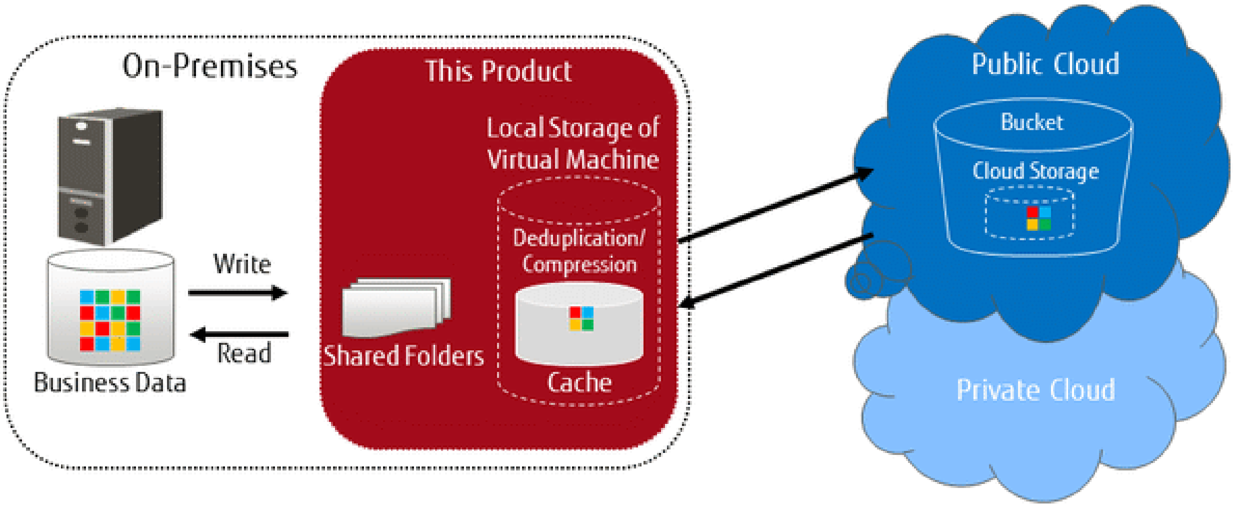
Chapter 1 Product Description

1.1 Product Overview

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

It provides a "shared folder" that can be accessed with the NFS/SMB protocol, performs an internal deduplication on data that is written to this shared folder, and temporarily 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. It is not necessary to change or integrate backup software when backing up data 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.

1.2 System Configuration

The system configuration diagrams of this product are shown below.

Figure 1.2 System Configuration (When Using a Public Cloud)

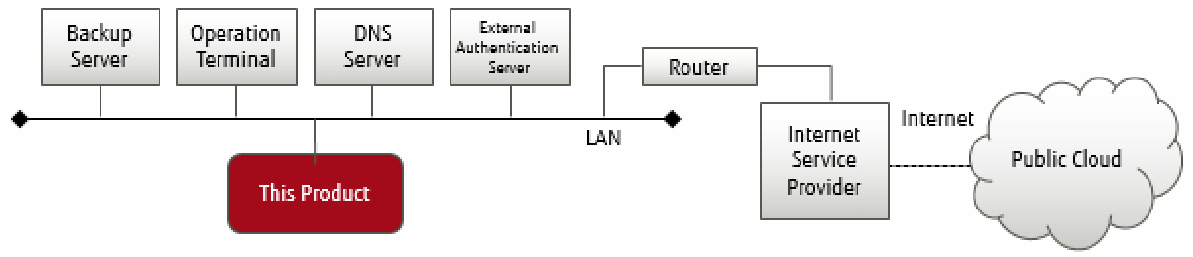
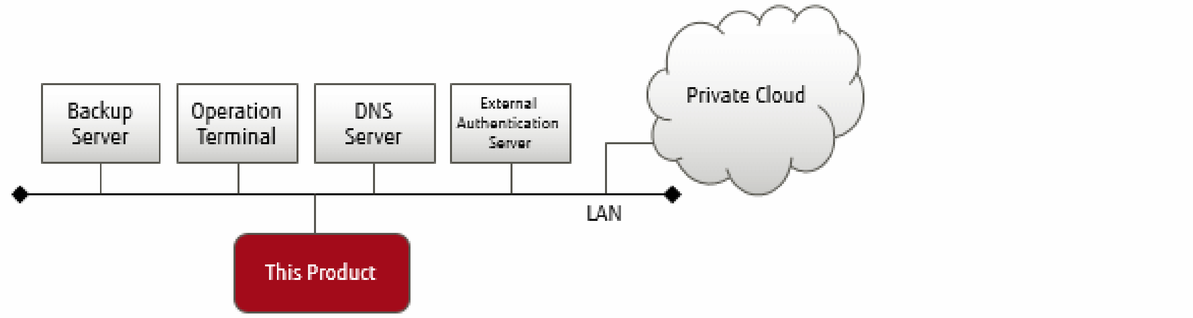


Figure 1.3 System Configuration (When Using a Private Cloud)



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

Figure 1.4 Component Layout

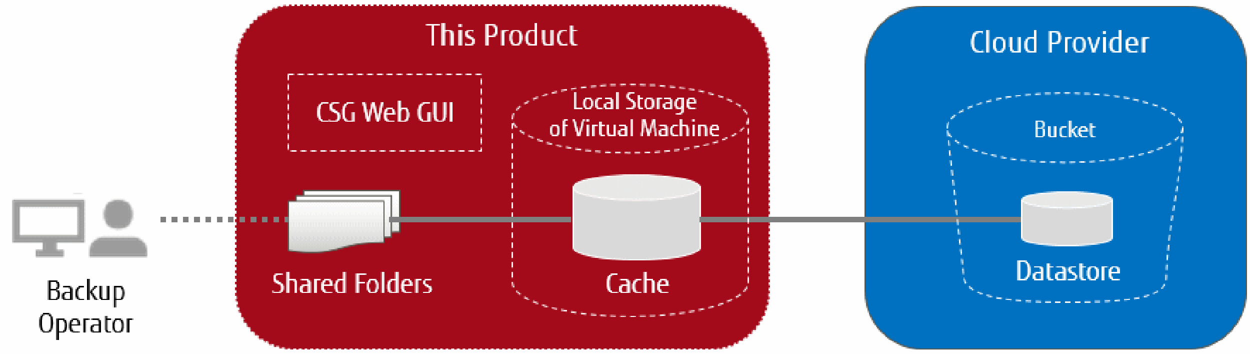


Table 1.1 List of Required Components

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 K5 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	An area for storing data in a cloud storage after the data in the cache is transferred to the cloud storage. A datastore is created in a bucket in the cloud storage.

Component Name	Description
	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.	Stored in cache. Not subject to deletion.

Cache Usage Rate	Handling of Actual Data	Handling of Meta Data
	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%.	

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.

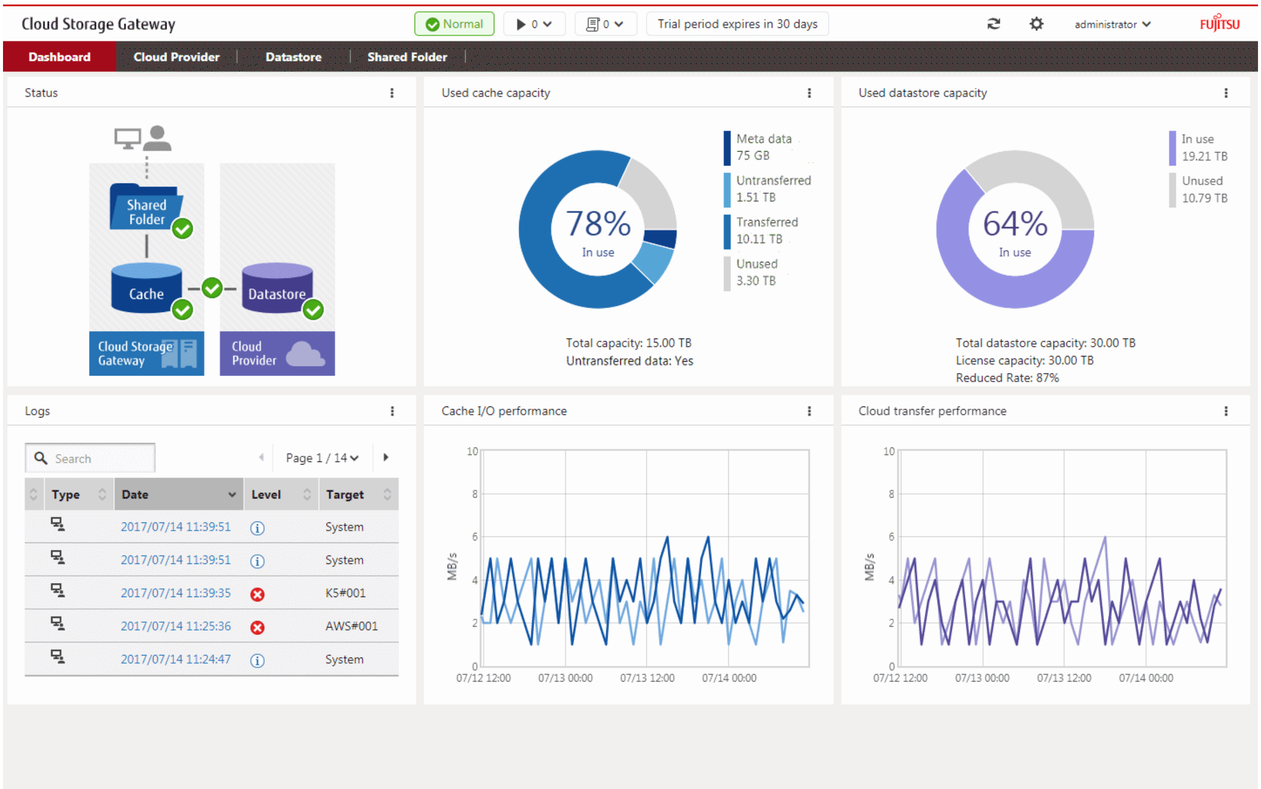
1.4.2 User Interface

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



Total capacity: 15.00 TB
Untransferred data: Yes

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

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

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".

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 "2.5.7 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.

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.

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.

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 "20% of the datastore capacity" to the "size of a virtual disk connected to the virtual machine in which this product is running - 1MB".
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".

Note

Once the cache capacity has been set, it cannot be changed.

2.1.3 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 K5 Object Storage

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

Amazon S3

- URI (Cloud provider access point)
- Access key ID
- Secret access key
- Bucket name

NIFCLOUD Object Storage

- URI (Cloud provider access point)
- Access key ID
- Secret access key
- Bucket name

OpenStack Swift

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

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.

2.2.1 Deploying to VMware vSphere Environment

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

1. Start the vSphere Client, and click **Deploy OVF Template...** in the **File** menu.
2. In the source selection 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 **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed** 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. 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_v100_kvm.tar.gz
CSG_v100_kvm/
CSG_v100_kvm/CSG_v100_kvm.qcow2
CSG_v100_kvm/CSG_v100_kvm.xml
```

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

```
# cp CSG_v100_kvm.qcow2 /var/lib/libvirt/images
# cp CSG_v100_kvm.xml /etc/libvirt/qemu
```

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

```
# virsh define /etc/libvirt/qemu/CSG_v100_kvm.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. 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". In the virtual machine details screen, click **Add Hardware** and then click **Storage** in the **Add New Virtual Hardware** dialog box.

10. 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.

11. Return to **Add New Virtual Hardware** dialog box and set **Bus type** to "**VirtIO**".

12. Click **Finish**.

2.3 Setting Up Virtual Appliances

After starting the virtual appliance for this product, use the Initial Setup 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 initial_setup in the current directory. (Pressing the Tab key after entering "init" allows you to enter the completed command "initial_setup".)

3. When the Initial Setup 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**
   - **Configure DHCP**
   - **Setting Hostname**

  - Configure Network
  - 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

- The default password is set for the administrator account. For security purposes, be sure to change this password under **"Change Administrator Password"** in the Initial Setup Wizard. Set from 8 to 64 characters for the password. You must use at least three of the following four types of characters: uppercase letters, lowercase letters, numbers, and symbols (!"#$&'()*+,-./@[\]^_`{|}~:;<=>?).
- To use an external authentication server, be sure to enable Network Time Protocol (NTP).
- If an external authentication server (Active Directory server) is used with SMB, the DNS server setting is required.

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 as an example. For KVM, change "/dev/sdX" to "/dev/vdX".

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.

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 Initial Setup 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
   ```

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 Web Console 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 Web Console 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 address of this product is displayed in **Websites you've added** to **Compatibility View**, select the 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.

```
>..\bin\openssl.exe 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.

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

Item	Required?	Description
		- 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 FTP to the virtual server in which this product is running.
   Transfer destination: /Administrator/ftp
   User: administrator
   Password: The password set under **"Change Administrator Password"** in the Initial Setup 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 FTP 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

   - To use an external authentication server, be sure to enable NTP.

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

- 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.

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.

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 the "**Done"** button.
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 2.1 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.

2.5.7 Monitoring Settings

Configure the settings in "2.5.7.1 E-mail Server Settings" and "2.5.7.2 E-mail Notification Settings" to send E-mail notifications regarding events that occur in this product.

2.5.7.1 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 the **"Apply"** button.

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.

2.5.7.2 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 the **"Apply"** button.

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 "2.5.7.1 E-mail Server Settings".
To	The notification E-mail addresses that were specified in "2.5.7.2 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 "Message".

- Test E-mail

Item	Content
Subject	Cloud Storage Gateway Test Mail
From	The sender's E-mail address that was specified in "2.5.7.1 E-mail Server Settings".
To	The notification E-mail addresses that were specified in "2.5.7.2 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

2.6 Setting CSG Web GUI / CSG REST API Users

There are two methods for a user without a user account created in "2.5.5 Starting CSG Web GUI" to use this product, as described below:

- With a local authentication user

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

- With an external authentication user (user account that is authenticated externally)

  You can register an authentication server in this product, and then access CSG Web GUI and CSG REST API via a user account that is registered on that authentication server.

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 an 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 the "**Done**" button.
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"**.

2.6.2 Settings When Using CSG Web GUI and CSG REST API with the External Authentication User

When using CSG Web GUI and CSG REST API with the external authentication user, register the external authentication server (LDAP server or Active Directory server) in this product in advance.

Setting Procedure

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

1. Create the following user role groups in the authentication server.

Role Name	Group Name
Administrator	CsgAdmin
Monitor	CsgMon

2. In the authentication server, register the externally authenticated user in the user role group.
3. In CSG Web GUI, click [⚙] on the global pane.
4. The **Settings** dialog box is displayed.
   Click **Authentication** > **Authentication server** on the left pane.
5. The **Authentication server list** screen is displayed.
   Click **"Register"** in the Action on the right.
6. The **Register authentication server** screen is displayed.
   After entering the required fields, click the **"Done"** button.
7. In the **Authentication server list** screen, confirm that the authentication server you registered appears.
8. Select a registered authentication server and run "Test" from the Action on the right.
   If the test fails, please check whether the Input Items for the registered authentication server has been entered correctly.

Point

For authentication servers, up to 8 LDAP/AD authentication servers can be registered.

Input Items

Item	Required?	Description
Type	Required	Select LDAP or AD.
IP address	Required	Specify the IP address of the authentication server.
Port	Required	Specify the port number of the authentication server. The default is 389.
Domain	Required	Specify the domain name.
User search base	Required	Specify the identification name to use for the user search. Exclude the domain portion for the identification name. (Example: cn=users)
Group search base	Required	Specify the identification name to use for the group search. Exclude the domain portion for the identification name. (Example: cn=users)
Administrator user	Required	Specify the user name for logging in to the authentication server.
Administrator password	Required	Specify the password for logging in to the authentication server.
SSL	Required	Select one of the following for the encryption communication method. The default is **"None"**. - None - SSL/TLS - STARTTLS
Priority	Optional	Specify the priority of the authentication servers.

Item	Required?	Description
		The smaller this number is, the higher the priority becomes. If the value already in use is specified, the priority of the registered servers all increase by one. If omitted, the lowest priority is assigned.
Description	Optional	Enter a description.

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.

Similar to CSG Web GUI/CSG REST API users, 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 LDAP servers or AD servers).

If you use the procedure described in "2.6 Setting CSG Web GUI / CSG REST API Users" to define an authentication server, the authentication server is also used for NAS authentication.

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 the **"Done"** button.

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,

Item	Required?	Description
		ssh_keys, sys, systemd-bus-proxy, systemd-journal, systemd-network, tape, tss, tty, users, utempter, utmp, vauser, video, wbpriv, wheel
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.

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 the **"Done"** button.

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
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.

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 an NFS 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" screen is displayed on the right pane.
     Click "Set NFS authentication servers" in the **Action** on the right.
  4. The **"Set NFS authentication servers"** screen is displayed.
     On the left side of the screen, select the LDAP server that you want to register and then click the **[→ Add]** button.
     Repeat this step for each server that you want to register.
  5. Click the **"Done"** button.
  6. In the **NAS authentication server** screen, confirm that the LDAP server you registered appears.

- When Setting 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" screen is displayed on the right pane.
     Click "Set SMB authentication servers" in the **Action** on the right.
  4. The **"Set SMB authentication servers"** screen is displayed.
     On the left side of the screen, select the AD server that you want to register and then click the **[→ Add]** button.
  5. Click the **"Done"** button.
  6. In the **NAS authentication server** screen, confirm that the AD server you registered appears.

Point

You can select whether to use local authentication or external authentication for each protocol. For example, you can use external authentication for SMB and local authentication for NFS.

Input Items

- When Setting an NFS Authentication Server

Item	Required?	Description
LDAP server	Optional	Set an authentication server (LDAP server) to use with NFS. You can set up to 4 servers. If you register multiple LDAP servers, they are used for authentication in the order they are displayed in the "NAS authentication server" screen of CSG Web GUI. If no server is set, authentication is performed based on the NAS Access User Settings.

- When Setting an SMB Authentication Server

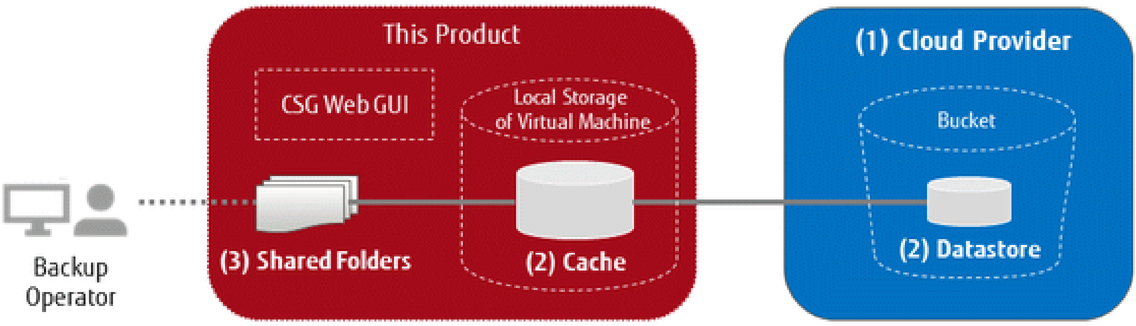
Item	Required?	Description
AD server	Optional	Set an authentication server (AD server) to use with SMB. You can set only 1 server. If no server is set, authentication is performed based on the NAS Access User Settings.

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



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.

3.1.1 Supported Cloud Providers

This product supports the following cloud providers:

- FUJITSU Cloud Service K5 Object Storage
- Amazon S3
- NIFCLOUD Object Storage
- OpenStack Swift

3.1.2 Information Required for Registering a Cloud Provider

FUJITSU Cloud Service K5 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.
Account	An account name for accessing FUJITSU Cloud Service K5 Object Storage.
Password	A password for accessing FUJITSU Cloud Service K5 Object Storage.
Domain ID	A domain ID for accessing FUJITSU Cloud Service K5 Object Storage.
Project ID	A project ID for accessing FUJITSU Cloud Service K5 Object Storage.

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 "https://s3-ap-northeast-1.amazonaws.com/". - If the bucket is in the US East (Northern Virginia) region, specify "https://s3.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.

NIFCLOUD 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.
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.

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.

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 the "**Done**" button.
6. In the "**Cloud Provider**" screen, confirm that the cloud provider you registered is displayed.

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 20% of the datastore or larger, 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	Set whether to compress the data when storing it in the datastore. The default setting is "Enable".
Datastore encryption	Optional	Set 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".

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 the **"Done"** button.
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.

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 encoding). The following characters cannot be used:

Item	Required?	Description
		- 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)
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.
Group	Optional	The name of the group to which the shared folder belongs. If omitted, "root" is set.
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".

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. You can specify up to 10 IPv4 or FQDN addresses. When specifying multiple hosts, separate them with a comma (,). If this setting is omitted, all hosts are granted NFS access.
NFS root squash hosts	Optional	Hosts specified in **NFS allow hosts** and granted root access. You can specify up to 10 hosts. When specifying multiple hosts, separate them with a comma (,). If this setting is omitted, root access is not granted for any host.

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. You can specify up to 10 IPv4 or FQDN addresses. When specifying multiple hosts, separate them with a comma (,). If this setting is omitted, all hosts are granted SMB access.
SMB deny hosts	Optional	Host information for which SMB access is not granted. You can specify up to 10 IPv4 or FQDN addresses. When specifying multiple hosts, separate them with a comma (,). If this setting is omitted, all hosts are granted SMB access.

3.3.3 Procedure for Registering a Shared Folder

The procedure for registering a shared folder 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.
   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 "3.3.2 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 "3.3.2 Information Required for Registering a Shared Folder" to enter the required information and then click **Next**.

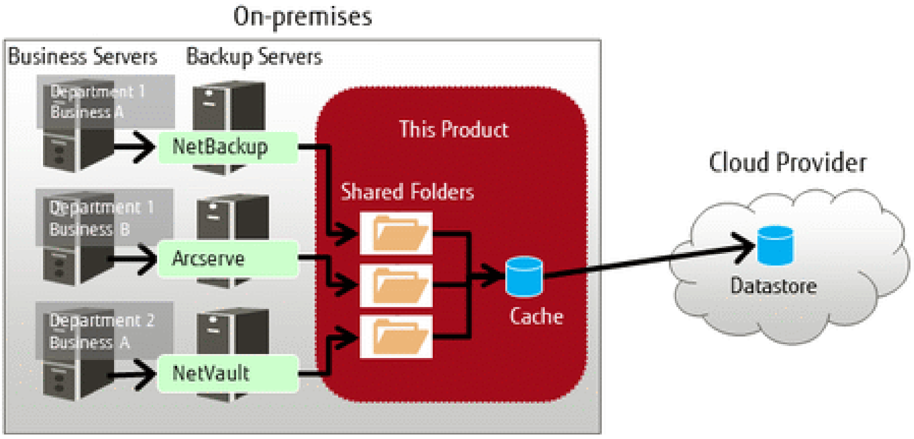
5. The **Confirm** screen is displayed.
   Confirm that there is no problem with the registered content that is displayed and then click **the "Done" button**.

6. In the **"Shared folder"** screen, confirm that the shared folder you registered is displayed.

Chapter 4 Operation

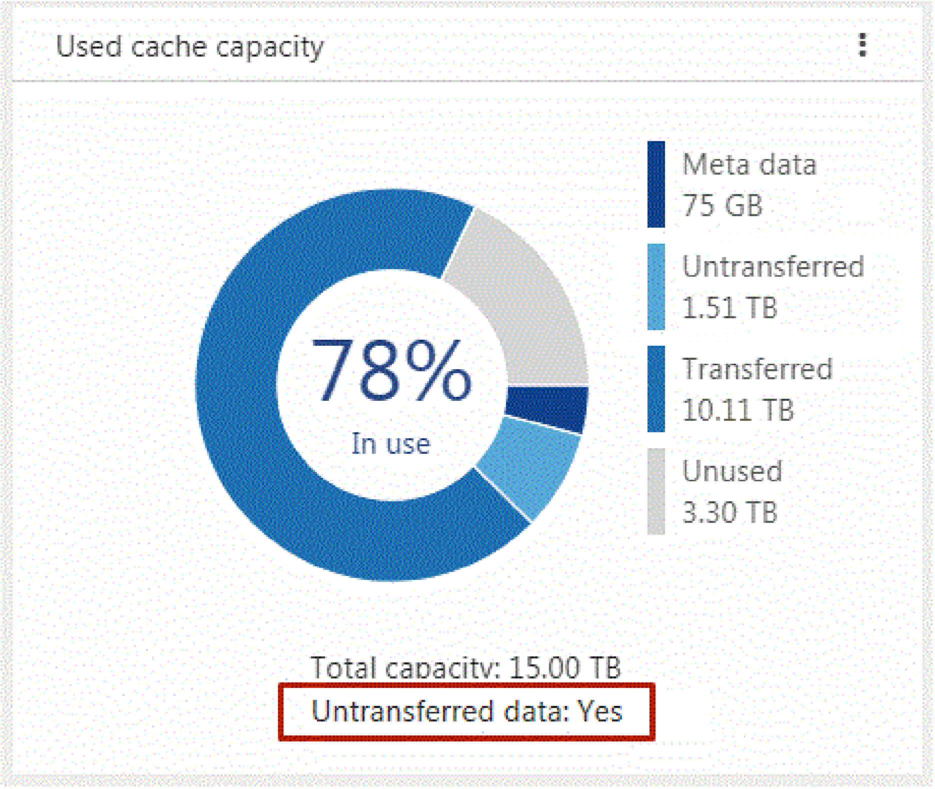
4.1 Backing up to Cloud Provider

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.



Total capacity: 15.00 TB

Untransferred data: Yes

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 "2.5.7 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

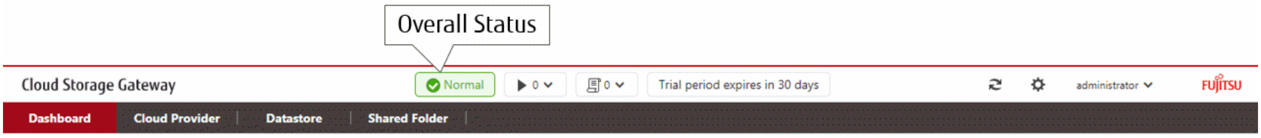


Table 4.1 Types and Meanings of Icons Displayed in Overall Status

Icon	Status	Meaning
✓ Normal	Normal state	All resources displayed on the **Status** panel are operating normally.

Icon	Status	Meaning
⚠ 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.

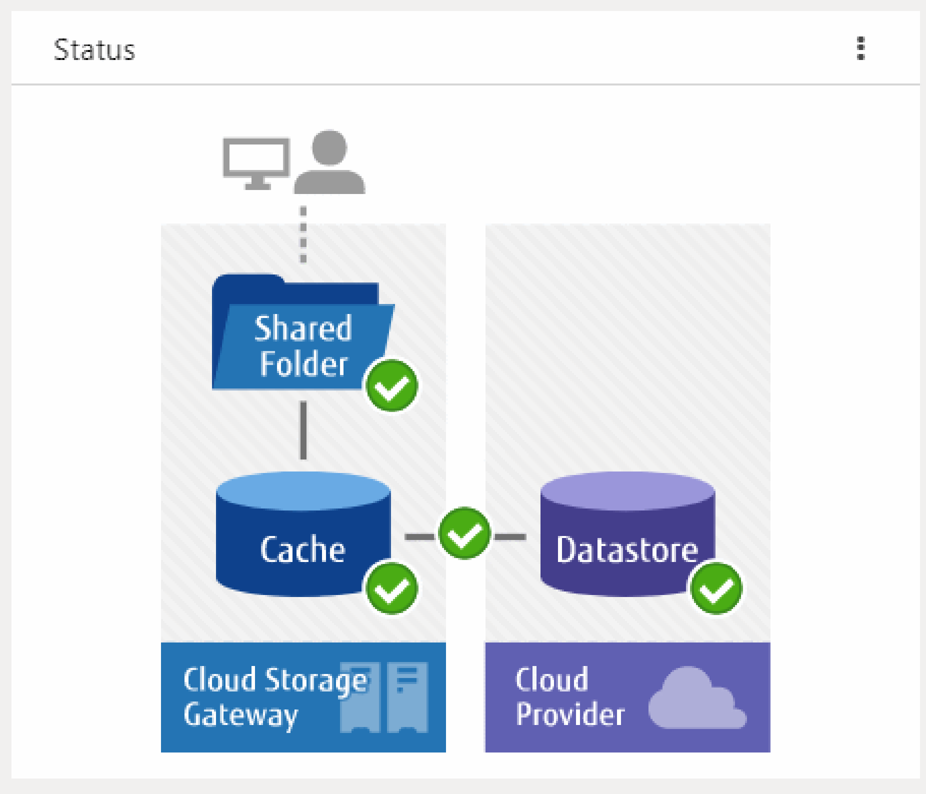
Point

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.

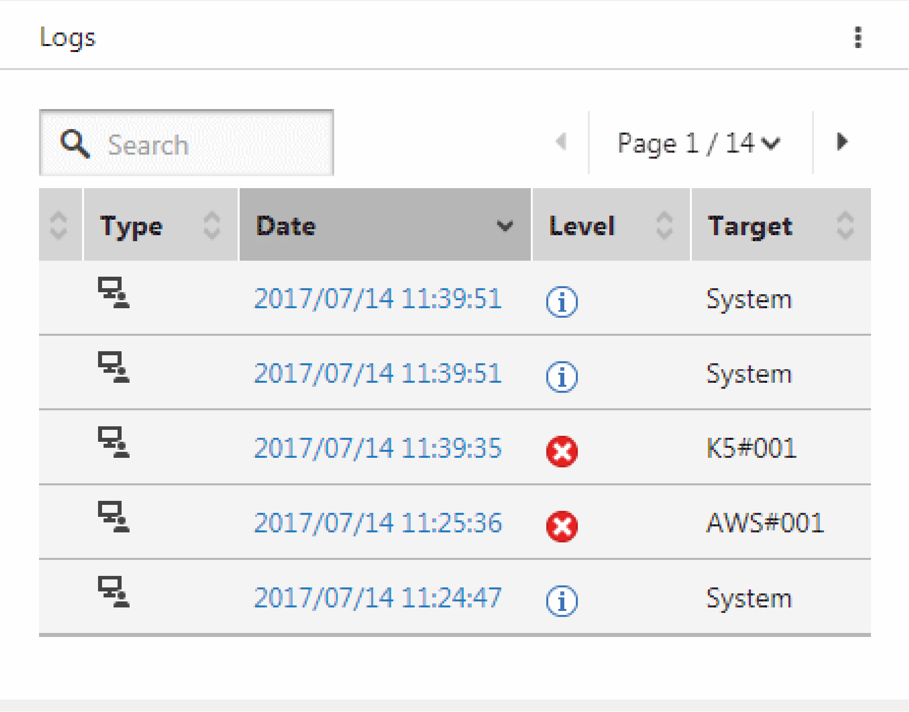
Table 4.2 Types and Meanings of Status Icons

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.

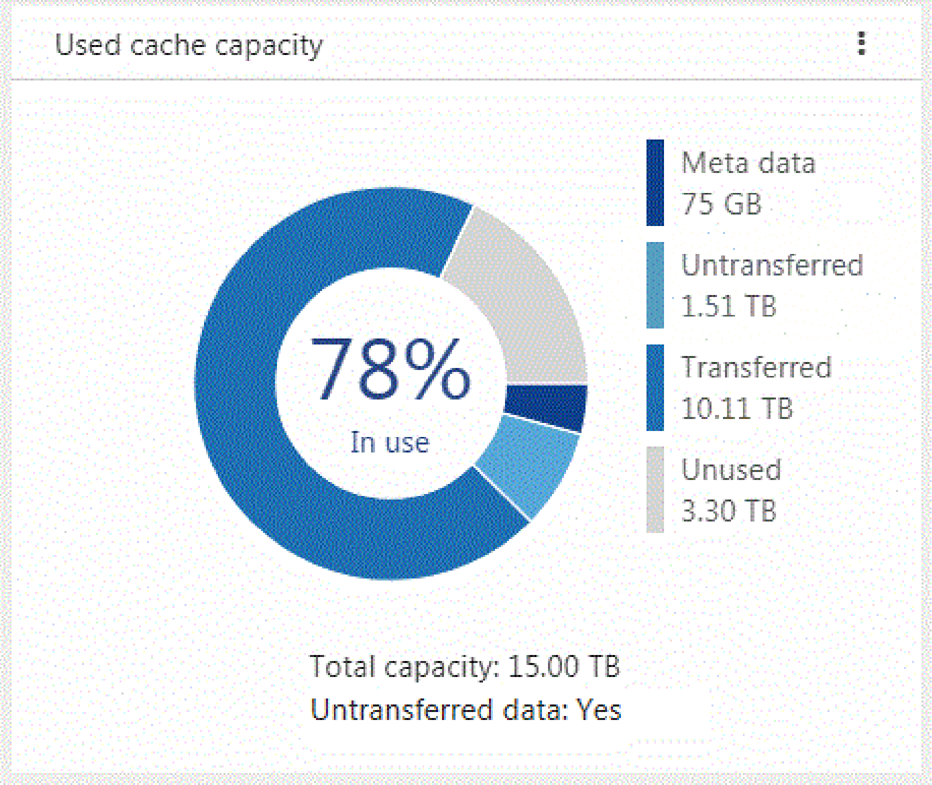
4.4 Capacity Checking

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

Used cache capacity is displayed as a pie chart.
If the unit for the values **Meta data**, **Untransferred**, **Transferred**, **Unused**, and **Total capacity** is GB, an integer value is displayed and if the unit is TB, a value up to two decimal places is displayed.

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

Table 4.3 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.

Note

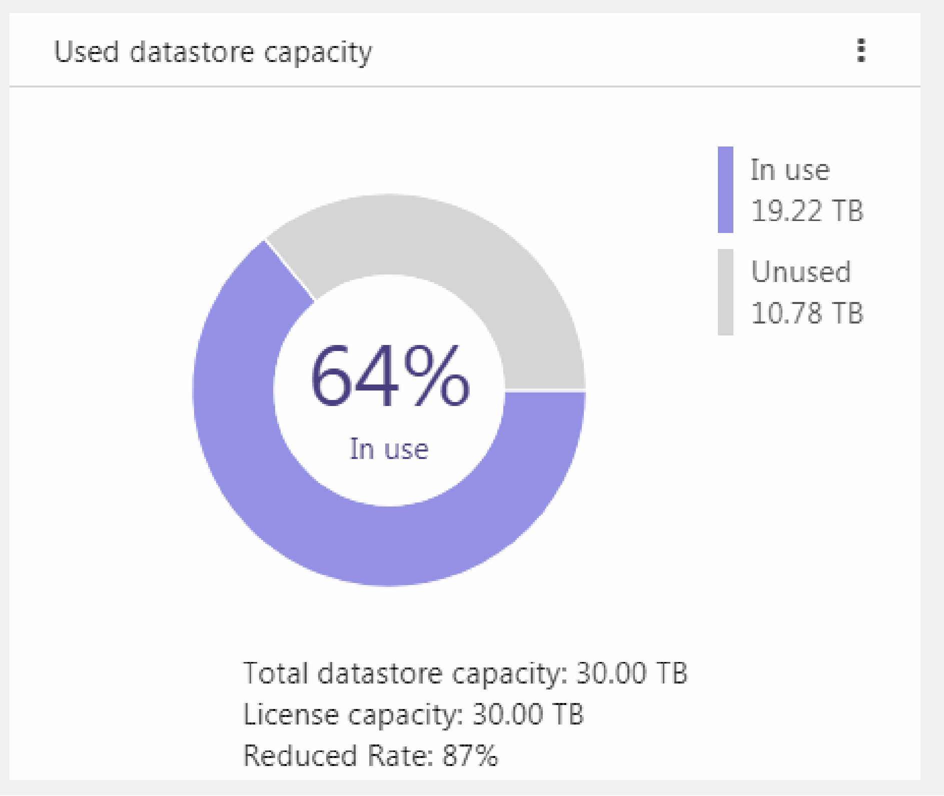
Values displayed in Transferred differ from the values displayed in "**In use**" in the Used datastore capacity panel.

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

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: 30.00 TB
Reduced Rate: 87%

Used datastore capacity is displayed as a pie chart.
If the unit for the values In use, **Unused**, **Total datastore capacity**, and **License capacity** is GB, an integer value is displayed and if the unit is TB, a value up to two decimal places is displayed.

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

Table 4.4 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.
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.
In use(%)	Displays the rate of **In use** to **Total datastore capacity** as a percentage.

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.

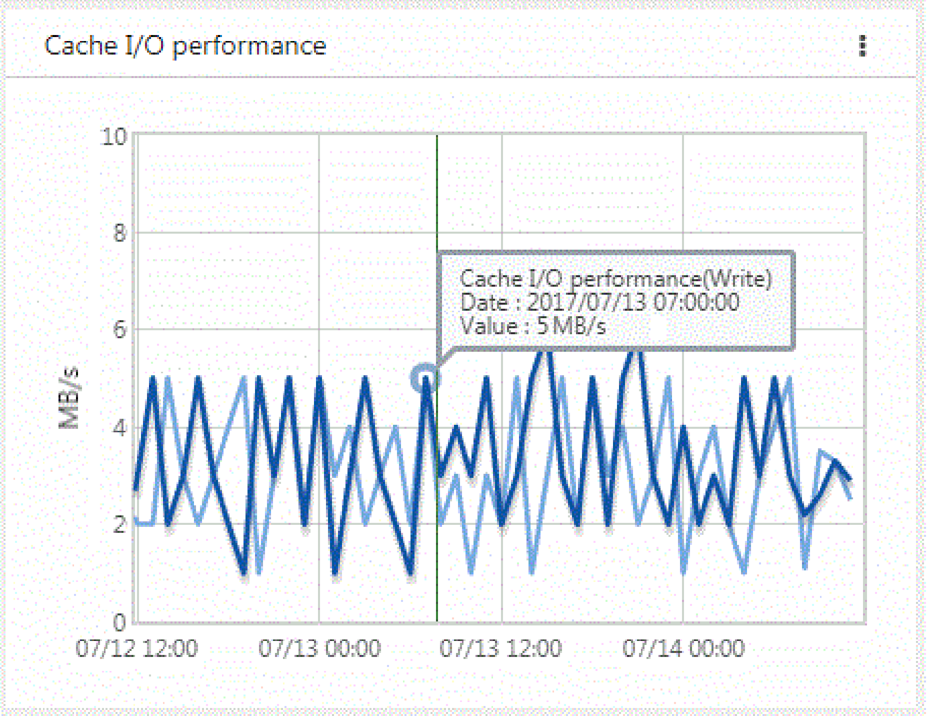
4.5 Performance Checking

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.

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 1-hour 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.

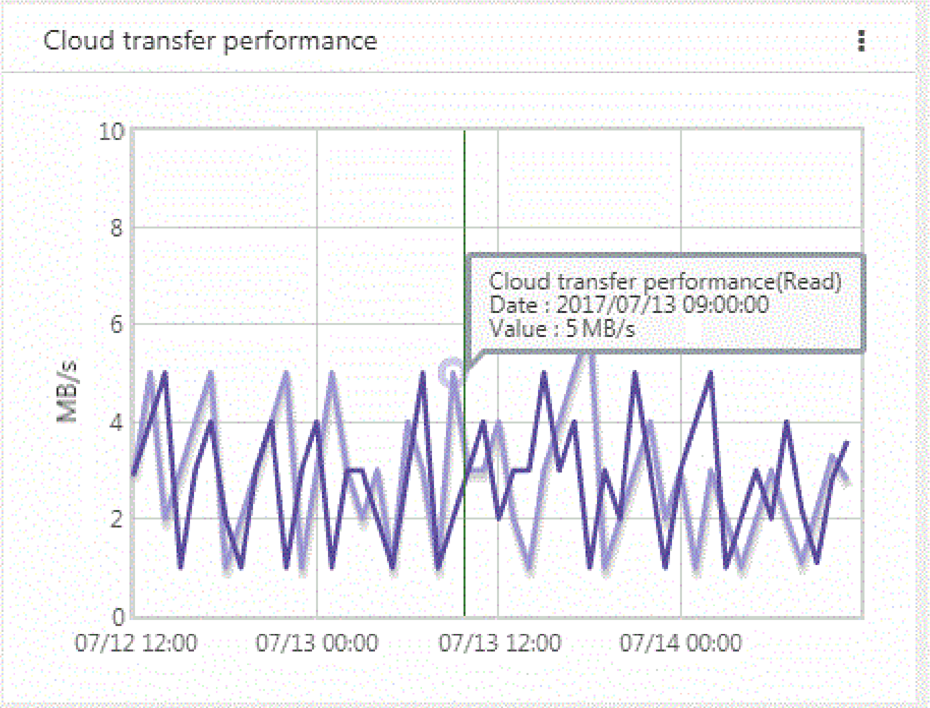
Table 4.5 Displayed Items

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 blue line graph	Displays the Read throughput to cache when reading from shared folders. The average value per hour is displayed by the graph.
Dark blue line graph	Displays the Write throughput to cache when writing to shared folders. The average value per hour 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
10
8
6
4
2
0
MB/s
Cloud transfer performance(Read)
Date : 2017/07/13 09:00:00
Value : 5 MB/s
07/12 12:00
07/13 00:00
07/13 12:00
07/14 00:00

The cloud transfer performance is displayed as a line graph in 1-hour 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 4.6 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.
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 hour is displayed by the graph.
Dark purple line graph	Displays the transfer performance from the cache to a cloud provider (Write) as the Write throughput. The average value per hour is displayed by the graph.

Chapter 5 Changing Operating Environments

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

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 "3.3.2 Information Required for Registering 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

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 the "**Done**" button.
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.

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

Compression

Note

It is not possible to change only the cache capacity.
If you want to change the cache capacity, you must recreate the datastore.

The data that is already registered is not compressed.

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.
   Confirm that the activation status of all shared folders for the datastore is "Disable".

   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 the **"Done"** button.

8. In the **Datastore** screen, confirm that the setting information for the datastore has been changed correctly.

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**

Point

- If you change the **Account/Access key ID** or **Password/Secret access key** of a cloud provider, 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.

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 or secret access key only
- When changing the account or the access key ID, and the password or the secret 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 the "Done" button.

7. In the "Cloud provider" screen, confirm that the setting information of the cloud provider has been changed correctly.

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

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 initial_setup.
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.

Chapter 6 Maintenance

This chapter describes how to perform maintenance for this product.

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 6.1 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. 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

Displayed Item	Description
	[❌]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.

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 6.2 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 6.3 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.

Displayed Item	Description
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 6.4 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.

6.2 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 FTP.
User: administrator
Password: The password set in "Change Administrator Password" of the Initial Setup Wizard.

6.3 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.

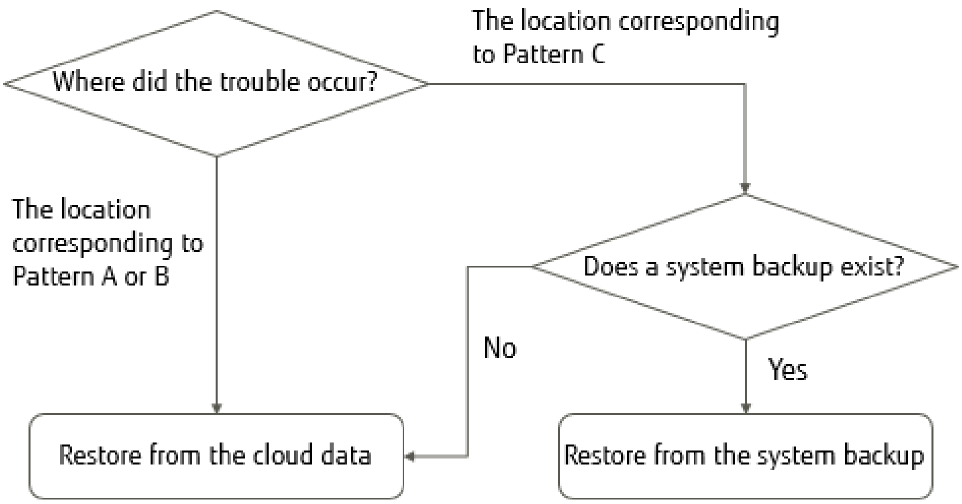
6.3.1 Restoration Procedure

6.3.1.1 Overview of the Disk Restoration Procedure

Table 6.5 Areas where Disk Failure Occurs

Pattern	System Area	Data Area
A	Failure	Failure
B	Normal	Failure
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 6.5 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 "6.3.1.2 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 "6.3.1.2 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 "6.3.1.3 Restoring from a System Backup" for details about the restoration procedure.

6.3.1.2 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 6.5 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 meta data recovery with the status key for CSG REST API response.

    - While the process is in progress

      The status key is "Active".

    - When the process is complete

      The status key is "N/A".

    - If a process error occurs

      The status key is "Error". You can identify the cause of the error in the event log that is output to the **Logs** panel on the CSG Web GUI dashboard. To perform a meta data recovery again after identifying the cause of the error, first delete the datastore and then start the procedure from step 6.

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

    Enter the same information for each item (other than the name of the shared folder) that was entered before the failure occurred. If you enter information that is different from the one entered before the failure occurred, that information is set in 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.

6.3.1.3 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.

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
    ```

6.4 Updating Software

The procedure for applying an update patch for this product is described below.

6.4.1 Procedure for Updating Software

The procedure for applying an update patch to this product is described below.

1. Obtain a patch from the support desk website.

2. Use a file transfer program (such as FTP) to transfer the patch to the virtual machine in which this product is running. (The transfer destination is /Administrator/ftp and the user name is administrator.)

3. Stop access to shared folders.

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

5. Execute the following commands to stop the service.

    ```
    # csgadm service stop fjsvcsgcp-webserver
    # csgadm service stop fjsvcsgcp-system
    # csgadm service stop fjsvcsgcp-database
    # csgadm service stop nfs
    # csgadm service stop smb
    # csgadm service stop fjsvcsgdp-datastore@*
    # csgadm service stop fjsvcsgdp-database@*
    ```

6. Execute the following command to apply the update patch. Change the file name, as required.

    ```
    # csgadm system patch-add -file /Administrator/ftp/CSG100_S20171203-01.tar.gz
    ```

7. Reboot the system by executing the following command.

    ```
    # csgadm power restart
    ```

6.5 Stopping and Rebooting the System

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

6.5.1 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
```

6.5.2 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
```

6.6 Changing the IP Address of This Product

The procedure for changing the IP address of the virtual machine in which this product is running is described below.

1. Start CSG Web GUI
2. In CSG Web GUI, click **Shared Folder** on the global pane.
3. Set the activation status of all shared folders to "Disable".
4. Start the Initial Setup Wizard, and change the IP address in "**Configure Network**".
   Refer to "2.3 Setting Up Virtual Appliances" for details about this procedure.
5. Restart the system.
   When inquired to restart the system as the last operation of step 4, restart the system. If you elected not to restart during the inquiry, execute the following command and restart the system.

```
# csgadm power restart
```

6. Restart CSG Web GUI after the system reboots.
7. In CSG Web GUI, click **Shared Folder** on the global pane.
8. Set the activation status of all shared folders to "Enable".

Information

This procedure is used to change the temporary IP address used for testing operations to the official IP address immediately before starting actual operations.

6.7 Expanding Areas by Recreating Cache

You can use the following procedure to expand the cache area.

1. Record the current settings of the cloud provider, datastore, shared folder, and system settings ([⚙] in the global pane).

2. Refer to the **Used cache capacity** panel in the dashboard of CSG Web GUI and wait until "Untransferred data" becomes "No".

3. In CSG Web GUI, click **Shared Folder** on the global pane.

4. Set the activation status of all shared folders to "Disable".

5. From the server virtualization software, delete the virtual machine in which this product is running.

6. 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.
   In this step, create a virtual disk for the cache area with the size after the expansion.

7. 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".

8. Register a cloud provider according to the settings recorded in step 1.
   Refer to "3.1 Registering a Cloud Provider" for details about how to register a cloud provider.

9. Create a datastore on the cloud provider that you registered in step 8 according to the settings recorded in step 1.
   Refer to "3.2 Registering a Datastore and Cache" for details about how to create a datastore.
   At this time, set a value for cache capacity that is sufficient to prevent the cache from becoming full.

10. Perform a meta data recovery for the datastore in order to restore the meta data in the cloud provider to the cache.
    Refer to step 7 in "6.3.1.2 Restoring from Cloud Provider Data" for details about how to perform meta data recovery.

11. Register the shared folder according to the content recorded in step 1.
    For the registration method, refer to "3.3 Registering a Shared Folder".

Note

Rebuilding the cache will delete the cache I/O performance and cloud transfer performance data on the dashboard.

Chapter 7 Deleting Operating Environments

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

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 the "Done" button.
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 the "Done" button.
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 the "Done" button.
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 the "Done" button.
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	In addition to 4.0GB, 1.2GB per 1TB datastore.	
Server virtualization software	For VMware vSphere	VMware vSphere 6.0 VMware vSphere 6.5
	For KVM	Red Hat(R) Enterprise Linux(R) 7.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)
Network adapter	For VMware vSphere	VMXNET3
	For KVM	Virtio
Virtual disk	System area	100 GB
	Data area	Greater than or equal to (cache capacity + 1MB). However, it should be at least 100 GB. It is recommended that you use RAID 1+0 for the disk space where the virtual disk is located.

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	Minimum: 20% of the datastore capacity Maximum: Size of the virtual disk connected to the virtual machine in which this product is running
Number of shared folders	128
Number of simultaneously connected servers	10
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	100 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

Item	Content
Types of supported files	Normal files, directories, symbolic links, hard link (However, directory hard links are not supported.)
Administrative user authentication	Local authentication, LDAP, Active Directory
NAS user authentication	Local authentication, LDAP, 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 K5 Object Storage Amazon S3 NIFCLOUD 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	20	FTP
		21	
		22	SSH
		9856 (Can be changed)	HTTPS
This product	Mail server	25 (Can be changed)	SMTP
	DNS server	53	DNS
	NTP server	123	NTP
	LDAP/AD server	389 (Can be changed)	LDAP/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.
Error	An error has occurred	When one of the following events occurs: - The cache capacity is used up - Error in cache disk
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	-
Error	An error has occurred	When one of the following events occurs: - Authentication failed when a datastore is connected

Status	Overview	Timing
		- 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.